



UNDERSTANDING AND MITIGATING CYBERFRAUD IN AFRICA

Oluwatoyin Esther Akinbowale, Mariann Polly Mashigo
& Mulatu Fekadu Zerihun

UNDERSTANDING AND MITIGATING CYBERFRAUD IN AFRICA



Published by AVARSITY Books, an imprint of AOSIS Scholarly Books, a division of AOSIS (Pty) Ltd.

AOSIS Publishing

15 Oxford Street, Durbanville, 7550, Cape Town, South Africa
Postnet Suite 110, Private Bag X19, Durbanville, 7551, Cape Town, South Africa
Tel: +27 21 975 2602
Website: <https://www.aosis.co.za>

Copyright © 2024 Oluwatoyin E Akinbowale, Mariann P Mashigo & Mulatu F Zerihun.
Licensee: AOSIS (Pty) Ltd

The moral right of the authors has been asserted.


Cover image: This cover design was created by Natascha Olivier/Coco Design with the use of an illustration by Vecteezy {33219991} obtained from Vecteezy.com, titled 'Cyber security and internet protection background ai generate', available from <https://www.vecteezy.com/photo/33219991-cyber-security-and-internet-protection-background-ai-generate>, copyright-free under the Vecteezy License terms.

Published in 2024

Impression: 1

ISBN: 978-1-991269-08-9 (print)

ISBN: 978-1-991270-08-5 (epub)

ISBN: 978-1-991271-08-2 (pdf) 

DOI: <https://doi.org/10.4102/aosis.2024.BK485>

How to cite this work: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town.

Printed and bound in South Africa.

Listed in OAPEN (<http://www.oapen.org>), DOAB (<http://www.doabooks.org/>) and indexed by Google Scholar. Some rights reserved.

This is an open-access publication. Except where otherwise noted, this work is distributed under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). A copy of this is available at <https://creativecommons.org/licenses/by-nc-nd/4.0/>. Enquiries outside the terms of the Creative Commons license should be sent to the AOSIS Rights Department at the above address or to publishing@aosis.co.za.



The publisher accepts no responsibility for any statement made or opinion expressed in this publication. Consequently, the publishers and copyright holders will not be liable for any loss or damage sustained by any reader as a result of their action upon any statement or opinion in this work. Links by third-party websites are provided by AOSIS in good faith and for information only. AOSIS disclaims any responsibility for the materials contained in any third-party website referenced in this work.

Every effort has been made to protect the interest of copyright holders. Should any infringement have occurred inadvertently, the publisher apologises and undertakes to amend the omission in case of a reprint.

UNDERSTANDING AND MITIGATING CYBERFRAUD IN AFRICA

**Oluwatoyin E Akinbowale
Mariann P Mashigo
Mulatu F Zerihun**



Social Sciences, Humanities, Education and Business Management domain editorial board at AOSIS

Commissioning Editor: Scholarly Books

Andries G van Aarde, MA, DD, PhD, D Litt, South Africa

Board members

Anthony Turton, Professor in the Centre for Environmental Management and Director of the TouchStone Resources (Pty) Ltd, University of the Free State, South Africa

Charles O'Neill, Associate Professor in the Department of Business Administration, The British University in Egypt, El Sherouk, Cairo Governorate, Egypt

Christi van der Westhuizen, Associate Professor and Head of the Centre for the Advancement of Non-Racialism and Democracy (CANRAD) research programme, Nelson Mandela University, South Africa

Emmanuel O Adu, Professor of Teacher Education and Curriculum Studies, Faculty of Education, University of Fort Hare, South Africa

Elphinah N Cisse, Professor of Nedbank Research Chair, Department of Continuing Professional Teacher Development, Faculty of Educational Sciences, Walter Sisulu University, South Africa

Jayaluxmi Naidoo, Associate Professor of Mathematics and Computer Science Education, College of Humanities, University of KwaZulu-Natal, South Africa

Johann Tempelhoff, Professor and Lead of the Cultural Dynamics of Water (CuDyWat) research niche and Head of the South African Water History Archival Repository, School of Basic Sciences, North-West University, South Africa

Llewellyn Leonard, Professor of Environmental Management and Chair of the Centre for Excellence (CoE) (Adaptation and Resilience), School of Ecological and Human Sustainability, University of South Africa, South Africa

Piet Naudé, Professor of Ethics related to Politics, Lead of the MBA programme in Business in Society and Leadership Development and Director of the University of Stellenbosch Business School, University of Stellenbosch, South Africa

Reina-Marie Loader, Programme Lead of the MA programme in Producing Film and Television and Lecturer in Film Production, Faculty of Media and Communication, Bournemouth University, United Kingdom

Siphamandla Zondi, Professor of Politics and International Relations, Faculty of Humanities, University of Johannesburg, South Africa

Stanley Murairwa, Professor and Head of the Department of Business Sciences, College of Business, Peace, Leadership and Governance, Africa University, Zimbabwe

Tembi Tichaawa, Associate Professor and Head of the Department of Tourism, School of Tourism and Hospitality, University of Johannesburg, South Africa

Vusiwana C. Babane, Department of Educational Psychology, Faculty of Education, University of the Western Cape, South Africa

Zilungile Sosibo, Professor of Education, Faculty of Education, Cape Peninsula University of Technology, South Africa

Peer-review declaration

The publisher (AOSIS) endorses the South African 'National Scholarly Book Publishers Forum Best Practice for Peer-Review of Scholarly Books'. The book proposal form was evaluated by our Social Sciences, Humanities, Education and Business Management editorial board. The manuscript underwent an evaluation to compare the level of originality with other published works and was subjected to rigorous two-step peer-review before publication by two technical expert reviewers who did not include the authors and were independent of the authors, with the identities of the reviewers not revealed to the authors. The reviewers were independent of the publisher and the authors. The publisher shared feedback on the similarity report and the reviewers' inputs with the manuscript's authors to improve the manuscript. Where the reviewers recommended revision and improvements, the authors responded adequately to such recommendations. The reviewers commented positively on the scholarly merits of the manuscript and recommended that the book be published.

Research justification

Cyberfraud is a global problem which has negative consequences on the global economy, public trust and the profitability, operation and reputation of financial institutions. The increasing rate of cyberfraud perpetration, especially in Africa, calls for sustainable solutions. The advancement in the technology, dynamics and anonymity of cyberspace make the process of cyberfraud mitigation a challenging task. An in-depth synthesis of the existing literature around cyberfraud carried out in this book reveals trends of occurrences, impact and state-of-the-art approaches deployed by financial institutions to mitigate cyberfraud. There is a high risk of falling victim to cyberfraud in Africa compared to the rest of the world. This is inspired by the evolution of Internet banking and its increasing population of subscribers in Africa coupled with the vulnerability of financial institutions in Africa to cyber-attacks, the slow pace of technological deployment and non-implementation of cybersecurity frameworks. If these trends continue, the implications of cyberthreats to the African economy may be damaging. The African continent cannot afford to lag in the global quest for cybersecurity and safe Internet banking operations. Efforts must be geared towards achieving cybersecurity and cyber resilience using enabling digital technologies. This is necessary for Africa's digital economy to thrive. Therefore, this scholarly and groundbreaking book seeks to engage in a conversation with experts specialising in the field of cyberfraud. Its primary audience comprises academics in the realm of digital technology, with the goal of elevating awareness regarding the perpetration of cyberfraud and establishing an effective strategy to ensure cybersecurity and the secure operation of Internet banking in Africa. The awareness includes the identification of the roles of the stakeholders: financial institutions, government, law enforcement agencies, policymakers, public and private sectors, including those who develop cyberspace, information and communication technology (ICT) sector, as well as the digital products and services providers. As cyberfraud is a cross-border challenge, regional and international synergy can promote technology aid, adoption or transfer to counter cyberfraud. These are some of the major focal points explored in this edited collection to provide statistics and explanations regarding the fraud phenomenon in terms of the rationale, loopholes exploited by the perpetrators and the possible innovative ways of mitigating it. It unravels the causes and dynamics of cyberfraud as well as the activities of cybercriminals to provide insights into sustainable and practical measures to mitigate it. The objective of this book is to enhance our comprehension of emerging technologies, the investigative processes involved in addressing fraud and the resources required to combat fraudulent activities. This involves identifying the underlying reasons and root causes of fraud and exploring potential strategies to reduce its occurrence. To accomplish this, this book utilises a combination of case studies, empirical data, systematic literature reviews and theoretical concepts, offering practical solutions to mitigate cyberfraud in this comprehensive study. The authors of this scholarly book confirm that no part of this work has been plagiarised or previously published elsewhere and that all possible similarities and overlaps were cleared by the use of iThenticate similarity check software.

Oluwatoyin E Akinbowale, Department of Economics, Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa.

Mariann P Mashigo, Department of Economics, Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa.

Mulatu F Zerihun, Department of Economics, Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa.

Dedication

To the staff members and students at TUT who succumbed to the dreadful coronavirus disease 2019 (COVID-19) pandemic between 2020 and 2022.

Contents

Biographical notes	xv
Abbreviations and acronyms, figures and tables appearing in the text and notes	xvii
List of abbreviations and acronyms	xvii
List of figures	xx
List of tables	xxiv
Acknowledgements	xxix
Foreword	xxxi
Preface	xxxiii
Chapter 1: Cyberfraud: Global trends, statistics and the impact on economic well-being	1
Introduction	1
Global trends	3
Statistics on cyberfraud	7
Impact on economic well-being	16
Conclusion	18
Chapter 2: Fraud investigation and mitigation	19
Introduction	19
Overview of fraud	20
Cyberfraud and its prevalent forms	25
Phishing	27
Data theft	27
Hacking	29
Malware	29
Spamming	29
Skimming	30
Online theft	30
Identity theft	30
Spying	30
Cyberstalking	30
Pharming	31
Vishing	31
Spoofing	31

Whaling	31
Software supply chain attack	31
Motivation for cyberfraud perpetration	31
Major loopholes for cyberfraud perpetration	32
Customers	32
Organisation	33
Cyberspace	35
Impact of cyberfraud	36
Impact of cyberfraud at the micro level	37
Shareholders' dissatisfaction	39
Loss of money and profitability	41
Loss of goodwill and reputation	43
Impact of cyberfraud at macro level	44
Possible mitigation approaches to cyberfraud	44
Conclusion	46
Chapter 3: Cyberfraud: Theoretical perspectives	47
Introduction	47
General fraud theories	48
Fraud triangle theory	48
Fraud scale theory	50
Fraud diamond theory	51
Fraud box key model	52
Fraud management lifecycle theory	53
Routine activity theory	57
The self-control theory	58
Akers' social learning theory	59
Denial of risk theory	60
General strain theory	62
Agency fraud theory	63
Control fraud theory	63
Eclectic theory	63
Probable causes of fraud from theoretical perspectives	63
Management control systems theories for fraud mitigation	63
Closed-end management control system	65
Corporate social responsibility theory	68
The Carroll theory	69
Triple bottom-line theory	71

Stakeholders' theory	71
Forensic accounting	71
Forensic accounting theory	75
Conclusion	77
Chapter 4: Cyberfraud mitigation decision-making: From theory to application	79
Introduction	79
Cyberfraud mitigating approaches from the theoretical perspectives	80
Methodology: Cyberfraud mitigation using the fuzzy analytical hierarchy process	81
Results and discussion	86
Conclusion	91
Chapter 5: Combatting cyberfraud in the digital era: The machine learning approach	93
Introduction	93
The machine learning approach	95
Application of the machine learning approach for classification problem	96
Procedure for the clustering analysis	99
Results and discussion	100
Results obtained for the classification analysis	100
Results obtained for the clustering analysis	104
Conclusion	109
Chapter 6: The role of big data technology in fraud mitigation	111
Introduction	111
The role of big data technology	112
Methodology: Systematic literature review on big data technology	114
Data sources	114
Keywords search	114
Inclusion and exclusion criteria	115
Review of the role of big data technology in combatting fraud	115
Theoretical literature review on the role of big data in fraud mitigation	116
Empirical review on the role of big data in cyberfraud mitigation	118
Empirical review on the role of big data in general fraud mitigation	120

Conceptual literature review on the role of big data in fraud mitigation	121
Conclusion	124
Chapter 7: Impact of information and communication technology and forensic accounting in fraud mitigation	127
Introduction	127
Information and communication technology and fraud mitigation	128
Fraud, information and communication technology and forensic accounting	130
Systematic literature review	131
The concept of fraud	131
Forensic accounting and information and communication technology	131
The nature of forensic accounting	133
Challenges and prospects of computerised forensic investigation	136
Techniques involved in forensic accounting for fraud examination	137
Benford's law	137
Computer-assisted auditing tools	138
Theory of relative size factor	138
Basic skills required by forensic accountants	138
Core skills	139
Enhanced skills	140
The fraud deterrence cycle	140
Empirical review on forensic accounting	141
Empirical review on information technology and forensic accounting	146
Underpinning theories of fraud	147
Sociological theory of crime or fraud (or both)	147
Psychological or physiological theory	147
Culture transmission theory	148
Fraud triangle theory	148
Perceived pressure, incentives and motivation	148
Perceived opportunity	148
Rationalisation	149
The independent variables	150
The dependent variable	150
Variables	151
Conclusion	152

Chapter 8: The effect of forensic accounting software on the accuracy of financial investigation	155
Introduction	155
Forensic accounting software	156
Method	159
Results and discussion	164
Conclusion	171
Chapter 9: The implementation of forensic accounting for fraud mitigation in financial institutions: A strength-weakness-opportunity-threat approach	173
Introduction	173
The implementation of forensic accounting for fraud mitigation	174
Fraud types and some associated concepts	175
Fraud and types of fraud	176
The concepts of forensic accounting	176
Methodology	177
Conclusion	191
Chapter 10: The roles of digital forensics in fraud investigation: A systematic literature review	193
Introduction	193
The roles of digital forensics in fraud investigation	193
Systematic literature review on digital forensics	195
Types of digital forensics	206
Disk and storage forensics	206
Network forensics	206
Database forensics	206
Malware forensics	207
Email forensics	207
Memory forensics	207
Mobile phone forensics	209
Challenges faced by digital forensics	210
Merits and demerits of digital forensics	211
Demerits	211
Methodology, results and discussions	213
Methodology	213
Results and discussions	214
Conclusion	216

Chapter 11: A systems-thinking approach	217
Introduction	217
Information and security frameworks for internal and cyberfraud mitigation in financial institutions	218
Challenges of organisation’s information security	219
Information security risk management	221
Methodology: Systems thinking	225
Information and cybersecurity framework development	227
Systems’ component	228
Sensor	228
Connectivity	229
Big data analytics	229
User interface	229
Procedure for information security system implementation	230
Use of a checkpoint firewall with good processing capability	230
Network firewall	230
Endpoint security firewall	231
Network access control	231
Acquisition of a database or web server firewall	232
Conclusion	233
Chapter 12: Towards cyberfraud risk mitigation: A bow tie approach	235
Introduction	235
Risk management	238
Methodology: Bow tie technique	241
Results and discussion	247
Conclusion	250
Chapter 13: Cyberfraud occurrences: Africa’s experience	251
Introduction	251
Cyberfraud: Africa’s experience	252
Cybersecurity in Africa	258
Leading African countries in tackling cyberfraud and improving cybersecurity	261
Mauritius	261
Rwanda	262
Kenya	262
Nigeria	263

Uganda	263
South Africa	264
Conclusion	271
Chapter 14: Investigating the effectiveness of management control systems employed for fraud mitigation in the South African banking industry	273
Introduction	273
Management control systems fight against cyberfraud	274
Methodology	277
Non-parametric analysis	278
Cross-tabulation	278
Fisher's exact test	278
Spearman's correlation analysis	279
Results and discussion	280
Conclusion	298
Chapter 15: Policy lessons	301
Introduction	301
Policy lessons for combatting and mitigation strategies	301
Policy lessons on minimising economic welfare impacts	303
Lessons for African economies	305
Lessons from emerging and developed economies	307
Conclusion	308
References	311
Appendix	351
Index	355

Biographical notes

Oluwatoyin E Akinbowale

Department of Economics, Faculty of Economics and Finance,
Tshwane University of Technology,
Pretoria, South Africa
Email: oluwateee01@gmail.com
ORCID: <https://orcid.org/0000-0001-5886-3018>

Oluwatoyin E Akinbowale obtained her Bachelor of Science (BSc) in Accounting from Joseph Ayo Babalola University, Ikeji Arakeji, Nigeria, in 2013 and her Master of Science (MSc) from Afe Babalola, Ado-Ekiti (ABUAD), Nigeria, in 2016. She worked briefly at ABUAD as an assistant lecturer before proceeding to Tshwane University of Technology (TUT), Pretoria, South Africa (RSA), as a doctoral candidate, where she obtained her Doctor of Business Studies with a specialisation in Finance in 2022. She is a member of the South African Institute of Business Accountants (SAIBA) as well as a member of the Nigerian Institute of Management (NIM). She was a postdoctoral research fellow at the Department of Economics, Faculty of Economics and Finance, TUT, RSA, during her contribution to this scholarly book. Her research fields include forensic accounting, management accounting, strategic management and accounting information systems.

Mariann P Mashigo

Faculty of Economics and Finance,
Tshwane University of Technology,
Pretoria, South Africa
Email: mashigomp@tut.ac.za
ORCID: <https://orcid.org/0000-0002-0810-1506>

Mariann P Mashigo is the executive dean of the Faculty of Economics and Finance at TUT, Pretoria, RSA. She began her academic career as a lecturer and has held senior positions within the university. She earned her PhD in Economics from the University of Johannesburg (UJ), Johannesburg, RSA, which focused on extending credit to the low-income and poor households in RSA with particular reference to a system of principles. She has completed her Doctorate in Business Administration (DBA) specialising in Higher Education Management from the University of Bath in the United Kingdom (UK), which focuses on the assessment of co-operative governance in the post-1994 democratic South African higher education (HE) sector. She has successfully supervised postgraduate students and has published various research articles in several accredited journals, both locally and internationally. She received an excellence award from the South African Savings Institute and Metropolitan, which was held at the South African Reserve Bank (SARB) in 2004. She further received eight awards as Faculty Woman Researcher of the Year (between 2011 and 2017) in the Faculty of Economics and Finance, TUT, Pretoria, RSA.

Mulatu F Zerihun

Department of Economics, Faculty of Economics and Finance,
Tshwane University of Technology,
Pretoria, South Africa,
Email: zerihunmf@tut.ac.za
ORCID: <https://orcid.org/0000-0003-4797-928X>

Mulatu F Zerihun is a professor of Economics and a National Research Foundation (NRF) C2-rated researcher. Currently, he is the head of the Department of Economics at the Faculty of Economics and Finance, TUT, Pretoria, RSA. He earned his MSc in Economics from Addis Abba University, Ethiopia, in 2005; a DBA from TUT Business School, Tshwane University of Technology, in 2014; and PhD in Economics from the University of Pretoria, Pretoria, in 2015. He has been receiving academic excellence awards in different categories since 2014. He has extensive teaching and research experience for more than two decades in higher education institutions (HEIs) and five years' experience in the industry. His research interest focuses on development issues in the sub-Saharan African context. He has published widely in areas related to open economy macroeconomics, international trade and finance, development macroeconomics and environmental economics.

Abbreviations and acronyms, figures and tables appearing in the text and notes

List of abbreviations and acronyms

4IR	Fourth Industrial Revolution (Industry 4.0)
5IR	Fifth Industrial Revolution (Industry 5.0)
ABSA	Amalgamated Banks of South Africa
AfCFTA	Africa Continental Free Trade Area
AHP	analytic hierarchy process
AI	artificial intelligence
AICPA	American Institute of Certified Public Accountants
ANN	artificial neural network
APP	Authorised Push Payment
ASLT	Akers' social learning theory
ATM	automated teller machine
BDA	big data analytics
BEC	Business Email Compromise
BVN	bank verification number
CAAT	computer-assisted auditing techniques
CANRAD	Centre for the Advancement of Non-Racialism and Democracy
CART	Classification and Regression Tree
CDE	comprehensive digital evidence
CECC	Council of Europe Convention on Cybercrime
CFE	certified fraud examiner
CFFTPM	Computer Forensics Field Triage Process Model
CI	consistency index
CIRT	Computer Incident Response Team
CR	consistency ratio
CSIRT	Computer Security Incident Response Team
CSR	corporate social responsibility
DBA	Doctorate in Business Administration
DDoS	distributed denial-of-service

DF	digital forensics
DFIF	digital forensic investigation framework
DIN	digital identity network
DML	data manipulation language
DoS	denial-of-service
DRT	denial of risk theory
DTL	digital technology level
ECT	<i>Electronic Communication and Transaction Act 25 of 2002</i>
EET	extent of employee theft
EFAP	extent of forensic accounting practices
EFCC	Economic and Financial Crimes Commission
EFR	extent of financial fraud
ETMT	extent of top management fraud
EU	European Union
FA	forensic accounting
FAHP	fuzzy analytical hierarchy process
FBI	Federal Bureau of Investigation
FDI	foreign direct investment
FDT	fraud diamond theory
FIRST	Forum of Incident Response and Security Teams
FMLT	fraud management lifecycle theory
FNB	First National Bank
FST	fraud scale theory
FTK	Forensic Tool Kit
FTT	fraud triangle theory
GA	genetic algorithm
GCI	Global Cybersecurity Index
GDP	gross domestic product
GPS	global positioning system
GST	general strain theory
HE	higher education
HEI	higher education institutions
HMM	Hidden Markov Model
ICT	information and communication technology
IDS	intrusion detection system
IFC	International Finance Corporation
IoT	Internet of Things
IP	Internet protocol
ISO	International Standardisation Organisation

IT	information technology
ITU	International Telecommunication Union
LP	linear programming
MCD	multicriteria decision
MCS	management control system
MCSs	management control systems
ML	machine learning
NAFT	number of accountants with forensic accounting skills
NCPF	National Cyber Security Policy Framework
NCSA	National Cyber Security Authority
NCSI	National Cyber Security Index
NGOs	non-governmental organisations
NIM	Nigerian Institute of Management
OCR	optical character recognition
PAIA	<i>Promotion of Access to Information Act 2 of 2000</i>
PFA	presence of forensic accountant
PIN	personal identification number
POPIA	<i>Protection of Personal Information Act 4 of 2013</i>
POS	point-of-sale
PRISMA	preferred reporting items for systematic reviews and meta-analysis
ProDF	proactive digital forensics
PwC	PricewaterhouseCoopers
R&D	research and development
RAM	random access memory
RAT	routine activity theory
ReDF	reactive digital forensics
RI	random index
RIDITS	relative to an identified distribution
RSF	relative size factor
SABRIC	South African Banking Risk Information Centre
SAIBA	South African Institute of Business Accountants
SAPS	South African Police Service
SARB	South African Reserve Bank
SCT	self-control theory
SIM	subscriber identity module
SMEs	small and medium-sized enterprises
SOM	self-organising map
SPSS	Statistical Package for Social Science

SWOT	strength, weakness, opportunity and threat
TFN	triangular fuzzy number
TUT	Tshwane University of Technology
UAE	United Arab Emirates
UJ	University of Johannesburg
UK	United Kingdom
UN	United Nations
US	United States
USB	universal serial bus
VPNs	virtual private networks

List of figures

Figure 1.1:	Reported economic crime rates across various regions of the world.	8
Figure 1.2:	The global average cost of data breach in 2022 (in millions, USD).	12
Figure 1.3:	Survey on the rate of internal and external fraud.	12
Figure 1.4:	Wide fraud risk assessment and response rate.	13
Figure 2.1:	The major components of fraud.	21
Figure 2.2:	Types of internal fraud.	24
Figure 2.3:	An approach to internal fraud control.	25
Figure 2.4:	Reported economic crime of selected countries in 2018.	36
Figure 3.1:	Fraud triangle.	49
Figure 3.2:	Fraud scale.	50
Figure 3.3:	Fraud diamond theory.	51
Figure 3.4:	Fraud box key model.	52
Figure 3.5:	Fraud management lifecycle.	54
Figure 3.6:	Fraud investigation skillsets.	56
Figure 3.7:	Routine activity theory.	57
Figure 3.8:	The constructs of the denial of risk theory.	61
Figure 3.9:	Carroll's theory of corporate social responsibility.	70
Figure 4.1:	Fuzzy analytical hierarchy process hierarchy structure.	82
Figure 4.2:	Triangular fuzzy elements computation for the criteria.	88
Figure 4.3:	Criterion 1 triangular fuzzy elements (internal control) with respect to the options (alternatives).	88

Figure 4.4:	Criterion 2 triangular fuzzy elements (cybersecurity) with respect to the options (alternatives).	88
Figure 4.5:	Criterion 3 triangular fuzzy elements (synergy among all anti-fraud capacities and regulators) with respect to the options (alternatives).	89
Figure 4.6:	Criterion 4 triangular fuzzy elements (digital technologies and data analytics) in relation to the alternatives.	89
Figure 4.7:	Normalised weights of the options (alternatives) in relation to the identified criteria.	91
Figure 5.1:	Neural network architecture for fraud detection.	98
Figure 5.2:	Neural network architecture for the clustering analysis.	99
Figure 5.3:	Validation performance goal.	100
Figure 5.4:	The gradient and validation check.	101
Figure 5.5:	Error histogram.	102
Figure 5.6:	Confusion matrix.	103
Figure 5.7:	Receiver operating characteristics.	104
Figure 5.8:	Self-organising map topography.	105
Figure 5.9:	Self-organising map hits.	105
Figure 5.10:	Self-organising map neighbour weight distance.	106
Figure 5.11:	Self-organising map neighbour connections.	107
Figure 5.12:	Self-organising map weight positions.	107
Figure 5.13:	The weights of the eleven potential red flags.	108
Figure 6.1:	Conceptual framework for big data analysis for fraud detection.	113
Figure 6.2:	Big data analytics value chain.	121
Figure 7.1:	Framework employed for article selection.	132
Figure 7.2:	Forensic accounting and management control systems for cyberfraud mitigation.	135
Figure 7.3:	Core skills of a forensic accountant.	139
Figure 7.4:	Enhanced skills of a forensic accountant.	140
Figure 7.5:	Fraud deterrence cycle.	141
Figure 7.6:	Fraud triangle theory.	149
Figure 7.7:	Framework for the investigation of the effect of it on forensic accounting practice.	151
Figure 8.1:	Framework for the methodology employed.	161

Figure 8.2:	Framework for the implementation of forensic accounting software for fraud detection.	162
Figure 8.3:	Pie chart for the responses for Q1.	165
Figure 8.4:	Pie chart for the responses for Q2.	166
Figure 8.5:	Pie chart for the responses for Q3.	167
Figure 8.6:	Pie chart for the responses for Q4.	168
Figure 9.1:	Prevalence of various forms of economic crimes in 2018.	175
Figure 9.2:	Potential of forensic accounting implementation for fraud mitigation based on the three major threats or weaknesses affecting the implementation of forensic accounting.	185
Figure 9.3:	Framework for addressing capacity development and curriculum review for effective forensic accounting implementation.	186
Figure 9.4:	Framework for evidence management.	187
Figure 10.1:	Digital forensic model proposed by Reith et al.	196
Figure 10.2:	Components of the advanced data acquisition model for digital forensic accounting proposed by Adams.	197
Figure 10.3:	Components of the digital model proposed by Carrier and Spafford.	198
Figure 10.4:	Proposed model for cybercrime investigation.	199
Figure 10.5:	Proposed computer forensics field triage process model by Rogers et al.	200
Figure 10.6:	Framework for digital forensic investigation proposed by Köhn et al.	201
Figure 10.7:	Forensic process proposed by Kent et al.	201
Figure 10.8:	Digital framework for forensic accounting, which incorporates legal issues proposed by Leong.	202
Figure 10.9:	Process model for incidence response and digital forensics proposed by Freiling and Schwittay.	204
Figure 10.10:	Framework for the systematic literature review.	214
Figure 11.1:	Information security management framework recommended by NIST.	223
Figure 11.2:	Causal loop diagram for internal and cyberfraud.	225
Figure 11.3:	Conceptual information security framework for internal and cyberfraud mitigation.	227

Figure 11.4:	Components of the designed information security system for internal and cyberfraud mitigation.	228
Figure 11.5:	Firewall and its specifications for cybersecurity.	233
Figure 12.1:	Risk management cycle.	241
Figure 12.2:	Link between fraud control, risk assessment, risk management and investigation.	241
Figure 12.3:	Bow tie framework for cyberfraud risk management.	243
Figure 12.4:	Cause-and-effect diagram.	247
Figure 12.5:	Likelihood and consequences of cyberfraud risk.	247
Figure 13.1:	Reported economic crime in South Africa and global average rate in 2020.	256
Figure 13.2:	Total cyberfraud incidents reported from 2017 to 2020 and the losses incurred.	257
Figure 13.3:	Type of cyberfraud and the losses incurred.	258
Figure 13.4:	Five pillars of cybersecurity assessment in Africa.	259
Figure 14.1:	Cross-tabulation of the effect of investigation on the rate of cyberfraud occurrence.	283
Figure 14.2:	Cross-tabulation of the effect of disclosure to the board on the rate of cyberfraud occurrence.	283
Figure 14.3:	Cross-tabulation of the effect of disclosure to the regulator on the rate of cyberfraud occurrence.	284
Figure 14.4:	Cross-tabulation of the effect of disclosure to the regulator on the rate of cyberfraud occurrence.	284
Figure 14.5:	Cross-tabulation of the effect of disclosure to the auditor on the rate of cyberfraud occurrence.	284
Figure 14.6:	Cross-tabulation of the effect of external counsel on the rate of cyberfraud occurrence.	285
Figure 14.7:	Cross-tabulation of the effect of disclosure to other stakeholders on the rate of cyberfraud occurrence.	285
Figure 14.8:	Cross-tabulation of the effect of public disclosure on the rate of cyberfraud occurrence.	285
Figure 14.9:	Cross-tabulation of the effect of governance resources on the rate of cyberfraud perpetration.	290
Figure 14.10:	Cross-tabulation of the effect of third-party management on the rate of cyberfraud perpetration.	290
Figure 14.11:	Cross-tabulation of the effect of risk assessment on the rate of cyberfraud perpetration.	291

Figure 14.12:	Cross-tabulation of the effect of training and communication on the rate of cyberfraud occurrence.	291
Figure 14.13:	Cross-tabulation of the effect of monitoring and auditing on the rate of cyberfraud occurrence.	291
Figure 14.14:	Cross-tabulation of the effect of investigation and incentives on the rate of cyberfraud occurrence.	292
Figure 14.15:	Cross-tabulation of the effect of policies and procedures on other stakeholders on the rate of cyberfraud occurrence.	292
Figure 14.16:	Link between fraud control, risk assessment, risk management and investigation.	296

List of tables

Table 1.1:	Comparative analysis of the period before, during and after COVID-19.	4
Table 1.2:	Human-initiated and bot attacks carried out across the continents.	7
Table 1.3:	Reported economic crime rates across various regions of the world.	8
Table 1.4:	Most prevalent cyberattacks by region.	9
Table 1.5:	Countries with the highest and lowest cases of data breaches between the second and third quarters of 2022.	10
Table 1.6:	NCSI and the digital technology level.	11
Table 1.7:	Banking survey report on economic crime.	15
Table 1.8:	Cost of cybercrime as a function of the gross domestic product for selected countries.	17
Table 1.9:	Global cost of financial crime compliance.	17
Table 2.1:	Forms of cybercrimes in financial institutions.	28
Table 2.2:	Cybercrime density for the top 10 countries in the world.	40
Table 2.3:	Prevalent form of cybercrime, average loss, number of victims and total loss for 2021.	43
Table 2.4:	Impact of cybercrime on the global economy.	45
Table 3.1:	Probable causes of fraud from the fraud theories reviewed.	64
Table 3.2:	Strength, weaknesses and benefits of the three major corporate social responsibility theories.	72

Table 4.1:	Suggested approaches for mitigating cyberfraud.	81
Table 4.2:	Fuzzy linguistic scale.	83
Table 4.3:	Impact of the criteria and the assigned triangular fuzzy numbers.	84
Table 4.4:	Assessment of Criterion 1 (internal control) with respect to the three options (alternatives).	84
Table 4.5:	Assessment of Criterion 2 (cybersecurity) with respect to the three options (alternatives).	85
Table 4.6:	Assessment of Criterion 3 (synergy among all anti-fraud capacities and regulators) with respect to the three options (alternatives).	85
Table 4.7:	Assessment of Criterion 4 (use of digital technologies and data analytics) with respect to the three options (alternatives).	85
Table 4.8:	The values of the eigenvector and geometric mean for the criteria.	86
Table 4.9:	Consistency indices for the pairwise comparison process.	86
Table 4.10:	Summary of the companies with respect to the four criteria.	89
Table 4.11:	Defuzzified and normalised weights of the criteria.	90
Table 4.12:	Defuzzified and normalised weights of the alternatives.	90
Table 5.1:	Prevalent forms of cybercrime, the average loss, number of victims and total loss for 2021.	96
Table 5.2:	Output factors and the allocated values.	97
Table 6.1:	Search strategy adopted in the present systematic review and meta-analysis.	115
Table 6.2:	Possible sources of data for fraud investigation, the possible measures and indicators.	122
Table 6.3:	DBA for fraud investigation	122
Table 6.4:	Summary of the major big data analytics technologies and their functions.	123
Table 6.5:	Summary of the major findings on the application of big data for fraud mitigation.	124
Table 8.1:	Survey results for Q1 (information technology enables easy presentation of data and supporting evidence by forensic accountants).	164

Table 8.2:	Survey results for Q2 (forensic accountants can use specialised computer software and hardware by forensic accountants to preserve, collect, analyse and document evidence).	165
Table 8.3:	Survey results for Q3 (computerised information enables forensic accountants to investigate disputes or fraud).	166
Table 8.4:	Survey results for Q4 (the implementation of forensic accounting principles is a challenge for regular accountants and accounting auditors in Nigeria).	167
Table 8.5:	Accuracy of financial reporting investigation.	170
Table 8.6:	Results from chi-square and Fischer’s exact tests.	170
Table 9.1:	The strength-weakness-opportunity-threat analysis of forensic accounting.	179
Table 9.2:	Combination of the components of the strength-weakness-opportunity-threat approach.	183
Table 10.1:	Recent advances in the development of a sustainable digital forensic framework for fraud investigation.	215
Table 12.1:	Cyberfraud risk and risk scores.	245
Table 12.2:	Risk matrix.	249
Table 13.1:	Business email compromise recorded from January 2020 to April 2022.	255
Table 13.2:	Cybersecurity security ranking of selected African countries.	260
Table 13.3:	The GCI report on cybersecurity for African member states.	260
Table 13.4:	Attempts made by selected African countries to fight cybercrime and the limitations.	269
Table 14.1:	Methods of fraud identification.	280
Table 14.2:	Statistical analysis for the pair of significant factors for cyberfraud occurrence and method of identification.	281
Table 14.3:	Cross-tabulation for variables with positive and strong relationship with cyberfraud perpetration.	282
Table 14.4:	Cross-tabulation for variables with negative but weak relationship with cyberfraud perpetration.	282
Table 14.5:	Organisation’s fraud programme.	287

Table 14.6:	The statistical analysis for the pair of the significant factors for cyberfraud occurrence and organisation's fraud programme.	288
Table 14.7:	Cross-tabulation for variables with positive and strong relationships with cyberfraud perpetration.	289
Table 14.8:	Cross-tabulation for variables with negative and strong relationships with cyberfraud perpetration.	289

Acknowledgements

Our appreciation goes to the Almighty God, the Father and the Source of our inspiration, for giving us his sufficient grace, strength, wisdom, understanding and guidance and for sparing us throughout the preparation of this scholarly book.

We are highly grateful to the internal and external reviewers, editors and, in particular, the editorial board members of AOSIS Scholarly Books for bringing our dream into reality. Their thoughts, ideas and perspectives have given us exposure to the knowledge we have placed in this book. Sincere thanks go to the Tshwane University of Technology (TUT) for their financial support and motivation. We extend our special thanks to the following people who positively contributed to the shaping and completion of this book:

- Prof. Georgina Phillipina Coetzee and Mrs Eurika Coetzee for all the logistical support, motivation and encouragement from the beginning to the successful completion of this book.
- Dr Helena Kruger-Roux for her professional editing of the text of this book.

We are highly grateful to and appreciative of our family members and children for their patience and understanding during our late-night book-writing and preparation sessions. We further acknowledge the unwavering support and encouragement of our friends, colleagues and relatives.

Foreword

Oladipo O David

School of Economic Sciences, North-West University,
Vanderbijlpark, South Africa

Digitalisation promotes deploying machines, digital technology and the Internet to perform economic tasks, including financial and banking transactions. The Fourth Industrial Revolution (4IR) (Industry 4.0) further capacitates the Internet of Things (IoT), creating a smart society, production and transactions. The 'digital provide' penetration has increased the concern for cyber safety and fraud, especially in developing countries like Africa. The advent of the Fifth Industrial Revolution (5IR) (Industry 5.0) tends to checkmate the grey areas of digitalisation highlighted by the 'technophobes'. The recent evolution of information technology (IT), digital technology and the number of Internet users continue to spark an increase in the rate of cyber-attacks, resulting in cyberfraud perpetration and exposing people and businesses to cyber risk. Business organisations now rely on IT and big data for value creation, products and service improvement. This makes IT and data valuable to business organisations and the prime targets for cyberfraud perpetrators. In the quest to meet the bottom-line goals of profitability, customer satisfaction and expansion of the customer base, financial institutions continue to digitalise their operations through innovations and applications, which allow remote access to their products and services. The technological solutions promote the resilience of financial institutions during disruptions such as the global pandemic, which necessitated remote business operations. However, the solutions also pose significant threats to critical infrastructures of financial institutions as the threat actors often exploit the vulnerabilities of these digital systems to commit fraud from any location.

This book offers a comprehensive analysis of financial cybercrime and an integrative approach to mitigating it for the overall economic well-being of organisations, stakeholders and nations. This book provides a synthesis of different literature on the various types of cybercrime, the rate of perpetration and the cost implications, the approaches employed globally for its detection, as well as the efforts of some selected countries in curbing cyberfraud. Furthermore, this book presents different conceptual, empirical and analytical frameworks for cyberfraud mitigation. It also delves into

How to cite: David, OO 2024, 'Foreword', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. xxxi-xxxii. <https://doi.org/10.4102/aosis.2024.BK485.Of>

digitalisation, the broader role of antifraud technologies and the stakeholders: business organisations, regulators, customers, government, service providers, and governmental and non-governmental organisations (NGOs) in combatting cyberfraud and digital financial risk.

In summary, the book *Understanding and mitigating cyberfraud in Africa* provides an overview of cyberfraud and the statistical facts; critical conceptual, empirical, theoretical and methodological frameworks; digital forensic investigation and cybercrime legislations; and regulations and policy frameworks across the globe regarding African economies.

This book suggests practical and implementable solutions to mitigate cyberfraud. It also provides policy recommendations that enable the stakeholders to be proactive in their combat against cyberfraud. In addition, it offers valuable insight into the impact of cyberfraud and information security frameworks that can help reduce the system's vulnerability and intrusions. In this book, one of the takeaways is financial literacy for all levels, which will equip people and businesses on digital financial risk and cyberfraud mitigation. This book will be helpful for researchers, professionals and postgraduate students in understanding the phenomenon of digital financial risk and cyberfraud for sustainable and proactive measures against its occurrence in the world and Africa in particular.

Preface

This book examines the challenge of corporate fraud with an emphasis on cyberfraud. Globally, cyberfraud poses a severe threat to the world economy. In many countries, it has profound implications on the financial institutions and national economy because it lacks an appropriate framework to combat cyberfraud incidence. The deployment of digital technologies for business transactions and the dynamics of cyberspace contributed to the surge in crime. However, there are emerging technologies that have been proven to be effective and sustainable in the fight against cyberfraud. Therefore, this book aims to be helpful to students, practitioners and organisation management from various disciplines in understanding the phenomenon of cyberfraud and how to mitigate it.

This book comprises fifteen chapters. Chapters 1 and 2 present the general overview of fraud, global statistics and the experience of different African countries on cyberfraud incidences. Chapter 3 presents the theoretical perspectives of fraud to profile cyberfraud, while Chapters 4 and 5 deal with practical applications of decision-making relating to cyberfraud mitigation. These include using the fuzzy analytical hierarchy process (FAHP) and the machine learning approach. Data drive the world, and the role of big data technology in fraud mitigation cannot be overemphasised. Thus, Chapter 6 systematically reviews the trending big data technologies, tools and analytics employed in fraud mitigation. Chapter 7 considers the impact of information and communication technology (ICT) and forensic accounting (FA) on cyberfraud mitigation, while Chapter 8 presents a case study that details the effect of forensic accounting software on the accuracy of financial investigation. Chapter 9 details how FA can be effectively deployed for cyberfraud mitigation. The chapter presents a strength, weakness, opportunity and threat (SWOT) approach to investigate the feasibility of FA for fraud mitigation in financial institutions. Chapter 10 discussed the role of digital forensics in cyberfraud mitigation using a systematic literature review approach. Chapter 11 deploys a systems-thinking approach to address information and security challenges to mitigate internal and cyberfraud. Chapter 12 employs a bow tie technique to mitigate cyberfraud risks, while Chapter 13 presents a narrative of the cyberfraud experiences by some selected African countries and the efforts geared towards its mitigation. Chapter 14 employs secondary data to

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Preface', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. xxxiii-xxxiv. <https://doi.org/10.4102/aosis.2024.BK485.00>

analyse cybercrime activities in South Africa and the management control systems (MCSs) strategies the South African banking industry employs, respectively. The last chapter presents a practical guideline for mitigating cyberfraud and discusses policy lessons.

Cyberfraud and cybersecurity are continually evolving and transforming. The previous magnitude of cyber-attacks and inventions of threat actors necessitate developing robust mitigation plans. It is envisaged that the findings reported in this book will provide a practical, guided approach in the phases of developing and implementing innovative and sustainable solutions geared towards cyberfraud mitigation. The robustness of this book lies in the combination of a case study approach, empirical findings, systematic literature review and theoretical and conceptual concepts to provide practicable solutions to mitigate cyberfraud.

Cyberfraud: Global trends, statistics and the impact on economic well-being

■ Introduction

This chapter presents the global trends and statistics reflecting the cyberfraud rate and the strategies employed for cyberfraud mitigation, including their measure of success and effectiveness to ensure economic well-being in the current digital era. The reports reviewed indicate that the impact of cyberfraud is far-reaching, and the challenge poses a significant threat to the global economy. Furthermore, the adaptation to the coronavirus disease 2019 (COVID-19) pandemic was found to have contributed to the surge in both the advanced and emerging economies.

Cyberfraud is a critical challenge many banks and other financial institutions face. The threat actors usually leverage the dynamics of cyberspace to intrude into personal or organisational information for fraud perpetration. Walden (2007) indicated that cyberfraud is generally perpetrated when a threat actor secures an Internet connection to cyberspace to gain access to personal or organisational information and communication technology (ICT) systems or devices. Crime has become

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Cyberfraud: Global trends, statistics and the impact on economic well-being', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 1-18. <https://doi.org/10.4102/aosis.2024.BK485.01>

widespread because of the increase in the number of Internet users, the reliance of financial institutions on digital technologies for business processes and the volume of online transactions that are processed. The versatility of cyberspace makes it easy for the threat actors as the crime can be committed anywhere once an Internet connection is secured. Dalla and Geeta (2013, p. 997) stressed that cyberfraud is an illicit activity committed by taking undue advantage of exploring cyberspace or other ICT outfits. According to the PricewaterhouseCoopers (PwC) global report (2016), cyber breaches and other forms of security violation often expose sensitive or confidential data, which the threat actors can leak, copy, transmit, view, steal, alter or use without authorisation. Intruding into F-sensitive information may lead to unlawful data and system compromise, thus resulting in electronic fraud (Tiwari, Bhalla & Rawat 2016, p. 46). Cyberfraud is defined as illicit computer-enabled activities aided by the Internet either by individuals or corporate entities (Meephlam 2017, p. 17; Monni & Sultana 2016, p. 13). Okeshola and Adeta (2013, p. 98) stated that cyberfraud refers to fraudulent activities enabled via the use of computers, Internet and other information technology (IT) devices. Hence, the crime is both digital and virtual. The crime's digital and virtual nature often makes the threat actors' investigation and prosecution process more complex and time-consuming than conventional frauds (Clayton 2011, p. 271). Crime has become a significant challenge for financial institutions, their shareholders, the general public and law enforcement agencies globally. Kshetri (2019, p. 77) stated, 'The cases of cyberattacks on emerging economies are rising rapidly'. This is because unscrupulous activities can be perpetrated via cyberspace because of its unanimous nature (Uma & Padmavathi 2013, p. 392). Threat actors can exploit cyberspace and beat security measures to secure information without authorisation. This is evident in the global statistics for cases involving phishing and other forms of cyberfraud (Detica 2011, p. 1). According to Raghavan and Parthiban (2014, p. 176), the banking sector has witnessed numerous online fraud-related incidences such as phishing, malware attack, credit or debit card fraud, and cyber money laundering, to intrude into personal or organisational account to syphon money. According to Dzomira (2014, p. 17), Internet fraud can be categorised into two major classes, viz. direct fraud (money laundering, cash transfer, and credit or debit card fraud) and indirect fraud (malware, phishing and identity theft), as discussed in Chapter 2. The difference is that direct fraud involves direct access to personal or corporate accounts for fraud perpetration. In contrast, the latter involves acquiring information such as authentication passcodes to gain access to personal or corporate accounts for fraud perpetration.

■ Global trends

The increasing evolution of digital technology, which continues to revolutionise banking operations, has also increased the risks and insecurity of the system. Thus, there is a need to develop resilient cyber systems and banking operations that are resistant to disruptions or quick to recover from disruptions. The development of a resilient banking and cyber system is necessitated following the aftermath of global COVID-19 and the unrest in some countries, such as Russia and Ukraine, where banking operations were disrupted. These uncertain events have exposed the loopholes in the banking system and presented a gap in improving the banking system. In response to these challenges, many banks increased their visibility by growing online transactions. This has significantly increased the number of logins and payments done via the Internet (LexisNexis Risk Solution Report 2022). The global and accelerated digitalisation of banking operations fuelled by the pandemic and unrest in some parts of the world continues to revolutionise the banking sector (LexisNexis Risk Solution Report 2022). As a result, fraudsters also leverage the increasing use of the Internet for banking operations to perpetrate fraud. Fraudsters take undue advantage of unsecured or unmonitored networks to commit fraud as business is remotely transacted. AAG Report (2022a) indicated that the global cyber security landscape has witnessed increased risks and threats in recent years. For instance, in 2020, malware attacks increased by 358% compared to 2019. Thus, cyberattacks increased by 125% globally through 2021, and this surge continued in 2022 (AAG Report 2022a). The World Economy Forum Report (2022) indicated that the top three forms of cyberattacks of primary concern to business organisations globally include ransomware, social engineering and malicious insider activity.

The war between Russia and Ukraine also fuelled cyberattacks. About 3.6 million Russian Internet users experienced cyber breaches in the first quarter of 2022, which accounts for an 11% increase every quarter. Phishing is the most common online crime, as 323 972 Internet users reportedly fell victim to phishing attacks (AAG Report 2022a). Fraudsters leverage the unrest between Russia and Ukraine by building false stories around it to carry out social engineering, such as phishing emails to steal sensitive information from the victims.

Table 1.1 presents a comparative analysis of the period before, during and after COVID-19 to substantiate the effect of COVID-19 on the surge in cyberfraud.

TABLE 1.1: Comparative analysis of the period before, during and after COVID-19.

Indicators	Year				
	2001	2019	2020	2021	2022
Victim count (victims per hour)	6.00	53.00	90.00	97.00	-
Global average cost of data breach per hour (US\$)	2,054.00	-	-	787,671.00	-
Average cost of data breach to businesses (million US\$)	-	-	-	4.24	4.35

Source: AAG (2022b).

The PwC (2022a) Global Economic Crime Survey stated that on a global scale and across all organisations, cybercrime continues to pose the most significant challenge and threat, followed by customer fraud and asset misappropriation. The rate of cyberfraud is directly proportional to the increasing use of digital technologies for banking operations. As the use of digital technologies such as banking applications, e-commerce, online transactions and electronic business communication for transactions and business processes increases, the threats and risks of cyberfraud also increase (PwC Global Economic Crime Survey 2014).

LexisNexis Risk Solution (2022) reported that from July to December 2021, 35.5 billion transactions were processed, accounting for a 44% increase in global transactions. The global business environment continues to adapt to the changes that emanated from the COVID-19 pandemic by using various digital platforms, such as mobile or banking applications, for Internet-enabled transactions as opposed to the traditional face-to-face banking system. Banking application transactions have become dominant as a means by which customers carry out transactions globally to adapt to the global pandemic disruption. Dzomira (2014) indicated that cyberfraud is prevalent in the aspect of electronic transactions involving the use of mobile or smart devices.

The South African Banking Risk Information Centre (SABRIC) (2021) reported that in 2021, there was a 13% increase in the reported fraud incidences attributed to using different banking applications, accounting for an increase in the reported fraud cases to 12 095 compared to 10 667 in 2020.

According to LexisNexis Risk Solutions (2022), between July and December 2021, financial service transactions increased by 52%; communication, mobile and media transactions increased by 45%; and e-commerce transactions increased by 29%. For transactions via a channel during the same period, 75% of transactions occurred via mobile devices as opposed to 25% of transactions via desktop. The mobile apps also account for 79% of the transactions as opposed to 21% via the mobile browser.

The transactions on the new accounts increased by 4%, with a 9% increase in the reported attack rate. For logins, the transactions increased by 51% with a 0.5% attack rate, while transactions relating to payment increased by 35% with a 3.25 attack rate in the second half of 2021 (LexisNexis Risk Solutions 2022). Thus, this increased the mobile traffic in the digital identity network (DIN). Fraudsters also invent and deploy automated bot attacks and other human-initiated attacks in response to the adaptation resulting from the COVID-19 disruption. LexisNexis Risk Solutions (2022) reported that human-initiated attacks increased by 46%, while the automated bot attack volume increased by 32% in the second half of 2021.

PwC Global Economic Crime Survey Report (2016, p. 66) indicated that on a global scale, cyberfraud is the second most reported economic crime which affects organisations. The report indicated that close to half of the organisations surveyed opined that law enforcement is not adequately equipped to investigate and combat economic crime, leaving the onus on the organisations. The rate of cyberfraud incidences can be linked to technological advancement (Ali et al. 2017). In other words, the use of technology-enabled business processes for transactions such as ATMs, e-commerce, online purchases and electronic business communication has increased the risk of cyberfraud (PwC Global Economic Crime Survey 2014, p. 6). Hence, cyberfraud escalates more in a hyper-connected business ecosystem (PwC Global Report 2016). For instance, the global report of the PwC (2018) indicated that organisations that accept deposits and offer other forms of financial services are more susceptible to cyberfraud than those that are not. Böhme and Moore (2012, p. 10), Arachchilage and Love (2014, p. 310) and Wada and Odulaja (2012, p. 69) stated that the recent advances in technology have led to a significant reliance on the Internet and other IT-based infrastructure for transactions and banking operations which have also created an opportunity for crime perpetrations. The PwC (2018) report also ranked South Africa second among the top 15 countries, with a reported economic crime rate of 70%.

The KPMG (2019, p. 6) Global Banking Fraud Survey considered ten fraud typologies: merchant fraud, Internet fraud (cyberfraud), internal fraud, scams, identity theft, data theft, impersonation, financial statement fraud and mortgage application fraud. The report indicated that more than 50% of the participants were from the United States of America, Europe, the Middle East, Africa and Asia-Pacific and that their retrievals from losses because of cyberfraud were less than 25% of the total losses incurred. This means that significant revenue is still lost to cyberfraud. In 2018, UK Finance (2018) reported that the impact of cybercrime globally exceeded US\$450 billion a year. This encompasses forms of crime such as online fraud, blackmail and ransomware.

In 2022, UK Finance (2022) stated that financial fraud losses resulting from unauthorised payment cards, remote banking and cheques in the United Kingdom (UK) amounted to £730.4 million in 2021. This accounts for a 7% decrease compared to 2020. By implication, the banks and other financial institutions prevented £1.4 billion resulting from fraud in 2021 in the UK. In terms of Authorised Push Payment (APP) scams (scams occur via social engineering attacks involving impersonation whereby a person or business is deceived into sending money to a fraudster who poses as a genuine payee), UK Finance (2022) reported that there were 195,996 incidents with gross losses of £583.2m, compared with £420.7m in 2020 in the UK. As of November 2022, the UK is ranked 22nd on the National Cyber Security Index (NCSI), scoring 77.92 and second on the GCI. The country also ranked 5th on the ICT Development Index and 10th on the Network Readiness Index (NRI) (E-Governance Academy Report 2022). In 2021, 39% of the businesses in the UK also experienced one or more forms of cyberattack. Cybercrime reportedly cost small businesses in the UK an average of £4,200 in 2021, while a cyberattack for medium and large businesses was estimated at £19,400. The most common form of cyberattack suffered in the UK as of November 2022 was phishing, which accounts for 83% of the identified cyberattacks (AAG Report 2022a).

Over the years, Pakistan has witnessed increasing cases of cybercrime involving financial fraud. A total of 20,218 cyberfraud cases relating to financial fraud and 7,966 cases relating to hacking were reported in 2020. Fraudsters often employ social media such as Facebook, as financial frauds perpetrated via social media increased by 83% between 2018 and 2021 (AAG Report 2022a). In India, the number of reported cyber-related incidences was 208,456 in 2018. In the first two months of 2022, reported cyberfraud-related incidences increased to 212,485. In 2019, 394,499 cyberfraud-related incidences were reported, rising to 1,158,208 in 2020 and 1,402,809 in 2021. Prevalent among the cyberattacks perpetrated was hacking. In 2018, 17,560 websites were reported hacked, while a total of 43,681 websites were reported hacked in 2020 (AAG Report 2022a). Canada has also witnessed a surge in the rate of cybercrime over the years. Between 2017 and 2021, the number of reported cybercrime incidents rose from 27,829 cases in 2017 to 70,288 cases in 2021, accounting for a 153% increase. Canadian organisations reported that US\$1.5bn was lost to cybercrime in 2017 (AAG Report 2022a). In 2021, 85.7% of Canadian organisations were victims of at least one cyberattack (AAG Report 2022a).

■ Statistics on cyberfraud

Financial institutions employ the DIN as a means of sharing intelligence as it relates to fraud events. The DIN prevents high-risk fraudulent activities before the transaction is completed. It also aids in transaction monitoring by classifying transactions as high- and low-risk transactions. The primary activities of the cyberfraudsters have been categorised as information gathering through social engineering, account access, transfer or cash out. The PwC Global Report (2016) stated that the rate of cybercrime heightens in a hyper-connected business ecosystem.

Table 1.2 presents a comparative analysis of the volume of transactions vis-à-vis the human-initiated and bot attacks carried out across the continents for the second half of 2021.

Table 1.2 shows that Latin America recorded the highest percentage of transaction volume increases with the highest rate of human-initiated and bot attacks.

Table 1.3 presents the reported economic crime across various regions of the world. The table shows that Africa tops the list of the regions with the highest reported cases of economic crime in the world. This agrees with the report of Cassim (2016) that cybercrime is growing faster in Africa than in other continents. This results from the increasing number of Internet users in the continent (Cassim 2016). The author traced the growing rate of cybercrime to inadequately equipped law enforcement agencies in terms of infrastructure, lack of anti-fraud experts, lack of personnel and intelligence gathering, lack of modern IT infrastructure and lack of appropriate legal frameworks to curb cyberfraud at all levels (Cassim 2016).

PwC (2020) presented a detailed report on the rates of economic crime across some regions from 2016 to 2020 (PwC 2020). Figure 1.1 represents the summary of the report.

TABLE 1.2: Human-initiated and bot attacks carried out across the continents.

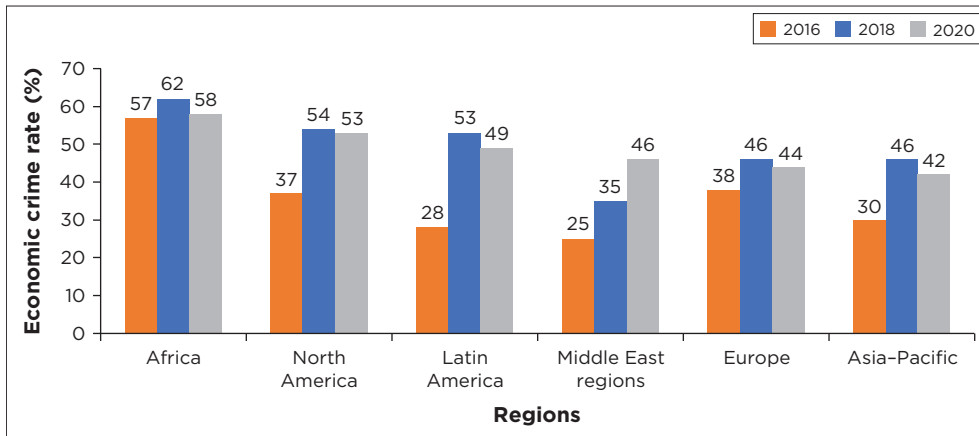
Region	Increase in volume of transactions (%)	Increase in human-initiated attack (%)	Increase or decrease in bot attacks (%)
North America	22	50	-7
Asia-Pacific	90	50	135
Europe, the Middle East and Africa	16	7	16
Latin America	473	138	455

Source: LexisNexis Risk Solutions (2022).

TABLE 1.3: Reported economic crime rates across various regions of the world.

Regions	2016 economic crime (%)	2018 economic crime (%)	2020 economic crime (%)
Africa	57	62	58
North America	37	54	53
Latin America	28	53	49
Middle East	25	35	46
Europe	38	46	44
Asia-Pacific	30	46	42

Source: PwC (2020).



Source: PwC (2020).

FIGURE 1.1: Reported economic crime rates across various regions of the world.

Table 1.4 presents the prevalent cyberattacks by region.

The PwC Global Report (2018) confirmed that organisations that offer financial services are more susceptible to cybercrime. The KPMG (2019) Global Banking Fraud Survey indicated that the retrieval of losses because of cyberfraud across the United States of America, Europe, the Middle East, Africa and Asia-Pacific were less than 25% of the total losses incurred. This means that significant money is lost to cyberfraud globally. Thus, the financial loss to cyberfraud damages the financial institutions and their shareholders.

The recent technological advancements, coupled with Internet-enabled devices, have increased the threat level of cyberfraud (Arachchilage & Love 2014; Böhme & Moore 2012; Wada & Odulaja 2012). Although emerging digital technologies and cyberspace have promoted the competitiveness, visibility and effective delivery of bank services, it is also an avenue for cyberfraud perpetration. Ali et al. (2017), as well as Malik and Islam (2019), shared a similar sentiment that the use of borderless cyberspace, digitisation, deployment of emerging IT solutions, and use of mobile and

TABLE 1.4: Most prevalent cyberattacks by region.

Regions	Most prevalent cyberattack (%)					Overall attack (%)
	Ransomware (%)	Network/server access (%)	Data theft (%)	Email compromise (%)	Misconfiguration (%)	
Middle East and Africa	-	18	-	-	14	14
North America	30	9	-	12	-	23
Latin America	29	-	-	21	-	13
Europe	26	12	10	-	-	24
Asia	11	20	10	-	-	26

Source: AAG (2022b).

smart devices have contributed significantly to the increasing rate of transformation in the business sector but with the risk of cyberfraud.

UK Finance (2018) stated that '[...] in recent times, the global impact of cybercrime was estimated to have exceeded \$450bn a year in the form of crime, extortion, blackmail and fraud online'. The effect of cyberfraud on financial institutions is detrimental to their reputation and goodwill, customers' satisfaction, public perception and profitability (Akinbowale, Klingelhöfer & Zerihun 2020, 2021, 2022,a 2023a). Fraudsters are increasingly becoming clever in social engineering activities, smishing, phishing, spam emails, phone calls, fake websites and impersonation to obtain information from victims for fraudulent operations. With people working from home in 2021 because of the prevalence of COVID-19, fraudsters targeted victims across different online banking platforms (Chigada & Madzinga 2021; Lallie et al. 2021; Li & Liu 2021).

To minimise the threats and trends of cyberfraud, Dzumira (2014) suggested implementing mitigating measures such as using forensic experts, implementing anti-fraud digital technologies and developing IT infrastructure with real-time monitoring and management capabilities, among others.

Synergy among financial institutions, regulators, fraud investigators, governments and the public is crucial to combat cyberfraud effectively. The public needs adequate sensitisation about cyberfraud trends, fraudsters' activities, and precautionary or countermeasures for its mitigation. The negligence or ignorance of the public is a weakness often exploited by the fraudster to perpetrate cyberfraud. For instance, in South Africa, the Symantec Report (2016) revealed that some people display their confidential information and lifestyle on social media, while others connect directly with unsecured networks, thus risking public exposure of their personal information.

Table 1.5 presents the countries with the highest and lowest cases of data breaches between the second and third quarters of 2022.

Table 1.6 presents the NCSI and the digital technology level (DTL) for the top 20 countries in the world and the top 20 countries in Africa as of November 2022. The NCSI is a global live index measuring countries' preparedness to mitigate cyber threats or manage cyber incidents. The table shows that the European countries dominate the rank regarding their NCSI and DTL, indicating their preparedness to mitigate cyber threats or manage cyber incidents. Morocco tops the list of African countries with high NCSI, followed by Egypt.

The KPMG Global Banking Fraud Survey (2019, p. 6) probed the internal and external fraud rate, and the value and fraud rate results are presented in Figure 1.3.

The survey also reports on the fraud risk assessment, which indicates that not all the respondents have a recorded fraud risk management operating model; therefore, an initiative-wide fraud risk assessment was conducted (Figure 1.4).

Alwan and Al-Zubi (2016, p. 101) stressed that the increasing cases of cyberfraud in Jordan can be traced to security and privacy issues because the Internet is a global social space prone to intrusion. Thus, the authors suggested that financial institutions implement security measures to protect customers' and organisations' information. Alagarsamy and Wilson (2013, p. 183) stated that innovative and technological solutions have

TABLE 1.5: Countries with the highest and lowest cases of data breaches between the second and third quarters of 2022.

	Country	No. of breached accounts
Highest cases	Russia	22,300,000
	China	14,157,775
	France	13,800,000
	Indonesia	13,200,000
	USA	8,400,000
	Spain	3,900,000
	Japan	1,246,373
	South Korea	1,669,124
Lowest cases	Sri Lanka	1,440,432
	Myanmar	17,887
	Iraq	16,113

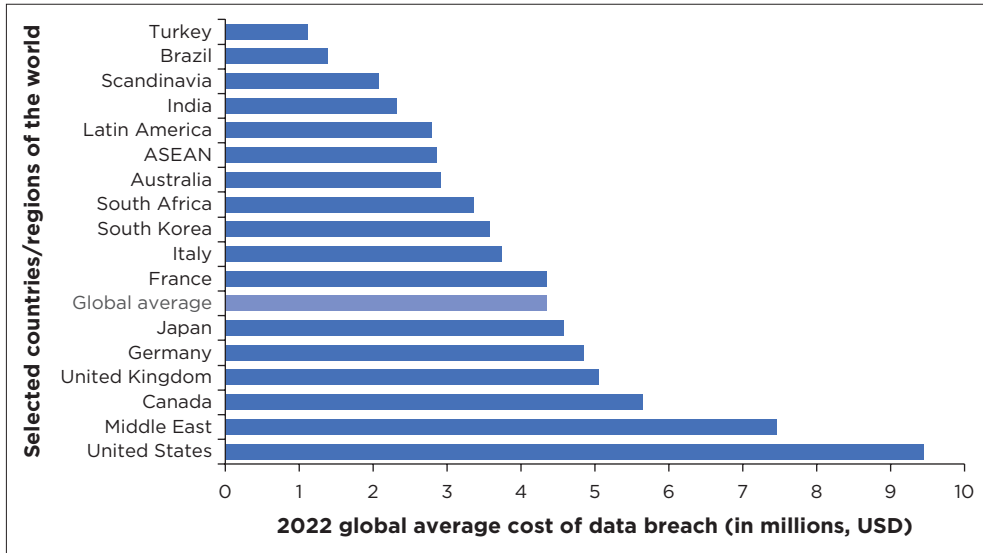
Source: AAG Report (2022a).

TABLE 1.6: NCSI and the digital technology level.

NCSI ranking	Country	NCSI	DTL	Difference
1.	Greece	96.10	64.47	31.63
2.	Lithuania	93.51	68.61	24.90
3.	Belgium	93.51	75.34	18.17
4.	Estonia	93.51	76.51	17.00
5.	Czech Republic	92.21	69.86	22.35
6.	Germany	90.91	81.43	9.48
7.	Romania	89.61	60.67	28.94
8.	Portugal	89.61	68.25	21.36
9.	Spain	88.31	73.92	14.39
10.	Poland	87.01	66.61	20.40
11.	Finland	85.71	79.64	6.07
12.	Saudi Arabia	84.42	63.46	20.96
13.	France	84.42	78.59	5.83
14.	Sweden	84.42	82.84	1.54
15.	Denmark	84.42	84.17	0.25
16.	Croatia	83.12	87.17	17.78
17.	Slovakia	83.12	66.53	16.59
18.	The Netherlands	83.12	83.48	-0.36
19.	Serbia	80.52	59.85	20.67
20.	Malaysia	79.22	62.53	16.69
	Africa			
29.	Morocco	70.13	46.88	23.25
55.	Egypt	57.14	46.93	10.21
56.	Zambia	55.84	29.66	26.18
59.	Benin	54.55	25.83	28.72
60.	Uganda	54.55	26.71	27.84
61.	Nigeria	54.55	31.76	22.79
64.	Tunisia	53.25	46.26	6.99
77.	Mauritius	44.16	53.57	-9.11
86.	Kenya	41.56	37.14	4.42
89.	South Africa	36.36	49.24	-12.88
92.	Rwanda	33.77	30.23	3.54
93.	Algeria	33.77	42.81	-9.04
95.	Ethiopia	32.47	20.70	11.77
96.	Cameroon	32.47	28.28	4.19
97.	Côte d'Ivoire	31.17	33.54	v2.37
98.	Ghana	31.17	40.68	-9.51
105.	Malawi	27.27	23.2	4.07
107.	Tanzania	24.68	26.96	-2.28
113.	Botswana	22.08	41.96	-19.88
116.	Chad	20.78	11.28	3.50

Source: E-Governance Academy Report (2022).

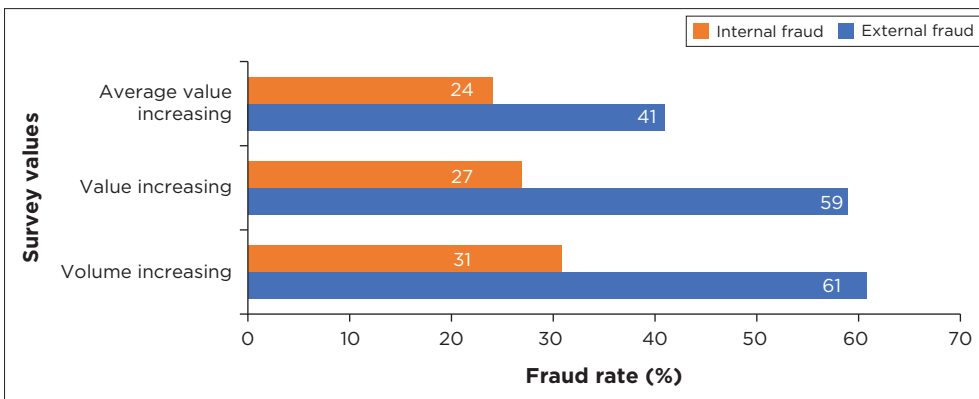
Key: NCSI, National Cyber Security Index; DTL, digital technology level.



Source: Statista (2022).

Key: USD, United States dollar (\$); ASEAN, Association of Southeast Asian Nations.

FIGURE 1.2: The global average cost of data breach in 2022 (in millions, USD).

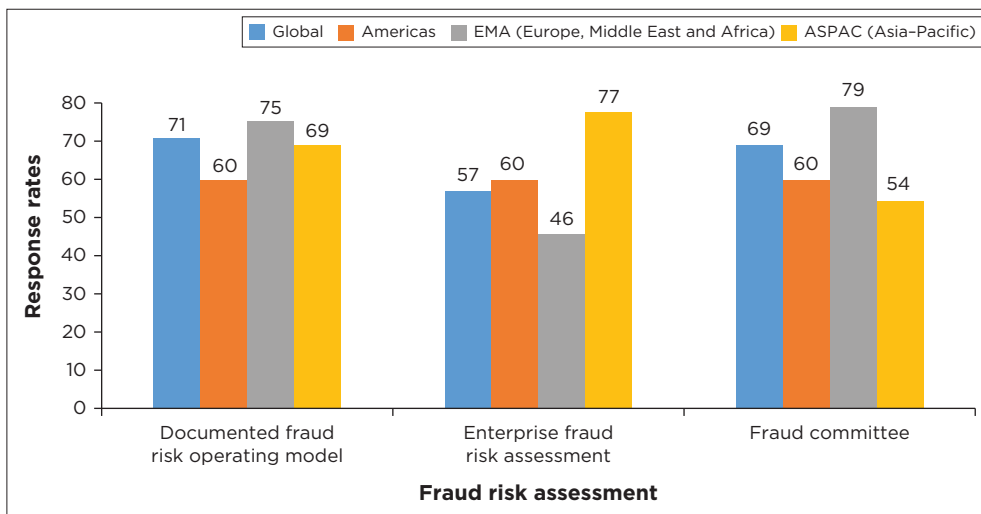


Source: KPMG Global Banking Fraud Survey (2019, p. 6).

FIGURE 1.3: Survey on the rate of internal and external fraud.

modified banking services to counter cyberfraud. Furthermore, Malik, Noreen and Awan (2017, p. 821) stated that the effect of cyberfraud has continued to impact the efficiency and integrity of banks in Pakistan negatively. The authors stated that, to a small extent, government policies have minimised the effect of cybercrimes.

Ali et al. (2017, p. 76) stated that in their study conducted to probe the effects of cyber threats on customers' behaviour who use online banking services, most respondents confirmed that a lack of proper



Source: KPMG Fraud Navigator (2019, p. 16).

FIGURE 1.4: Wide fraud risk assessment and response rate.

awareness promotes cyberfraud. A lack of awareness about the operation and activities of the fraudsters can cause cybercriminals to take undue advantage of customers to obtain confidential information for fraudulent activities. Furthermore, many customers who subscribe to online services also showed ignorance in the management of information security threats as well as the appropriate preventive measures to take when using e-banking services. This calls for financial institutions to improve customer sensitisation and information dissemination.

This finding agrees significantly with the conclusions of Malik and Islam (2019, p. 50) on the roles of awareness in information security and cyberfraud mitigation. Malik and Islam (2019, p. 50) posited that raising awareness levels is crucial to information security and the performance of financial institutions in Pakistan. The study's outcome shows that cyberfraud-related incidences negatively affect the goodwill, reputation and performance of financial institutions in Pakistan. However, with adequate sensitisation on security measures, the impact of cyberfraud can be substantially mitigated. Tariq (2018, p. 1) reported on cyberfraud incidences in financial institutions on five continents. The authors categorised the loss because of cyberfraud as direct and indirect losses. The direct losses because of theft and data breaches result in monetary loss, while the indirect losses are traceable to customer dissatisfaction and loss of the organisational reputation and goodwill. Tariq (2018, p. 1) recommended that financial organisations should be proactive in their combat against cyberfraud. Some recommended approaches include effective internal control, cybersecurity assessment, training and audits.

Balan et al. (2017, p. 65) also stressed the need for financial institutions to improve their internal control architecture, as developing effective internal control measures can counter fraud perpetration. Thus, one of the ways to achieve proactiveness in cyberfraud mitigation, as Balan et al. (2017) suggested, is to reinforce internal control measures. Arcuri, Brogi and Gandolfi (2017, p. 175) found significant negative market returns because of cyberattacks on the stock returns of some financial organisations.

Al-Suwaidi, Nobanee and Jabeen (2017, pp. 392–407) probed the reasons for cyberfraud perpetration in the reasons for cybercrime in ten countries, namely, Spain, India, the USA, the United Arab Emirates (UAE), Canada, Belgium, China, the Netherlands, Japan and Italy, between 2005 and 2017. They found no correlation between the unemployment factor and cybercrime perpetration in Italy, China, Belgium, the USA and the UAE. Instead, the rate of cyberfraud perpetration in these countries was traced to socio-economic values and sociocultural diversity. This implies that some cyberfraud perpetrators are not necessarily jobless but are influenced by the environment, pressure, greed and societal beliefs. In India, Kshetri (2015, p. 4) indicated that the cost of cyberfraud on the Indian economy was estimated at an average of US\$7.6bn a year. The author linked the high unemployment rate in India to vital social and economic indicators, such as low income, low education level, poor human development and social inequality. This implies that in some countries, unemployment cannot be totally exonerated from the possible causes of cyberfraud as it could easily influence other economic and social factors, leading to cyberfraud perpetration.

Kumudha and Rajan (2017, p. 1566) stated that the increasing rate of cyberfraud necessitates effective mitigation approaches, such as the deployment of digital technologies and the implementation of anti-fraud policies. However, Ivezic (2017) decried the slow implementation rate of such anti-fraud policy measures as one reason that promotes susceptibility to cybercrimes in many countries. Malik, Noreen and Awan (2018, p. 821) ranked the severity of the effect of cyberfraud perpetration on the efficiency of Pakistani banks. The authors found that cyberfraud has affected the efficiency of banks by 60%–80%.

UK Finance (2018, p. 6) traced the root cause of a cyberfraud attack on a Bangladesh bank to intrusions into its IT infrastructure, which allowed the threat actors perpetrators to gain unauthorised access to commit fraud. The anti-fraud squad significantly foiled the attack when the perpetrators attempted to transfer cash from Bangladesh to Sri Lanka and the Philippines via fraudulent transfers. Cyberattackers are becoming more advanced

through phishing, spamming, malicious attacks and hacking to access sensitive information and compromise the system (the KPMG Global Banking Survey Report 2019, p. 7). Table 1.7 presents some situations banks face that could perpetuate cyberfraud across the Americas, Europe, the Middle East, Africa and Asia-Pacific.

The evidence from the articles and reports reviewed indicates that cyberfraud remains a significant challenge in advanced and emerging economies. It affects an organisation's shareholders, profitability, efficiency and reputation. However, both emerging and advanced economies are deploying countermeasures to proactively and effectively mitigate the crime. Still, the fight against cyberfraud seems more effective and sustainable in advanced economies than the emerging ones. This is because emerging economies still face challenges, including implementing emerging technologies to mitigate cybercrimes, inadequate resources, inadequate enforcement of cybercrime laws and poor sensitisation.

There is a consensus from the studies and reports reviewed that cyberfraud is a global threat from IT and Internet-enabled devices. The crime is mainly targeted at financial institutions and is detrimental to their performance and stakeholders. The dynamic nature of crime and cyberspace makes it challenging for stakeholders to combat cybercrime effectively (Akinbowale et al. 2020). Existing studies recommend the following countermeasures: the use of a multidisciplinary strategy to disrupt the infrastructure of threat actors, sharing of uncompromised intelligence reports, cooperation among law enforcement agencies, fraud investigators and financial institutions, continuous improvement on cybersecurity, use of forensic accounting, big data technology, and effective development and allocation of resources most especially human resources (Akinbowale et al. 2020; Akinbowale, Klingelhöfer & Zerihun 2023a, 2023b; UK Finance 2018).

TABLE 1.7: Banking survey report on economic crime.

Americas	EMA (Europeans, Middle East and Africa)	Asia-Pacific
Cyber and data breaches	Cyber and data breaches	Cyber and data breaches
Faster payment	Faster payment	Social engineering
Open banking	Evolving digital channels	Faster payment
Evolving digital channels	Payment Services Directives 2 (PSD2) or open banking	Evolving digital channels
Virtual currencies	Social engineering	Open banking

Source: KPMG Banking Survey Report (2019, p. 7).

■ Impact on economic well-being

The advanced economies boast effective cybersecurity measures and response plans to mitigate cyberfraud compared to the emerging economies. However, there is a need for both advanced and emerging economies to step up their fight against cybercrime to minimise the effects on shareholders, the global economy, as well as organisations' reputations and profitability.

In the UK, a bank's fraud losses (majorly from telephone, Internet and mobile banking) in 2018 and 2019 were estimated at £152.9m and £150.7m from 31,797 and 43,906 incidents, respectively (UK Finance 2020). In Australia, Cross and Blackshaw (2015) indicated a low rate of Internet fraud reportage because of the fear of shame and stigma. In 2015, the Australian Cybercrime Online Reporting Network (ACORN 2015) reported that 39,491 cybercrime cases resulted in an estimated annual loss of AU\$1bn. Furthermore, the Australian Bureau of Statistics (2016) report indicated that 1.6 million Australians have fallen victim to personal fraud, while 126,300 are victims of identity theft. Broadhurst (2017) suggested that over 50% of the Australian population from fifteen years old and older have been exposed to at least one form of Internet fraud or the other, with 4% having revealed sensitive information (Broadhurst 2017). Between July 2021 and June 2022, the cyberattack rate in Australia increased by 81%. This accounts for losses of US\$72m through scams in 2022 (AAG Report 2022a).

In the first quarter of 2022 alone, Russia recorded 42.92 million cases of data breaches, while the number decreased to 28.78 million violations in the second quarter of 2022. However, data breach cases dropped to 22.3 million in the third quarter of 2022 (AAG Report 2022a).

Hence, it is evident that cybercrime via data breaches is a serious cyber threat in Russia. On average, more than 249,000 cases of digital fraud are reported annually, with a daily record of over 8 billion phishing emails traced to Russian addresses.

In the Middle East, Ali et al. (2017, p. 71) projected that the cost effects of cybercrime may increase over the next ten years and that financial institutions will be primarily affected. The summary of the cost of cybercrime as a function of the gross domestic product (GDP) for selected countries is presented in Table 1.8.

The Cyber Security Report (2020) indicated that 27% of organisations globally suffered from cyberattacks involving mobile devices, 18% because of banking operations, 18% because of information theft and 7% because of malware attacks. Table 1.9 presents the global cost of financial crime compliance.

TABLE 1.8: Cost of cybercrime as a function of the gross domestic product for selected countries.

Country	GDP (%)
Germany	1.6
The Netherlands	1.5
Norway	0.64
United States of America	0.64
China	0.63
EU	0.41
Singapore	0.41
Brazil	0.32
India	0.21
Ireland	0.2
Zambia	0.19
Malaysia	0.18
Canada	0.17
Mexico	0.17
Saudi Arabia	0.17
United Kingdom	0.16
Colombia	0.14
South Africa	0.14
Vietnam	0.13
France	0.11
United Arab Emirates	0.11
Russia	0.1
New Zealand	0.09
Australia	0.08
Nigeria	0.08
Turkey	0.07
Italy	0.04
Japan	0.02
Kenya	0.01

Source: Centre for Strategic and International Studies (2014).

Key: GDP, gross domestic product; EU, European Union.

TABLE 1.9: Global cost of financial crime compliance.

Continent	Cost (in billion US\$)
Europe	137
North America	32
Asia-Pacific	6
Latin America	5
South Africa	2

Source: LexisNexis Risk Solutions (2020).

■ Conclusion

This chapter aims to discuss the global trends and statistics of the rate of cyberfraud as well as the strategies employed for cyberfraud mitigation, including their measure of success and effectiveness. The articles reviewed indicate that the increasing evolution of digital technology, which continues to revolutionise banking operations, has also increased the risks and insecurity of the system. Thus, there is a need to develop resilient cyber systems and banking operations that are resistant to disruptions or quick to recover from disruptions. The reports reviewed also indicate that the impact of cyberfraud is far-reaching, and the challenge thereof poses a significant threat to the global economy. Furthermore, other disruptions, such as COVID-19 and its adaptation measures, contributed to the surge in cyberfraud in advanced and emerging economies. Although both emerging and advanced economies are deploying countermeasures to proactively and effectively mitigate crime, the fight against cyberfraud is still far from being won. Still, advanced economies boast effective cybersecurity measures and response plans to reduce cyberfraud, especially in comparison to emerging economies like Africa. This is because of technological advancement and the fast rate of adoption, as well as the implementation of digital technologies in advanced economies as compared to emerging ones. However, cyberfraud is still a significant threat to both advanced and emerging economies, and it continues to affect many organisations' shareholders, profitability, efficiency and reputations. Thus, there is a need for both advanced and emerging economies to step up their fight against cybercrime to reduce the effect on shareholders, the global economy and organisations' reputations and profitability.

Fraud investigation and mitigation

■ Introduction

This chapter presents an overview of fraud, with cyberfraud and its prevalent forms as a subset of general fraud. Typical forms of cyberfraud (such as phishing, data theft, hacking, malware, spamming, skimming, online theft, identity theft, spying, cyberstalking, pharming, vishing, spoofing, whaling and software supply chain attacks) were identified from the literature and explained. Out of these common forms of cyberfraud, existing reports indicate that phishing is the most prevalent. Some of the causes of cyberfraud identified by the existing literature are also highlighted in this chapter. These include customers' ignorance, organisations' weak controls and cyberspace dynamics. Practicable solutions to mitigate the occurrence of cyberfraud are presented in this chapter. The existing literature's findings indicate that cyberfraud's impact can be summarised into four major categories: shareholder dissatisfaction, loss of money and profitability, loss of reputation and goodwill and the effect on the global economy. Existing reports indicate that the impact of cyberfraud in these categories is detrimental, creating a need for implementing digital technologies for cyberfraud mitigation.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Fraud investigation and mitigation', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 19–46. <https://doi.org/10.4102/aosis.2024.BK485.02>

■ Overview of fraud

Lea and Bradbery (2020, n.p.) define fraud as a 'wrongful or criminal deception intended to result in financial or personal gain'. Concerning corporate fraud, the Association of Certified Fraud Examiners (ACFE) (2012a, 2012b) defines fraud as a deliberate misappropriation of an organisation's resources for personal gain. The American Institute of Certified Public Accountants (AICPA) (2002) indicates that fraud involves deception. The AICPA (2012) defines fraud as an intentional act by which an organisation or individual is deceived to exploit their resources for personal gains. Fraud involves deceit, breach of trust and justification for the act (rationalisation) (Hamilton & Justin 2012; Ramamoorti, Morrison & Koletar 2014). In a corporate setting, people can be deceived through false or inaccurately prepared financial statements or reports (Rezaee 2005). On a personal level, people can be deceived through impersonation, false claims and communications for financial or personal gains.

Idolor (2010) indicates that another component of fraud is concealment. This is the act of covering up the illicit fraud act committed. The perpetrator usually attempts to cover up the act to avoid penalty or sometimes to ensure that the same fraudulent trick can be used again. According to the Institute of Internal Auditors (IIA) (2009), fraud is an illicit act characterised by deceit, concealment or violation of trust. Sometimes, perpetrators might abuse the organisation's assets or privileges, resulting in fraud. Therefore, major components for easy comprehension of fraud involve deception, perpetration, abuse, trust violation, concealment and rationalisation (Figure 2.1). Dutta (2013) stated that fraud is not limited to the theft of money or exploitation of resources but also concealment (an attempt to cover it up). Bhasin (2016a) indicated that fraud is a global occurrence that impacts all continents.

Gbegi and Adebisi (2014) and Bhasin (2016a) stated that fraud is a serious global problem and affects virtually all sectors of the world's economy.

Fraud can be perpetrated internally, externally or by combining both approaches (Ezejiofor, Nwakoby & Okoye 2016). According to the Chartered Institute of Management Accountants (CIMA) (2008), internal fraud can be categorised into three major groups, namely, asset misappropriation (cash or non-cash forms), fraudulent statements (financial or nonfinancial statements) and corruption (conflict of interest or bribery). An internal employee may use familiarity with and access to the organisation's sensitive information to perpetrate fraud. Some may conspire with external fraudsters and supply them with sensitive information to commit fraud. Fraud may also be purely external.



FIGURE 2.1: The major components of fraud.

Regarding fraud perpetrators, Bhasin (2016) indicated that an individual can commit fraud, as well as a group of people or corporately, to acquire illicit assets such as money, property or services for personal gains and use. Fraud may also come about as a result of the evasion of certain payments by individuals or organisations. At a corporate level, fraud can be perpetrated internally by the organisation's employees or externally by people the organisation does not employ. It can also result from the collusion of an internal employee with external perpetrators. To perpetrate fraud, an internal employee can take undue advantage of understanding an organisation's assets, control systems and financial management policies. Such employees may also divulge some of the organisation's sensitive information to external perpetrators to commit fraud. Cyberfraud is one form of fraud and is perpetrated when cyber criminals take undue advantage of cyberspace and digital technologies or online banking platforms to commit fraud. Online fraud can include phishing, malware, hacking, data theft, spam email, online theft, skimming or spying (Akinbowale, Klingelhöfer & Zerihun 2020). This book's primary focus is to unravel the causes and rationale behind cyberfraud perpetration, the dynamics of cyberfraud and the activities of cyber criminals and to provide insights into sustainable and practical measures to mitigate it.

The report of the ACFE (2012) stated that the fraud profile of an organisation can be grouped into three types. These are asset misappropriation, corruption and financial statement fraud. In other words, engaging an organisation's resources for personal use without authorisation is known as asset misappropriation (ACFE 2012). Skalak, Alas and Sellito (2011, p. 5) believed that fraud can be classified into two major categories: asset misappropriation and financial statement fraud. Venegas (2012) stated that an organisation's fraud scheme could stem from doctored bills, corruption, asset misappropriation (cash and non-cash), false expense reimbursements and payroll doctoring or cheque alteration.

Kenyon and Tilton (2011, p. 232) categorised fraud into four types, namely, asset misappropriation, financial statement fraud, fraudulent acquisition of revenues and assets, and expenditures and liabilities for personal purposes. However, in the work of Skalak et al. (2011, p. 5), fraudulent acquisition of revenues and assets, as well as expenditures and liabilities for personal gains, has been categorised under the broad category of asset misappropriation. Asset misappropriation occurs when an employee steals or misuses an organisation's resources. The abuse of an organisation's assets could be in the form of cash theft, false billing or inflated expenses. Asset misappropriation encompasses fraudulent activities such as cash theft, credit fraud, inventory theft, revenue skimming, payroll fraud, fraudulent disbursement, expense reimbursement fraud, cheque tampering, cash register disbursement fraud and fund embezzlement. Thus, asset misappropriation is the most common type of fraud in any organisation (Kenyon & Tilton 2011, p. 232; Skalak et al. 2011, p. 5).

Conversely, corruption involves illegal acts intended to give the perpetrator an advantage. Corruption may include kickbacks or bribery, extortion, collusion and conflict of interest. It is a general term that encompasses the wrongful use of influence for personal gains or on others (ACFE 2012). According to Venegas (2012), corrupt schemes involve infringement on the principles of transparent transactions, contracts or procurement by exerting undue influence either for direct or indirect personal gains (Venegas 2012).

Financial statement fraud is fraud committed by the organisation's management or employees against the potential users of financial statements. Thus, it deliberately misleads people about the organisation's financial status (ACFE 2012). Venegas (2012) indicated that an organisation's employee can purposefully omit some facts about the financial position of an organisation or present a fabricated statement. This may be in the form of false revenues and incomplete, inflated, doctored or duplicated bills or financial reports. Financial statement fraud encompasses deliberate

activities such as deliberate omission, incorrect statements or false presentation in financial reporting, deliberate forgery, alteration or modification of records used to prepare financial statements. All these schemes aim to deceive financial statement users (Franceschetti 2017). Perpetrators of this category of fraud deliberately misapply accounting principles to manipulate results for personal gains. Financial statement fraud includes fraudulent misrepresentation, falsification of financial or accounting records, fictional sales recording, misrepresentation of transactions, false inventory valuation, deliberate infringement on accounting principles, false classification and false debt disclosure (Kenyon & Tilton 2011, p. 232).

Kenyon and Tilton (2011, p. 232) explained that financial statement fraud could be inclusive or exclusive. The inclusive form of financial statement fraud involves false entries into an organisation's record books. In contrast, the exclusive form of financial statement fraud involves omitting entries needed for presentation. Existing studies have indicated that financial statement fraud usually has a more significant impact on the organisation and the shareholders than asset misappropriation (Kenyon & Tilton 2011, p. 232; Skalak et al. 2011, p. 5). However, the rate at which employees perpetrate other categories of fraud, particularly asset misappropriation, is alarming (ACFE 2020). The Association of Certified Fraud Examiners (2020) reports that asset misappropriation accounts for 86% of all reported fraud incidences in 2020.

Asset misappropriation is a prevalent form of occupational fraud involving theft or misuse of the organisation's resources. It can be cash theft, fraudulent billing, doctored inventory or inflated expenditure reports. Often, the perpetrators trick or deceive others to misappropriate the organisation's assets. Asset misappropriation usually involves theft, concealment and conversion (Agarwal 2022). The Association of Certified Fraud Examiners (2012) indicates that fraud comprises three main elements: deception, benefit and abuse. Fraudulent activities are mainly based on an intentional deception committed for personal gain through misconduct or unethical means.

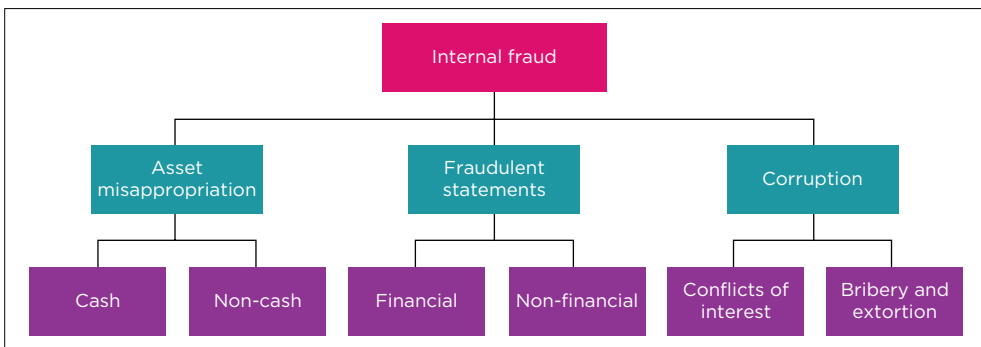
Golden, Skalak and Clayton (2006, p. 3) believe that fraud can be classified into four essential elements: false representation, disregard for the truth, reception of the false representation and the damages because of the financial consequences of other elements highlighted. Golden et al. (2006, p. 3) argued that for fraud to occur, there must be a false representation and the reception of the false representation by the victim with the resulting consequences. Asset misappropriation is a prevalent type of fraud, as perpetrators usually find it easy to commit. However, it does not always result in significant direct losses compared

to other kinds of fraud. The Association of Certified Fraud Examiners (2012) further grouped asset misappropriation schemes into categories. These are cash misappropriation and other forms of misappropriation, including inventory or other assets.

Figure 2.2 depicts the types of internal fraud and the internal structure of an organisation regarding fraud control, respectively.

Ezejiolor et al. (2016, p. 16) further attempted to classify fraud perpetration into three categories. These are internal fraud, external fraud and mixed fraud. Internal frauds are regarded as frauds committed by the organisation’s employees. This includes the management and employees. On the contrary, external fraud is committed by threat actors who are not connected to the organisation (external party). Mixed fraud, however, involves the collusion of an insider (internal threat actor who could be part of the management or an employee) with an outsider (external party) to perpetrate fraud (Ezejiolor et al. 2016, p. 6). The OECD (2007, p. 31) report categorised threat actors (fraudsters) into five subcategories. These are innovators, amateurs, insiders, copycats and criminals. The *innovators* are the threat actors who look for security lapses in an organisation to commit fraud, while the *amateurs* engage their computer skills to commit fraud, as in the case of cyberfraudsters. The *insiders* are organisational employees who commit fraud or disclose relevant information or external parties for fraud perpetration, while the *copycats* are concerned with recreating flexible tasks. The *criminals* are the actual threat actors who are highly organised in using any of the subcategories mentioned for fraud perpetration.

Detecting fraud cases is sometimes challenging because of fraud complexity and the dynamic techniques the threat actors employ daily. Fraud characteristics of conspiracy, deception and concealment sometimes



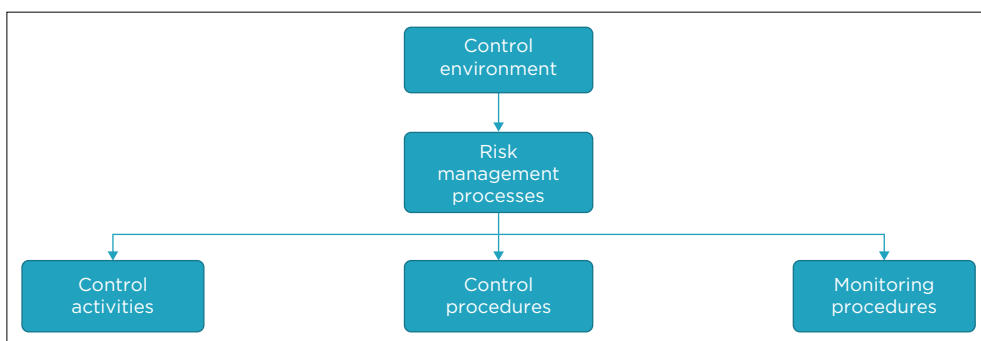
Source: CIMA (2008, p. 8).

FIGURE 2.2: Types of internal fraud.

make fraud detection challenging (Enofe et al. 2017, p. 40). Mac (2015) identifies some steps necessary for fraud mitigation. These include regulatory compliance, sound ethical culture, development of fraud risk management procedures and policies, training and other forms of human capacity development through training. Venegas (2012) presents a framework for internal fraud control (Figure 2.3). The framework comprises risk management and control processes. The general control environment includes the risk management processes, which can be broken down further into control activities, control procedures and monitoring procedures. The control system comprises the organisation's structure, ethical culture, management style and policies related to human resources, and communication. Management risk processes are undertaken to prevent fraud occurrence or to mitigate the effect of fraud occurrences. On the other hand, control activities aim to prevent or detect potential red flags of fraud, fraudulent cases and their associated risks. Examples of control activities include approvals, verifications, reconciliations and monitoring.

■ Cyberfraud and its prevalent forms

A subset of general fraud is bank fraud. Bank fraud is an unlawful act that happens whenever a person uses an illegal way to withdraw money or gain other forms of assets from a bank or other financial institutions (Wekesa et al. 2016, p. 376). As one of the primary motivations for fraud perpetrators is the quest for monetary gain, banking institutions become more susceptible to attack because they accept deposits (Sanusi et al. 2015). Banking institutions are increasingly prone to fraud risks; although various control measures have been implemented over the years to mitigate such risks, the schemes of perpetrators in circumventing existing control measures often jeopardise the efforts aimed at fraud prevention



Source: Venegas (2012).

FIGURE 2.3: An approach to internal fraud control.

(Sanusi et al. 2015, p. 107). The high rate of fraud, theft, embezzlement and manipulations in the banking sector can jeopardise banks' economic growth and stability (Ijeoma & Aronu 2013, p. 269). One of the significant fraud risks that constitute a threat to the bank and other financial institutions is cyberfraud.

Emerging technologies and the evolution of cyberspace for banking operations and other financial transactions have increased the vulnerability of financial institutions to cyberfraud. The PricewaterhouseCoopers (PwC) Global Fintech Report (2016) indicates increased cybersecurity threats because of security breaches, resulting in losses in the banking sector. One of the major causes of the increasing risk of cybersecurity has been traced to the advent of ICT and other digital technologies employed by the banking industries (Ali et al. 2017). While ICT and other emerging technologies have contributed to the increase and robustness of banking operations, the technologies have also increased the cyberfraud risk score. Cyberspace is vast and dynamic, thus paving the way for many unethical practices that can engineer cyberfraud (Uma & Padmavathi 2013, p. 392). The misuse of cyberspace by cybercriminals often results in cyberfraud.

Cyberfraud encompasses digital and organised crime in which the perpetrator employs computers, Internet connectivity and other IT-enabled devices to illegally obtain money or sensitive information from victims (Dalla & Geeta 2013; Okeshola & Adeta 2013; Walden 2007). It involves a range of crimes, such as unauthorised intrusion into computer systems, customers' data or organisation's information (KPMG 2011). Rodgers (2006) explains that it encompasses activities relating to unauthorised access to personal or organisational computers to commit fraud. The fraudulent act can range from illegally acquiring confidential information or data to destroying the information stored on a computer to syphon money. Akinbowale et al. (2020) further explain that cyberfraud is a significant problem financial institutions face. Organisations continue to commit resources to strengthening their cybersecurity against cyber threats.

Hunton (2009, n.p.) defines cyberfraud as a 'crime committed via the use of electronic media involving the cyberspace'. In other words, cyberfraud involves cyber breaches and data and information breaches. According to the PwC Global Report (2016), a cybersecurity breach is a security violation involving using cyberspace to view, steal, copy or transmit data by an individual not authorised to do so. It also involves other activities such as unauthorised data disclosure, leakage and theft. Tiwari, Bhalla and Rawat (2016) believed that cyberfraud is a criminal act involving ICT infrastructure to intrude into personal or corporate confidential information

for theft. It may also include interference with other personal or corporate data, networks and systems, data corruption and other forms of electronic fraud. Cyberfraud is usually enabled by the Internet and the perpetrators' actions (Meephlam 2017; Monni & Sultana 2016). Fraud involving cyber breaches can be classified into direct and indirect fraud (Dzomira 2014). Direct fraud involves unauthorised cash-outs or transfers from a personal or organisational account. In contrast, indirect fraud involves the tricks used by fraudsters to solicit or acquire confidential information to perpetrate fraud. This may include identity theft, malware and phishing. In some situations, fraudsters use fake identities to trick unsuspecting victims with modern technology (Jegade 2014).

Raghavan and Parthiban (2014) state that several cyberfraud-related cases have been witnessed in financial institutions. These include malware, spam email, credit card fraud, automated teller machine (ATM) fraud, phishing and cyberfraud activities, including unauthorised intrusion or acquisition of personal or organisational information, malware attacks, intellectual property, theft, online fraud, spying, denial-of-service or disabling of networks, fake links, impersonation, pharming, data and cash theft, spamming, skimming, phishing, credit or debit card fraud, hacking, bank verification number (BVN) scams, money laundering and pharming (Akinbowale, Klingelhöfer & Zerihun 2021; Ali et al. 2017; Detica 2011; Dzomira 2014; Mugari et al. 2016; Njeru & Gaitho 2019; Omodunbi et al. 2016; Rao 2019; UK Finance 2020). Table 2.1 highlights the outcome of some existing studies on the forms of cybercrimes prevalent in financial institutions.

■ Phishing

Phishing is a form of social engineering in which the fraudster deceives a victim through false claims or messages to steal the personal information or the identity of the victim. Fraudsters can disguise themselves as a representative of an authorised business or financial institution to deceive unsuspecting victims for fraudulent purposes (AICPA 2017; Chaudhary 2014; KPMG 2012; Mugari et al. 2016; Omodunbi et al. 2018).

■ Data theft

This is the theft of sensitive information stored on personal or organisational computers, databases, servers or other electronic devices to acquire confidential information and compromise privacy. Fraudsters can use various means to obtain data from unencrypted credit cards, source codes, customers' information and organisation records (AICPA 2017; Hedayati 2012).

TABLE 2.1: Forms of cybercrimes in financial institutions.

Reference	Contribution	Identified forms of cybercrime
Omodunbi et al. (2016)	Investigation of cybercrime occurrences	Hacking, BVN theft, phishing, malware, data theft and spamming
UK Finance (2020)	Summary of fraud in the payment industry	Internet fraud, phishing, ID theft, card theft and data theft
Ali et al. (2017)	Effect of cyber threats on customers' behaviour in online banking services	Malware, vishing, phishing, hacking, malware, Internet fraud and denial-of-service attacks
Mugari et al. (2016)	Investigation of the nature of prevalent cybercrime in financial institutions in Zimbabwe	Phishing, hacking, spamming and malware
<i>BusinessGhana</i> (2018)	Cyber security directives for Ghana's financial institutions	Malware, e-spam mail, phishing, hacking and credit card theft
AICPA (2017)	Cybercrime cost in the USA	Malware, phishing, hacking and data theft
Symantec Report (2016)	Cybercrime and cyber security trends in Africa	Phishing, malware, credit card theft, data theft, hacking and spamming
Njeru and Gaitho (2019)	Effect of cybercrime on the performance of commercial banks in Kenya	Phishing, hacking and credit card theft
Detica Limited (2011)	Cybercrime cost in the UK	Phishing, malware, hacking, spying and online fraud
Symantec Report (2016)	Cybercrime evaluation	Phishing, online fraud and crypto extortion
Tiwari et al. (2016)	Investigation of cybercrime and security	Phishing, malware, identity theft, denial-of-service attacks, cyberstalking and online fraud
Balan et al. (2017)	Data analysis of cybercrime	Phishing, hacking, online fraud and malware
Dzomira (2014)	Cyberfraud risk assessment	Internet theft, spamming, malware, phishing, hacking, pharming and credit card fraud
Rao (2019)	Assessment of cybercrime in financial institutions in India	Phishing, vishing, hacking, spamming and skimming
McGuire and Dowling (2013).	Review of cybercrime	Malware, online theft, phishing, hacking, spamming and fake SMS
Rezk et al. (2017)	Assessment of the impact of cybercrime on e-commerce	Phishing, SIM-box fraud, cyber terrorism, spamming, spoofing and credit card fraud
Bamrara, Singh and Bhatt (2013)	Cyberattacks and defence approaches in India	Hacking, spoofing, malware, online theft and credit card fraud
Broadhurst et al. (2014)	Organisations and cybercrime	Phishing, malware, hacking, spamming, data theft, domain squatting and Internet theft
Okutan and Çebi (2019)	Framework development for cybercrime investigation	Phishing, online theft, hacking, online theft, malware, spamming, data theft, cyber threat, cyberstalking and credit card fraud
Ajayi (2016)	Challenges of cybercrimes laws and policy	Credit card fraud, online theft, malware, data theft, hacking, phishing, spamming and cyber threat
UN (2013)	Investigation of cybercrime	Credit card fraud, phishing, malware, cyberstalking, hacking, online theft, whaling, spamming, data theft and cyber threat
Ch et al. (2020)	Cybercrime classification using machine learning	Credit card fraud, cyber threat phishing, spamming, spoofing, data theft, piracy, hacking and online theft

Source: Akinbowale et al. (2021, p. 4).

Key: BVN, bank verification number; ID, identity; AICPA, American Institute of Certified Public Accountants; USA, United States of America; UK, United Kingdom; SMS, short message service; SIM, subscriber identity module; UN, United Nations.

■ Hacking

Hacking refers to fraudulent activities that seek to compromise digital devices, such as personal or corporate systems or networks. Fraudsters achieve this by identifying and exploiting the weaknesses in a system or network to gain access to personal or corporate data or systems. For instance, the weakness could be a weak password that could easily be guessed or 'cracked' using a password-cracking algorithm to gain access to a computer system. The fraudster may then gain access to the system and hijack the system's control from the authorised owner to acquire sensitive information or illegally transfer money (Kumudha & Rajan 2018; Mugari et al. 2016).

■ Malware

Malware refers to viruses, files or codes delivered over a system or network to infect, explore and steal sensitive information. It involves the unauthorised use of malicious software to alter the network or security settings of a personal or corporate system for data collection. The malicious software is purposely designed to interfere with the normal functioning of systems to gain access to sensitive information. An example of malicious software is the botnet that fraudsters usually use to launch denial-of-service attacks.

Sometimes, fraudsters may secretly install illegal programs over the network used by individuals or organisations to steal confidential information. Such malicious software enables perpetrators to gain unlawful access to the organisation's data storage systems to acquire information for fraudulent activities (UN 2013; Uppal, Mehra & Verma 2014). An example of malware is a ransomware attack. Ransomware is a cyberattack involving software that prevents an organisation from accessing its data until a ransom is paid. Examples include the introduction of Trojan viruses into an organisation's database to copy the contents of a folder into a separate password-protected file. The original file will then be deleted, and the copied file will only be released to the authorised owner when the ransom is paid. Some threat actors can encrypt an organisation's entire data infrastructure and provide the encryption key once the ransom is paid (AAG 2022a).

■ Spamming

This involves using unsolicited spam electronic mail to trap innocent victims into divulging confidential information that threat actors can use to commit fraud (Rao 2019; UN 2013). It could be bulk messages sent via electronic mail, instant or text messaging or other digital communication tools.

■ Skimming

This illegal activity involves the secret installation of devices such as cameras, skimmers or keypad overlays that are not detectable to the victims on digital machines such as ATMs and point-of-sale (POS) terminals. The aim is to secretly record sensitive information, such as the victim's account or debit or credit card details, allowing the fraudsters to encode the acquired data onto a blank card to syphon money from the victim's account (Omodunbi et al. 2016).

■ Online theft

This usually occurs through cash transfers or credit/debit card theft. The threat actors can use the Internet to intrude into a personal or organisational account to make cash transfers once the information relating to the user or such account is illegally obtained (Omodunbi et al. 2016). For online credit or debit card fraud or theft, the fraudster decodes the victim's confidential codes and login credentials to commit fraud (Sonepat & Sonepat 2014, p. 45; Tan Harry 2002).

■ Identity theft

Identity theft occurs when a fraudster steals and illegally uses others' personal or corporate identifying information such as name, address, identity number, banking account number, username or password to perpetrate fraud.

■ Spying

Spying, otherwise known as cyber espionage, refers to using codes to gain access to an organisation's network webpages to acquire confidential information to commit fraud without knowing the rightful owner of such network or web account. Software programs such as spyware are usually employed by perpetrators to secretly capture information or communications within or among systems, networks or websites for fraud perpetration (Dzomira 2014).

■ Cyberstalking

Cyberstalking is a broad term for a series of unlawful activities, including threats, libel, defamation and sexual harassment aimed at intimidating the target to syphon money. It involves using ICT-enabled devices to commit unlawful activities such as threats, attacks, harassment or verbal abuse of an individual (UN 2019).

■ Pharming

Pharming involves the generation of a fake, duplicate website to deceive users into inputting their confidential information, such as passwords or login credentials (UN 2019). Fraudsters may use malicious code executed on the device to redirect a victim from the legal and authorised website to an attacker-controlled website.

■ Vishing

Vishing employs social engineering infrastructure or devices such as telecommunications or smartphones to gain unlawful access to personal or organisational information aimed at fraud perpetration (Rao 2019). Fraudsters may use mobile phones or other smart and Internet-enabled devices to steal personal or organisational confidential information.

■ Spoofing

Spoofing involves unscrupulous activities such as deceptive calls to solicit information to syphon money (Ch 2020). Fraudsters may launch a fake internet protocol (IP) address to disguise or hide locations to perpetrate fraud.

■ Whaling

A whaling attack is a method cybercriminals use to disguise themselves as an organisation's top management, aiming to steal money or sensitive information or gain access to their computer systems for fraud. Fraudsters may impersonate an organisation's high-level management or authority to deceive customers or employees (UN 2019).

■ Software supply chain attack

This is a threat that targets an organisation's software developers or suppliers to access secret codes for fraud (UN 2019).

■ Motivation for cyberfraud perpetration

Herselman and Warren (2004, p. 253) opine that cyberfraud perpetration can be internally or externally motivated. Van Niekerk (2017, p. 116) traces the motivation for cybercrime perpetration by the threat actors to the following: political and ideological reasons, vulnerability of an organisation's misconfigured systems, financial gain, opportunity, weak internal controls, greed and personal interests. However, Broadhurst et al. (2014, p. 3) explain

that the motivations for cyberfraud perpetration are diverse and vary based on the individual culprit. These may include financial pressure, financial gain, personal ideology and a desire to challenge powerful interests, sociocultural forces, obsession, compulsive attitude (lifestyle or habit) and greed.

Van Niekerk (2017, p. 116) states that some perpetrators commit cyberfraud to prove their skills. However, the author does not rule out the possibility of other ulterior motives of the perpetrators. Broadhurst and Grabosky (2005, p. 7), as well as Broadhurst et al. (2014, p. 7:20), further identify other motivating factors as follows: impunity, negative influence, retaliation by disgruntled elements, desire to demonstrate technical abilities, security vulnerability, competition for social status, financial motives and pressure. The authors admitted that other motivating factors may be involved to a certain extent, subject to the nature of the cybercrime being committed.

■ Major loopholes for cyberfraud perpetration

The major loopholes the perpetrators exploit can be classified into three categories: customers, organisations and cyberspace.

■ Customers

Balan et al. (2017) state that customers are vulnerable to cyberfraud attacks because they represent significant financial institution shareholders. Factors such as inadequate information, low awareness level, a shortage of online monitoring systems and inadequate real-time responses can increase the risk score and customers' vulnerability to cyberfraud. Sometimes, customers might be ignorant of security strategies because of a lack of awareness, and fraudsters can leverage this to commit fraud (Modugu & Anyaduba 2013). Sometimes, customers' negligence in taking proactive measures ahead of the fraudster or protecting their confidential information might make them vulnerable to cyberfraud attacks.

Customers' negligence to the activities of the cyberfraudsters, among others, may include the use of weak passwords (such as the year of birth); exposure of privacy, data and confidential information on the Internet or in public places; use of outdated security software on Internet-enabled devices; response to spam emails, fake links, unverified messages and calls; and failure to contact the financial institution for help in any event of cyberattack or loss of credit or debit cards or smart devices.

The following actions may reduce the vulnerability of customers to cyberfraud:

- Customers should ensure that all passwords used for banking operations are strong so they cannot be easily guessed and that they are kept secret and regularly updated.
- Customers should refrain from divulging sensitive information such as account details, passwords and credit or debit card details to third parties.
- The financial institutions must verify the source and authenticity of all information relating to banking activities before taking any action.
- Use safe platforms for Internet transactions and ensure that the information provided is not automatically saved on web applications.
- Read and understand the procedures of Internet banking and the safety tips financial institutions provide.
- Ensure the encryption of data and security of personal systems or databases.
- Avoid the use of publicly available networks for online banking or transactions.
- Protect the systems, mobile phones or other Internet-enabled devices used for online banking and transactions from viruses and malicious software.
- Report any suspicion, cyberattacks or loss of confidential information or devices to the designated centres swiftly.

■ Organisation

Financial institutions also partly contribute to the surge in the rate of cyberfraud. Bhasin (2012, p. 53) observes that financial institutions with weak internal or management controls are more vulnerable to fraud. Besides, financial institutions with a lack of good ethical practices or implementation of ethical practices may also be susceptible to cyberfraud-related incidences. Furthermore, lack of accountability, poor organisational controls and lack of suitable risk management plans and blueprints for cyberfraud mitigation in financial institutions are also contributing factors to the prevalence of cyberfraud. In addition, how the emerging technologies are deployed can also determine the rate of cyber-related incidents. One of the significant causes of cyberfraud is the advancement of digital technologies (Dzomira 2014). Financial institutions have leveraged the advancement in digital technologies to extend the scope of business transactions through mobile and online banking platforms for transactions. This has also increased their vulnerability to cyberfraud.

Broadhurst and Grabosky (2005) and Ali et al. (2017) explain that the emerging developments in IT are some of the architects of modern society that have brought about rapid transformation in data management. The business world is not left behind, with a high rates of business investment, expansion of networks and services, and fast and robust service delivery (Ali et al. 2017; Huang 2005; Ramaswamy 2005). For instance, online banking systems have made transactions seamless without needing physical interaction between the banking personnel and the customers. However, as society becomes increasingly driven by data technology, the associated risk concerns should also be addressed. Financial institutions are responding to these technological changes at different levels. Some of the challenges faced by the financial institutions that have hindered the pace of tackling cyberfraud include the level of technical know-how and lack of expertise in cyberfraud investigation and mitigation, lack of synergy between fraud investigators, lack of information and awareness about the dynamics of cyberfraud and the technologies needed to combat it, lack of strict cyber legislation, inadequate resources, lack of suitable cyberfraud detection and mitigation technologies, as well as a lack of robust internal and management controls.

PwC (2016, n.p.) states that, in some banks, 'security measures are not taken with priorities'. Furthermore, the organisation's resource commitment to protecting information and detecting cyberfraud is meagre (PwC 2016). Hence, such organisations may become more vulnerable to cybercriminals. Furthermore, some financial institutions are yet to fully deploy emerging technologies to combat cyberfraud, while some are not kept abreast of the dynamics of cyberspace and the activities of cyber fraudsters. Some are guilty of relying on old security measures without regularly updating security apparatus and software. Some are also not adequately investing in human capacity development for fraud mitigation.

Ajayi (2016, p. 10) indicates that an organisation's personnel may exploit identified loopholes in the organisation's controls or security system to perpetrate crimes. Furthermore, these crimes may be committed with impunity in the absence or nonimplementation of criminal laws that serve as deterrents.

The following actions may reduce the vulnerability of customers to cyberfraud:

- The first line of defence is cybersecurity. Cybersecurity awareness and initiatives should be geared up (Bamrara, Singh & Bhatt 2013; Dlamini & Modise 2012).
- Financial institutions need to strengthen their information security architecture and initiate collaboration between the security apparatus

and intelligent structures at all levels. This will make them more robust and proactive against cyberfraud occurrences rather than being reactive.

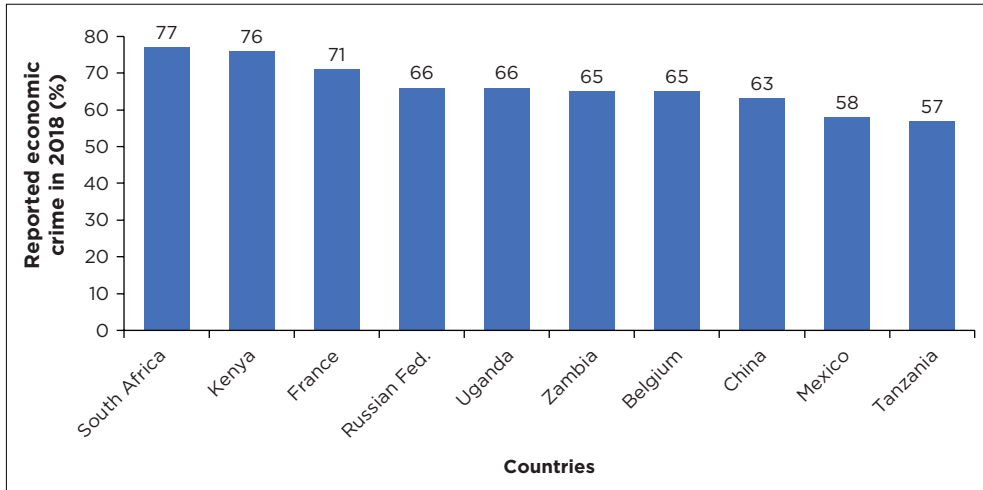
- Alert systems should be augmented for cyberfraud identification (Dzomira 2017).
- Employees and customers should be trained and sensitised about the type of cyberfraud committed by the threat actors and the measures to tackle it. Financial institutions should persistently fight against Internet banking fraud to the advantage of the customers and other shareholders (Dzomira 2017).
- Cyberfraud can be mitigated through robust internal control (Shahabuddin, Alam & Azad 2011). Effective internal control plays a significant role in fraud identification and mitigation as well as in the protection of the organisation's resources, both physical and tangible. Prabowo (2011) explained that adequate internal control can promote the implementation of fraud prevention policies, awareness and risk management plans, litigation processes and anti-fraud technologies. Some internal controls could include multi-factor authentication, fraud-awareness, implementation of transaction limits, security and network monitoring, threat detection tools, robust real-time incidence response and third-party risk management, among others.

■ Cyberspace

The vulnerability of cyberspace because of the lack of strict regulation for entry and exit can promote cyberfraud-related occurrences (Uma & Padmavathi 2013, p. 390). Protecting Internet of Things (IoT) devices from cyberattacks necessitates carefully considering the associated risk factors. This is because cyberattacks also target organisational IoT devices. Without adequate security measures deployed by financial institutions, cyberspace could be a target for cyberfraud, such as identity theft, malware, data theft, cash theft, unauthorised acquisition of sensitive information, impersonation, network disruptions and the generation of fake links.

According to Kopp, Kaffenberger and Wilson (2017), the anonymity of perpetrators who explore the virtual computer world sometimes increases the threat level of cyberfraud. Furthermore, financial institutions are vulnerable to cyberattacks because they rely on interconnected digital technologies within cyberspace for banking operations.

The following actions may reduce the vulnerability of customers and financial institutions to cyberfraud resulting from the exploitation of cyberspace:



Source: PwC (2018, p. 9).
Key: Russian Fed., Russian Federation.

FIGURE 2.4: Reported economic crime of selected countries in 2018.

- Network, system and database security, which involve using a checkpoint firewall with good processing capability, a network firewall and network access control, and a database or web server firewall.
- Periodic updates to anti-fraud software.
- Advanced data analytics.
- Development of robust internal controls, which includes periodic internal and external auditing, forensic investigation, monitoring of suspicious activities, account reconciliation and documentation, staff rotation, cybersecurity awareness and sensitisation, implementation of anti-fraud prevention and detection technologies, and development of effective cyberfraud risk management and response plans.
- Corporate security (IT and physical security).
- Social network monitoring.
- Transaction authentication.

The PwC (2018, p. 8) Global Economic Crime Survey report showed that cyberfraud threatens advanced and emerging economies. The survey reported that among the top ten countries surveyed, South Africa was ranked first, with the highest percentage of economic crime (77%), followed by Kenya (76%) and France (71%). This is indicated in Figure 2.4.

■ Impact of cyberfraud

This section considers the impact of cyberfraud at both the micro and macro levels.

■ Impact of cyberfraud at the micro level

Abdulrasheed, Babaitu and Tinusa (2012) and Abdurraheem, Isiaka and Muhammed (2012) indicate that cyberfraud significantly impacts Nigerian banks' financial performance regarding monetary loss because of perpetration and the cost incurred in combatting it. The outcome of this study agrees with the findings of Ikpefan (2007, p. 21), Ogunleye (2010, p. 120), Nwankwo (2013, p. 144), Kanu and Okorafor (2013, p. 253) and Kanu and Idume (2016, p. 10), who establish a significant correlation between the fraud perpetration in the banking sector and financial performance of the Nigerian banks. Thus, the studies show that an increase in bank fraud cases can negatively impact the performance of financial institutions.

In Botswana, Chimuka and Mashumba-Paki (2016, pp. 114, 117) report that the increasing rate of cybercrime in the country continues to affect the performance of financial institutions and emphasises the need for more proactive measures to combat crime. Cross and Blackshaw (2015, p. 119) report that Australia is also faced with cyberfraud cases, although with a low rate of reportage because of the fear of shame and stigmatisation. The Australian Cybercrime Online Reporting Network (ACORN 2015) report that in 2015, 39,491 cybercrime cases caused an estimated annual loss of AU\$1 billion. Also, the Australian Bureau of Statistics (2016) report that in 2016, 1.6 million Australians fell victim to personal fraud, while 126,300 were victims of identity theft. Broadhurst (2017, p. 2) stated that over 50% of the Australian population aged fifteen-years-old and older had fallen victim to one form of cyberfraud or another (Broadhurst 2017, p. 2).

PriceWaterhouseCoopers (2014, p. 14) indicates that in 2014, 19% of the organisation in the United States of America (USA) lost between US\$50,000 and US\$1m to cyberfraud. The Centre for Strategic and International Studies (2014, pp. 3, 21) estimates that cyberfraud accounts for about 0.8% of the global GDP and 0.64% of the United States (US) GDP. The indicators used for this estimate include financial and reputational loss; loss because of theft of personal information, data and intellectual property; and job displacement.

In the USA, fraud investigation in a corporate setting is a significant focus of the Federal Bureau of Investigation (FBI). Dutta (2013) states that the total number of fraud-related cases under the FBI's investigation was 653 as of 2010. By the end of 2011, the number rose to 726. This implies a 10% increase in fraud-related cases within a year. Within five years, fraud-related cases involving financial institutions reportedly increased by 37%, resulting in investor losses of over US\$1bn (Dutta 2013).

In the UK, the gross losses because of cyberfraud-related activities against all victims in the years 2006, 2010, 2011 and 2012 were approximately

£13bn, £30bn, £38bn and £73bn, respectively. The estimation of the losses experienced in 2012 accounted for a nearly 48% increase in the rate of cyberfraud perpetration within a year (National Fraud Authority 2012). In 2016, the banking sector in the UK spent a whopping sum of US\$360bn on information securing and its enabling technologies. On the contrary, the organisations linked to financial services have reportedly spent thrice the amount spent by nonfinancial institutions to tackle cyber insecurity (UK Finance 2018, p. 4). KPMG (2018) stated that 'In tackling economic-related crimes, the financial institutions now expend about £5bn annually'. The PwC (2007, p. 4) report indicated that in 2007, India lost US\$2.5m to cyberfraud, while a total of US\$1854m was reportedly lost by other Asian and Pacific countries that same year to cyberfraud-related incidences (PwC 2007, p. 4). In 2017, cyberfraud-related incidences reportedly cost the African economies US\$3.5bn. Out of this, US\$649m and US\$210m in losses were ascribed to Nigeria and Kenya, respectively. South Africa reportedly incurs an annual loss of US\$157m to cyber-related attacks (Kshetri 2019, p. 77). On a global level, financial institutions continue to incur losses because of cybercrime, either directly or indirectly. Anderson et al. (2013, p. 1, cited in Ali et al. 2017, p. 71) project that the cost consequence of cyberfraud will increase over the next ten years, with financial institutions in the Middle East the most likely to be affected.

There is no doubt that finance-related crimes are increasing globally with an impact on the economy, public and financial institutions and their shareholders (Bhasin 2013, p. 10). Cassim (2016) states that the rate of cyberfraud in South Africa is increasing in the banking sector, with phishing being the most prevalent (Cassim 2016, p. 130). The PwC (2016, p. 10) global economic crime survey also indicates an increasing economic crime rate in South Africa (69%). The statistics show that almost one-third of South African businesses have fallen victim to hackers. At the same time, only 35% have adequate response strategies to combat cyberfraud. The PwC (2018) report indicated that 'South African businesses continue to report the highest instances of economic crime in the world, reaching the highest level over the past decade'.

According to the PwC (2022a) report, cybercrime represents 36% of the economic crime cases experienced in 2022, with 26% of the fraud cases attributed to customers' fraud. Thus, cybercrime was ranked first among the categories of the widespread and most destructive economic crime over the past two years (2020–2022) in the US and worldwide. Cyberfraud has direct and indirect consequences on financial institutions, their stakeholders and the economy at large (Detica 2011). Bhasin (2011) states that fraud can impact organisations negatively in finance, operation, reputation and customer relations.

Martin and Rice (2011) stress that cybercrime directly impacts an organisation's profitability, reputation, customer satisfaction and goodwill. The effects of cyberfraud include loss of revenue; an organisation's reputation or goodwill; customer, stakeholder or public dissatisfaction; and other related risks (Goel & Shawky 2009; Kraemer-Mbula, Tang & Rush 2013; Lagazio, Sherif & Cushman 2014; Martin & Rice 2011; Saini, Rao, & Panda 2012).

The Information Security Institute (2013) and Cyber Security Ventures (2017) have underscored some of the effects of cybercrime as follows:

- theft of cash or data; data damage or destruction
- loss of information
- disruption to regular business operations or services
- loss of an organisation's reputation
- loss in the form of compensation to victims
- penalties for business or service interruptions
- cost implications relating to insurance and the development of countermeasures
- revenue or financial loss capable of affecting the organisation's profitability
- loss of productivity, competitiveness, business or jobs
- disruption of cyber infrastructure and restoration of hacked data and systems
- cost of investigation.

These impacts of cyberfraud on financial institutions are categorised into categories: Shareholders' loss and dissatisfaction, loss of profitability, loss of goodwill and reputation, as well as damage to banking infrastructure and compromise of information security. Wanemba (2010) indicates that cyberfraud negatively impacts operational costs, reputation, customer satisfaction and financial institutions' revenue. Tariq (2018) states that the loss incurred by financial institutions because of cyberattacks can be grouped into direct and indirect losses. The direct loss is the loss that can be measured directly. For instance, the loss is attributed to loss of money because of theft or data breaches. In contrast, an indirect loss is a loss that cannot be measured directly, such as because of customer dissatisfaction and the loss of reputation or goodwill.

□ Shareholders' dissatisfaction

In South Africa, SABRIC (2018) reported that 12,575 cases were reported of mobile banking fraud in 2018. In 2020, the reported number of mobile banking fraud incidences increased by 67.66% (SABRIC 2020). The South African Banking Risk Information Centre (2021) reported that digital

banking decreased the total number of cases by 18%. The South African Banking Risk Information Centre (2021) also noted that the reported number of mobile banking fraud cases decreased by 45% compared to 2020, with 10,998 incidences compared to 21,106 cases in 2021. However, mobile banking accounted for 38% of the reported digital banking fraud in 2021 (SABRIC 2021). In 2021, there was a 13% increase in the reported fraud incidences attributed to using different banking applications. This accounts for an increase in the reported fraud cases to 12,095 in 2021 compared to 10,667 in 2020 (SABRIC 2021). Thus, 42% of digital banking fraud is reportedly perpetrated through banking applications. This may be attributed to the increasing number of banking application users. According to the Surfshark Report (2021), South Africa witnessed a 2% increase in cybercrime density in 2021 compared to 2020. The increase in the number of reported cyberfraud-related incidences by customers indicates dissatisfaction.

Table 2.2 presents the reported cases of cybercrime documented by the FBI in 2021 and 2022, according to the Surfshark Report (2021). The table ranks the top ten countries based on their cybercrime density (the number of cybercrime victims recorded per 1 million Internet users). The report indicates that the UK, for the second year in a row (2020 and 2021), experienced the highest cybercrime density. The AAG Report (2022a) also corroborated that the UK has the highest number of cybercrime victims per million Internet users, followed by the USA. This can be traced to the fact that the UK is ranked 22nd on the world list of countries with a high NCSI with an NCSI of 77.92 as of November 2022. The US is ranked 41st with an NCSI of 64.94 (E-Governance Academy Report 2022). The NCSI is a global live index measuring countries’ preparedness to mitigate cyber

TABLE 2.2: Cybercrime density for the top 10 countries in the world.

No.	Country	Percentage increase or decrease in cybercrime density between 2020 and 2021	Number of victims per 1 million Internet users
1.	United Kingdom	40	4,783
2.	United States of America	-13	1,494
3.	Canada	7	174
4.	Australia	-22	102
5.	Greece	-75	72
6.	South Africa	2	52
7.	The Netherlands	50	41
8.	France	20	33
9.	Germany	-9	18
10.	Mexico	14	16

Source: Surfshark Report (2021).

threats or manage cyber incidents (E-Governance Academy Report 2022). 'An estimated 53.35 million US citizens were reportedly affected by cybercrime in the first half of 2022' (AAG 2022a, n.p.). US citizens reportedly lost US\$6.9bn to cyber-related crimes in 2021, while the cost of rectifying cyberattacks reportedly cost an average of US\$1.08m in 2021, as opposed to US\$2.09m in 2020 (AAG 2022a). Furthermore, 50% of US organisations have full cyber insurance coverage, while 28% of US organisations are not under full insurance coverage. This implies that many US organisations are either not under insurance or partially covered. This may pose a severe recovery challenge in any event of cyberattack (AAG 2022a).

Countries such as Greece, Australia, the USA and Germany witnessed a significant decrease in cybercrime density in 2021 compared to 2020, while countries like the UK, Canada, South Africa, the Netherlands, France and Mexico continue to experience a surge in cybercrime density. The estimate presented in Table 2.2 is based on the number of victims per 1 million Internet users across these top ten countries. In terms of Internet breaches, the USA has the highest reported incidences of Internet breaches, with an estimated one out of every two Internet users. At the same time, Oceania was ranked second, with an average of two out of five reported cases of Internet breaches. Statista (2022) indicated increasing complaints by customers of Internet fraud.

□ Loss of money and profitability¹

UK Finance (2018) indicates that the global impact of cyberfraud exceeds US\$450bn a year. According to the Centre for Strategic and International Studies (CSIS) (2020) estimate, the global cost of cyberfraud has surpassed US\$1tn between 2018 and 2020. Cybersecurity Ventures (2022) projected that the worldwide cost of cyberfraud will increase by 15% annually, reaching US\$10.5 trillion annually by 2025.

In South Africa, *BusinessTech* (2017) reported that the Amalgamated Banks of South Africa (ABSA) and Standard Bank customers lost between ZAR1m and ZAR2m to Internet banking or SIM swap fraud in 2017. The South African Banking Risk Information Centre (2020) reported that in 2019, a total of 3,304 cases of online fraud reportedly cost ZAR1,17,705,112 in gross sum, while in 2020, the number of online fraud-related incidences reported increased by 19% but with a 19% decrease in gross sum losses (SABRIC 2018). The South African Banking Risk Information Centre (2018) also noted that the mobile banking fraud in 2018 reportedly cost ZAR28,245,948 in gross loss, while in 2020, there was an increase in gross

1. The following section is derived on information from AAG (2023).

loss by 61.10% (SABRIC 2020). The South African Banking Risk Information Centre (2021) reports a significant increase of 45% in gross losses from ZAR310,484,349 in 2020 to ZAR438,238,743 in 2021 (SABRIC 2021). The South African Banking Risk Information Centre (2021) reports that the banking industry in South Africa has successfully implemented enhanced detection and prevention measures to curb fraud relating to mobile banking.

The most common form of digital banking crime that accounted for most losses incurred was social engineering, such as phishing, vishing, spam emails, hacking and online fraud (SABRIC 2020, 2021). Online banking fraud accounts for 20% of the total digital banking fraud, with an estimated 9% reduction in financial losses between 2020 and 2021 in South Africa (SABRIC 2021). The average cost per cyberfraud incidence was estimated at ZAR37,308 in 2020, compared to ZAR33,781 in 2021 (SABRIC 2021). However, the form of digital banking fraud that is still of great concern is the fraud emanating from using different banking applications. The South African Banking Risk Information Centre (2021) reported a 13% increase in fraud incidences because of using various banking applications, accounting for 49% in gross losses. The average financial loss per banking application fraud incidence increased to ZAR17,775 in 2021 compared to ZAR12,315 in 2020, thus accounting for a 44% increase.

Tassev (2022) states that the average cost of recovering data stolen from ransomware attacks in South Africa is estimated at ZAR6.8 million. The South African Banking Risk Information Centre (2021) also indicated that South Africa loses between ZAR157m and ZAR2.4bn per annum to cyberattacks. Wanemba (2010) stated that financial institutions in Kenya have regularly lost significant amounts of money to cyberfraud-related attacks or other forms of fraud, thus affecting the institution's profitability.

Table 2.3 presents the prevalent form of cybercrime, the average loss, number of victims and total loss for 2021 on a global scale. The table indicates that phishing is the most prevalent form of cybercrime, with about 324,000 victims in 2021. However, the impact in terms of loss is minimal compared to other forms of cybercrime, except for malware and denial-of-service attacks. The report of AAG (2022b) corroborates that despite the prevalence of phishing, it had the lowest loss to victims, as individuals report losing an average of US\$136 to phishing attacks in 2021, far below the average data breach cost of US\$12,124. Phishing remains the most common form of cybercrime. For instance, in North and Latin America, phishing accounts for 47% of cyberattacks on business organisations in 2022. As such (AAG 2022a):

Globally, 323 972 Internet users fell victim to phishing attacks in 2021 [...] with an average of \$136 lost per phishing attack. This amounts to \$44.2 million stolen by cyber criminals through phishing attacks in 2021. (n.p.)

TABLE 2.3: Prevalent form of cybercrime, average loss, number of victims and total loss for 2021.

Prevalent form of cybercrime	Average loss (in US\$)	Number of victims (in thousands)	Total loss (millions, US\$)
Online payment fraud	4,665.0	93.5	436.2
Identity theft	539.0	51.6	278.3
Credit card fraud	10,328.0	16.8	173.0
Impersonation	12,584.0	11.3	142.6
Spoofing	4,436.0	18.5	82.2
Ransomware	13,196.0	3.7	49.2
Phishing	136.0	324.0	44.2
Malware	6,910.0	0.6	5.6
Denial-of-service	197.0	1.1	0.2
Technical support scams	1,454.0	23.9	347.7

Source: AAG Report (2022a).

In 2022, the most common URLs in phishing email links to websites were Adobe, Google, Myportfolio, Backblaze and Weebly. In the first quarter of 2022, LinkedIn was the most imitated brand for phishing attempts globally. The top five most imitated brands in the first quarter of 2022 globally were LinkedIn (52%), DHL (14%), Google (7%), Microsoft (6%) and FedEx (6%). The top five origin countries for spam emails in 2021 were Russia (24.77%), Germany (14.12%), the USA (10.46%), China (8.73%) and the Netherlands (4.75%). In the first half of 2022, there were about 236.1 million ransomware attacks globally. In 2021, at least 15.45% of Internet users globally were victims of at least one malware-class attack, which includes ransomware (AAG 2022a). As of October 2022, ransomware accounted for around 20% of cyber breaches. These include using stolen credentials (hacking), which accounts for 40% of violations, and phishing, which accounts for around 20%. The FBI's Internet Crime Complaint Centre (IC3) reported that 2,084 ransomware incidents were reported between January and July 2021, accounting for losses of US\$16.8m (AAG 2022a). The top ten countries most affected by ransomware attacks were Israel, South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran and the UK. In terms of business organisations, the top five most affected countries were the USA (47%), Italy (8%), Australia (8%), Brazil (6%) and Germany (6%). Ransomware has accounted for 4% of cyber breaches in UK businesses so far in 2022. The most common entry point for ransomware attacks is through phishing, with 41% (AAG Report 2022a).

□ Loss of goodwill and reputation

BusinessTech (2017) indicates that cyberfraud could result in the loss of trust reposed in the financial institution by the shareholder. This may lead to a loss of credibility on the part of the institution and a lack of confidence

in the public. Odelabu (2014) mentioned that fraud perpetration affects organisations' reputations, resulting in a loss of public trust and customer confidence. Mohd et al. (2010) state that the inability of financial institutions to protect their customers' information or data can result in a loss of integrity, which can damage the customers' relationship. Alagarsamy and Wilson (2013) state that some of the customers' requirements from financial institutions are speed, precision, responsiveness and security. The inability to meet these requirements may result in a loss of competitive edge and visibility, with a resultant loss of customers. Furthermore, banks vulnerable to cyberfraud are more susceptible to low credit ratings by customers and experts. Some often receive warnings from regulatory bodies and experts because of cyberfraud activities or increasing customer complaints. This is an indication of loss of trust by customers and experts in the ability of the bank to protect customers' investments and confidential information. As the customer is the driver of any business, the loss of credibility could be detrimental to the success of such a financial institution.

■ Impact of cyberfraud at macro level

In 2014, the Centre for Strategic and International Studies (CSIS 2014) reported that cybercrime cost the world economy an estimated cost between US\$345bn and US\$445bn. Regarding the global GDP, cybercrime reportedly cost the global economy 0.62% of GDP in 2014 (CSIS 2014). In 2016, CSIS reported that the cost of cybercrime to the worldwide economy ranges between US\$445bn and US\$600bn (CSIS 2018), translating to 0.8% in 2016. The cost of cybercrime on the global economy includes the following (Broadhurst et al. 2018):

- loss of intellectual property and confidential business information
- online fraud and financial crimes
- opportunity costs, including disruption in business operations and services and a decline in trust for online activities
- cost of securing networks, cost of cyber insurance and paying for recovery from cyberattacks
- reputational damage and liability risk for the affected organisation, including its brand, as well as temporary damage to stock value.

CSIS (2018) summarises cybercrime's impact on the global economy (Table 2.4).

■ Possible mitigation approaches to cyberfraud

Herselman and Warren (2004, p. 256) identify the full deployment of digital technologies as one of the ways to mitigate cyberfraud effectively. At the

TABLE 2.4: Impact of cybercrime on the global economy.

Region	Region GDP (US\$, trillion)	Cost of cybercrime (US\$, billion)	Loss because of cybercrime (% of GDP)
North America	20.2	140–175	0.69–0.87
Europe and Central Asia	20.3	160–180	0.79–0.89
East Asia and the Pacific	22.5	120–200	0.53–0.89
South Asia	2.9	7–15	0.24–0.52
Latin America and the Caribbean	5.3	15–30	0.28–0.57
Sub-Saharan Africa	1.5	1–3	0.07–0.20
Middle East and North Africa	3.1	2–5	0.006–0.16
World	75.8	445–608	0.59–0.80

Source: CSIS (2018).

Key: GDP, gross domestic product.

same time, Obeng-Adjei (2017, p. 78) further recommends synergy among financial institutions, the government, the ICT sector, and the public and private sectors on cybersecurity and implementing stringent cyber law. Gumbi (2018, pp. 92–93) also recommends harmonising the ICT strategies in relation to the regulatory and policy frameworks. Furthermore, the codification of cybercrimes, penalties and prosecutorial procedures, as well as the development of human capacity and public sensitisation regarding cybercrime were also recommended by Gumbi (2018, pp. 92–93). The author recognised that cybercrimes are multi-jurisdictional. Hence, local, regional and international collaborations will be beneficial in combatting cybercrime.

Ali et al. (2017, p. 76) support using applications and security software for security reinforcement. At the same time, UK Finance (2018, p. 14) suggests the adoption of cyber threat intelligence, forensic and cyber-defence capabilities, and robust cloud technology for effective collaboration aimed at data collection and storage as well as information-sharing among the stakeholders involved in the mitigation of cybercrime. Akinbowale et al. (2020, 2021, 2022a, 2023a) propose developing and implementing sustainable and digital approaches such as forensic accounting, effective management control systems, balanced scorecards and big data technology. In addition, Ali et al. (2017, p. 76) indicate the need for regular updates of security software and other anti-fraud technologies to make them effective in tackling fraud. This is important because of fraud's dynamic nature in the financial institution.

Dzomira (2015b, p. 13, 2017, p. 143) suggests using Internet banking fraud alerts by financial institutions to communicate cybercrime perpetrated by cybercriminals in real time. To track down the perpetrators, Wu et al. (2018, p. 3) propose using tracking systems such as the intrusion detection

system (IDS) for real-time monitoring of intrusions into the organisation's system or network. The IDS can prevent and track intrusions, including identifying intrusions patterns and the intruders' location for easy tracking (Wu et al. 2018, p. 4).

Brickner, Mahoney and Moore (2010) provide an applied-learning exercise in teaching fraud detection. The study suggests the integration of fraud detection strategies into the academic curriculum so that students can gradually acquire and develop skills relevant to fraud detection.

■ Conclusion

This chapter presented an overview of fraud with cyberfraud and its prevalent forms as a subset of general fraud. It presented the common forms of cyberfraud as phishing, data theft, hacking, malware, spamming, skimming, online theft, identity theft, spying, cyberstalking, pharming, vishing, spoofing, whaling and software supply chain attack. Out of these common cyberfraud forms, existing reports indicate that phishing is the most prevalent. Various loopholes exploited by fraudsters for perpetrating cyberfraud were also identified. These include customers' ignorance, the organisation's weak controls and cyberspace dynamics. Practicable solutions to mitigate the occurrence of cyberfraud in all these identified loopholes were also presented. Finally, the impact of cyberfraud was categorised into four major categories: shareholder dissatisfaction, loss of money and profitability, loss of reputation and goodwill, and the effect on the global economy. Existing reports indicate that cyberfraud's impact in all four categories is still detrimental.

Cyberfraud: Theoretical perspectives

■ Introduction

The theoretical framework is a set of connected ideas and assumptions that presents a systematic view, explanation or prediction about a phenomenon. This chapter aims to provide theoretical frameworks that explain the concept of fraud. The essence is to give an insight into the rationale, probable causes and motivating factors for committing fraud. The general fraud theories discussed in this chapter include the fraud triangle theory (FTT), the fraud scale theory (FST), the fraud diamond theory (FDT), the fraud box key model and the fraud management lifecycle theory (FMLT), the routine activity theory (RAT), self-control theory (SCT), Akers' social learning theory (ASLT), denial of risk theory (DRT), general strain theory (GST), agency fraud theory, control fraud theory and the eclectic theory. The fraud theories identify and examine the significant factors influencing fraud perpetration under different circumstances. The theoretical assumptions further enhance the understanding of various concepts of fraud management to devise sustainable measures to mitigate the identified fraud causes. Hence, the fraud theories discussed in this chapter provide an in-depth understanding of the fraud investigative processes and the resources needed for combatting fraud, which could be helpful for organisations in their quest to mitigate fraud.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Cyberfraud: Theoretical perspectives', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 47-77. <https://doi.org/10.4102/aosis.2024.BK485.03>

This chapter considers cyberfraud from a theoretical perspective. Fraud theories are a set of assumptions and explanations about the fraud phenomenon in terms of the rationale, loopholes exploited by the perpetrators and the possible ways of mitigating it. The theoretical framework is a set of connected ideas and assumptions that presents a systematic view, explanation or prediction about a phenomenon (Imenda 2014). The theoretical framework helps contextualise formal theories, providing directions about the subject under investigation and can provide a basis for supporting the ideas or findings of researchers (Adom, Hussein & Agyem 2017; Grant & Osanloo 2014; Imenda 2014).

Theoretical frameworks were considered in this chapter to provide insight into the rationale, probable causes and motivating factors for committing fraud. It also provides an in-depth understanding of the fraud investigative processes and the resources needed for combatting fraud. General fraud theories were considered, followed by cyberfraud theories. The consideration of these theories provided an avenue to link the general fraud theories to cyberfraud theories to better understand the actors, causes and motivations for cyberfraud and the mitigating approaches.

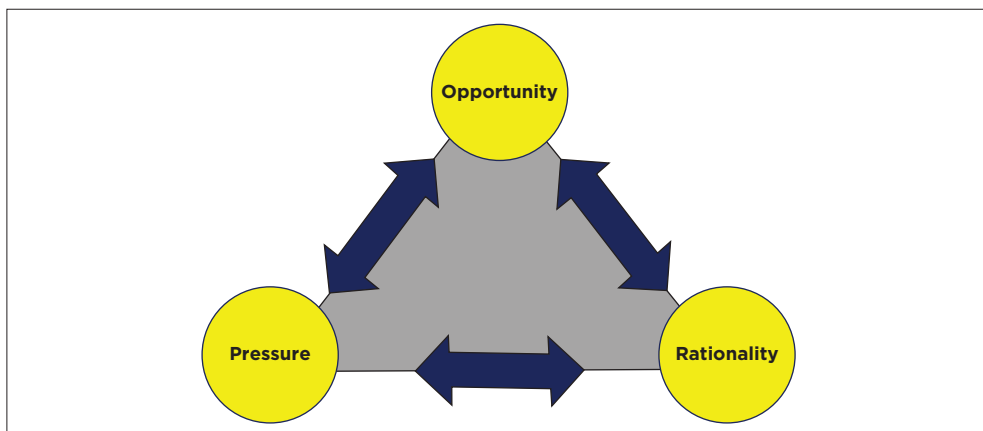
■ General fraud theories

The general fraud theories considered include the FTT, the FDT, the FST, the fraud box key model and the FMLT. Other fraud theories considered include the RAT (Bossler & Holt 2009; Holt & Bossler 2009, 2020; Nasser & Al-Dosari 2020; Reyns 2013), SCT (Donner et al. 2014; Reyns et al. 2019), ASLT (Hawdon, Bernatzky & Costello 2019; Holt, Burrus & Bossler 2010), DRT (Offei et al. 2019), GST (Dearden, Parti & Hawdon 2021; Patchin & Hinduja 2011), the agency fraud theory (Dalton 2007), the control fraud theory (Davia et al. 2001) and the eclectic theory (Riahi-Belkaoui & Picur 2000).

■ Fraud triangle theory

The FTT was developed by Cressey (1973). The theory explains the reasons for threat actors to commit fraud and highlights the justification provided by the threat actors. It summarises the factors that contribute to the growing fraud risk into three categories: (1) opportunity, (2) pressure or incentive and (3) rationalisation. These three factors are highlighted in Figure 3.1.

The *opportunity* to perpetrate fraud refers to the circumstances that lead to fraud occurrences. It is the only factor in the fraud triangle that an organisation can exercise complete control over. In the case of cyberfraud, the opportunity to commit fraud could be a result of ineffective organisational



Source: Adapted from Cressey (1973).

FIGURE 3.1: Fraud triangle.

control at all managerial levels, poor or weak internal controls (Cressey 1973), lack of ethical culture, inadequate or lacking monitoring and supervision, advancement in digital technologies and online banking platforms, ignorance of the customers or victims, override of internal controls by top management, inadequate accounting or financial policies and an ineffective legal framework for combatting cyberfraud, among others. For instance, fraudsters can identify the weaknesses in financial organisations and take advantage of loopholes and the vulnerability of weak organisational structures to commit fraud (Kelly & Hartley 2010; Rae & Subramanian 2008). Hooper and Pornelli (2010, p. 6) state that financial fraud cannot occur unless there is an opportunity to be exploited by the threat actors.

Pressure or incentive refers to the mindset of the threat actors in perpetrating fraud. For cyberfraud committed internally, pressure can lead to a breach of unethical behaviour (Rasha & Andrew 2012, p. 193). Lister (2007) identifies three types of pressure, namely, corporate, personal or external. Certain factors can influence the behaviour and beliefs of the threat actors towards committing fraud. Rasha and Andrew (2012) argue that corporate or personal pressures are significant reasons for committing fraud. This might include the need to acquire more money, the quest to make ends meet or just addiction to fraud. Vona (2008), similar to Rasha and Andrew (2012), argues that pressure can result from particular circumstances. Still, it is often believed to result from non-shareable financial needs.

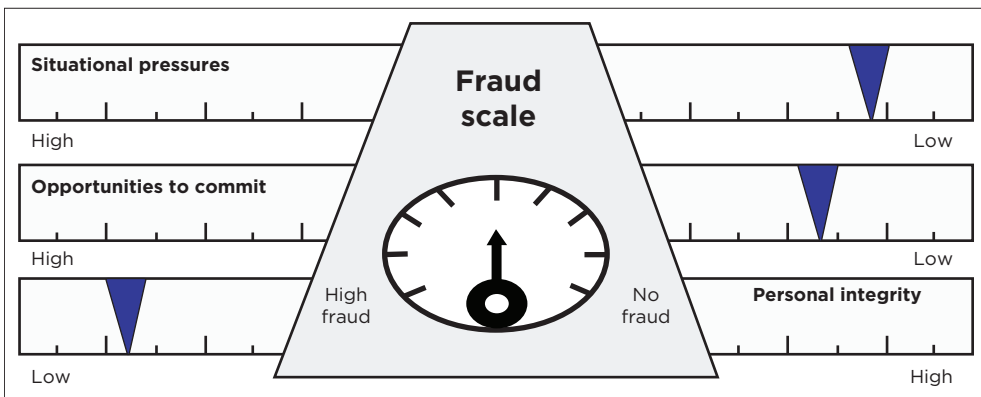
Rationalisation is the third factor of the FTT, and it indicates the morally acceptable idea formulated by perpetrators before engaging in any

unethical behaviour. This factor believes that fraudsters have a typical belief that permits them to defend their fraudulent activities (Hooper & Pornelli 2010, p. 7). For instance, employees or former employees may perpetrate cyberfraud to take revenge on an organisation. Threat actors may cite reasons such as unemployment indebtedness as justifications for committing fraud. However, Rae and Subramanian (2008, p. 106) submit that there is no proper justification for committing fraud and that fraudulent behaviour is a product of the threat actors' lack of integrity or moral reasoning.

Wolfe and Hermanson (2004), however, criticise the concept of the fraud triangle because of the omission of an essential factor (capability) that can contribute to the increasing fraud risk. This led to the FDT, which adds *capability* to the three factors identified under the FTT.

■ Fraud scale theory

The FST was developed by Albrecht in 1984 as a refined form of the FTT, which replaces rationalisation with integrity (Albrecht, Howe & Romney 1984). Thus, according to this theory, the main factors that determine the occurrence of fraud are situational pressure, opportunity to commit fraud and integrity (Figure 3.2). The theory posited that when the situational pressure and opportunity to commit fraud are high, the chances of fraud occurrence will be high and vice versa. However, when an individual's integrity is high, fraud occurrence is unlikely. Albrecht et al. (1984) stated that an individual's integrity can be judged through behaviour and past actions.



Source: Albrecht (1984).

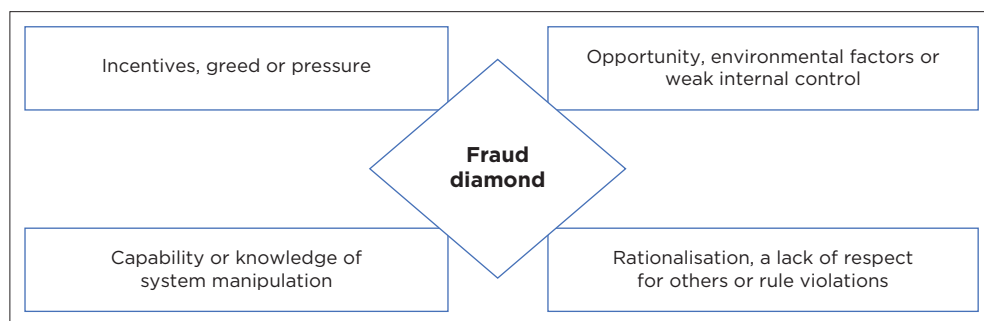
FIGURE 3.2: Fraud scale.

■ Fraud diamond theory

The FDT was introduced by Wolfe and Hermanson (2004) as an extension of the FTT. The theory indicates that capability is an essential factor that can engineer fraud perpetration in addition to opportunity, incentives and rationalisation. The theorist explained that many fraud-related incidents would not have happened without the wherewithal capabilities to commit fraud. Thus, it was perceived that the probability of fraud occurrence is a function of the capability and character of the perpetrator. Wolfe and Hermanson (2004, p. 3), therefore, indicate that opportunity gives room for fraud perpetration while incentive (pressure) and rationalisation can motivate the threat actor to commit fraud. Nevertheless, the perpetrator's ability to identify the opportunities to be exploited and the skills to perpetrate fraud should also be considered. Figure 3.3 displays the components of the FDT.

Wolfe and Hermanson (2004) identify six factors that constitute the capability of the threat actors:

- the position, responsibility and influence of the threat actors
- the experience and expertise of the threat actors in exploiting opportunities
- self-confidence and ability to cover up fraudulent schemes
- coercion of associates to participate in fraud (in the case of cyberfraud, threat actors may engage in cyberbullying, using electronic communication to bully the victim or associates, typically by sending intimidating or threatening messages)
- a consistent habit of lying to deceive the victims and to cover up
- ability to handle stress and the risk involved in fraud perpetration (the threat actors stand the risk of detection, exposure, prosecution and loss of social status).



Source: Wolfe and Hermanson (2004).

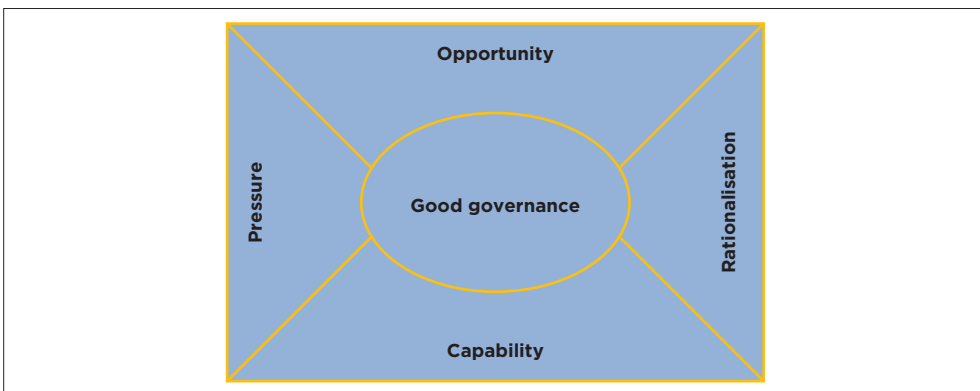
FIGURE 3.3: Fraud diamond theory.

Although the FDT enriched the FTT by introducing the fourth element (capability), Onodi, Okoye and Egbunike (2017) maintain that corporate governance cannot be ignored in fraud analysis. This is because corporate governance is instrumental in fraud investigation, deterrence, prevention and detection.

■ Fraud box key model

The fraud box key model was developed to address the perceived inadequacies of the fraud triangle and fraud diamond theories. Onodi, Okoye and Egbunike (2017) modified the FDT into a fraud box key model by incorporating the fifth factor, *corporate governance*. This essence is to ascertain that corporate governance can directly or indirectly influence the four factors from the previous fraud triangle and fraud diamond models, namely, pressure, opportunity, rationalisation and capacity (Figure 3.4).

Monks and Minow (2011) defined corporate governance as how an organisation's affairs are directed. Thus, corporate governance is a system of rules, processes and practices through which an organisation is controlled and directed. A sound corporate governance system can balance the diverse interests of the shareholders, management, government, regulators and public. Onodi et al. (2017) identify the seven essential corporate functions, namely, oversight, managerial, compliance, internal audit, advisory, external audit and monitoring. Corporate governance can provide a framework through which an organisation can achieve the set objectives. This encompasses the management action plans, internal controls and corporate disclosures. Monks and Minow (2011) identify the key forces governing any organisation: management, shareholders and board



Source: Onodi, Okoye and Egbunike (2017).

FIGURE 3.4: Fraud box key model.

of directors. Corporate governance encompasses ownership and control, mission or objectives, rights and responsibilities, and value distribution (Clarke & dela Rama 2006). Many organisations strive for good corporate governance through sound ethical practices and public awareness. This is because a sound corporate governance system can reduce the potential for fraud perpetration and financial loss and reduce waste and business risks. It can also provide an implementable action plan for long-term success, making the organisation resilient to specific disruptions. This can translate to profitability, financial viability and fraud control. This will build the trust of the shareholders, regulators, employees, government and employer by aligning their interests. Furthermore, it will also promote a clear organisation's direction and business integrity. The inefficiency of corporate governance in many organisations tends to facilitate fraud perpetration. Some of the inefficiencies of corporate governance that can provide the threat actors with an opportunity to commit fraud include abuse of the corporate governance code of conduct, a decline in productivity, poor management or leadership, and ethics-related issues (Onodi et al. 2017). The principle of good corporate governance is based on the following:

- **Fairness:** Consideration for the shareholders, regulators, employees, government and employees.
- **Transparency:** Provision of accurate, timely and unambiguous information about the organisation's performance.
- **Risk management:** Determination of inherent business risks and mitigating measures.
- **Responsibility:** Oversight of corporate matters and management activities.
- **Accountability:** Assessment of the organisation's competence, performance and communication with the shareholders.

■ Fraud management lifecycle theory

This theory was introduced by Wilhelm (2004, p. 9) as a network lifecycle comprising eight factors that determine the success or failure of an organisation in fraud management. The network lifecycle includes nodes where each of the network nodes is an aggregate unit comprising unified, dependent, independent actions, functions and operations. Compared to the traditional linear lifecycle, the stages of the FMLT are not necessarily sequential; hence, the activities in one stage do not necessarily depend on the completion of the preceding stage, as the network lifecycle enables concurrent and successive activities within each node of the network (it is time-effective). The FMLT comprises eight phases, namely, deterrence, prevention, detection, mitigation, analysis, policy, investigation

and prosecution. The interrelationship between these stages is illustrated in Figure 3.5:

- **Deterrence:** This is aimed at fraud prevention before the threat actors contemplate or attempt it. For instance, card activation via encrypted software can minimise the chances of online fraud. Fraud deterrence entails good division of tasks, staff management, work and performance monitoring, and the development of measures to ensure proper control when systems are accessed (Kimani 2011).
- **Prevention:** These are actions and activities aimed at averting fraud occurrence. In any cyberfraud control approach, prevention is of significant priority as the loss because of fraud is usually higher after fraud. In addition, whether the crime is ongoing or has occurred, the chances to stop or recover the loss are often minimal (Lucian 2004).
- **Detection:** These are actions and activities aimed at fraud identification and uncovering. An example is the statistical monitoring programmes usually employed to identify fraud before perpetration or during the crime. The essence of this stage is to detect fraud or fraud attempts. Fraud detection is an ongoing activity as criminals employ new strategies



Source: Adapted from Wilhelm (2004).

FIGURE 3.5: Fraud management lifecycle.

for fraud perpetration once they know sound detection and tracking methods have been implemented to checkmate their existing strategy. Management exercises the primary responsibility of fraud detection via implementing, documenting and operating a robust and effective internal control system.

- **Mitigation:** This stage aims to prevent losses or stop a continuous loss occurrence, that is, developing or introducing a technique to prevent fraudsters from fraud perpetration.
- **Analysis:** This involves identifying and examining the losses incurred and the factors responsible for such losses. Prominent among the methods used at this stage is the root cause analysis.
- **Policy:** This entails activities aimed at creating, evaluating, communicating and assisting in deploying guidelines to minimise fraud incidences. Balancing the fraud reduction framework with resource limitations and robust supervision of genuine customer activities is critical at this stage. It can assist in ensuring compliance concerning security, data and personal information privacy regulations.
- **Investigation:** This involves obtaining adequate evidence and statistics to prevent fraud incidences and recover assets or restitution. This stage also provides proof for litigation support and successful prosecution or conviction of the fraudsters. Fraud investigation encompasses three major activities, namely, internal and external investigations and law enforcement coordination. Internal investigation involves investigating people within the organisation, such as employees, consultants, contractors or vendors. In contrast, external investigation involves people outside the organisation, such as customers, fraudsters and other organised groups (Njenga & Osioma 2013; Wilhelm 2004). As Gottschalk (2010) discussed, law enforcement involves delivering resources and necessary information and maintaining collaborations with law enforcement agencies at all levels. According to the PricewaterhouseCoopers (PwC) (2011) Report on Economic Crime, fraud investigation largely falls into four skill sets: forensic accounting (FA) and transaction analysis, investigative intelligence and analysis, computer forensics, and fieldwork and interviews (Figure 3.6).
- **Prosecution:** This is the zenith of all the achievements and setbacks in the fraud management lifecycle. At this stage, failure can occur because the fraud incident was successful. On the contrary, it can be successful because the fraud was identified, and the suspect was detained with the appropriate charges filed. This stage includes restitution by the perpetrator, asset retrieval and sentence meted out to the perpetrator.

Figure 3.6 presents the fraud investigation skillsets.



Source: Adapted from PwC (2011).

FIGURE 3.6: Fraud investigation skillsets.

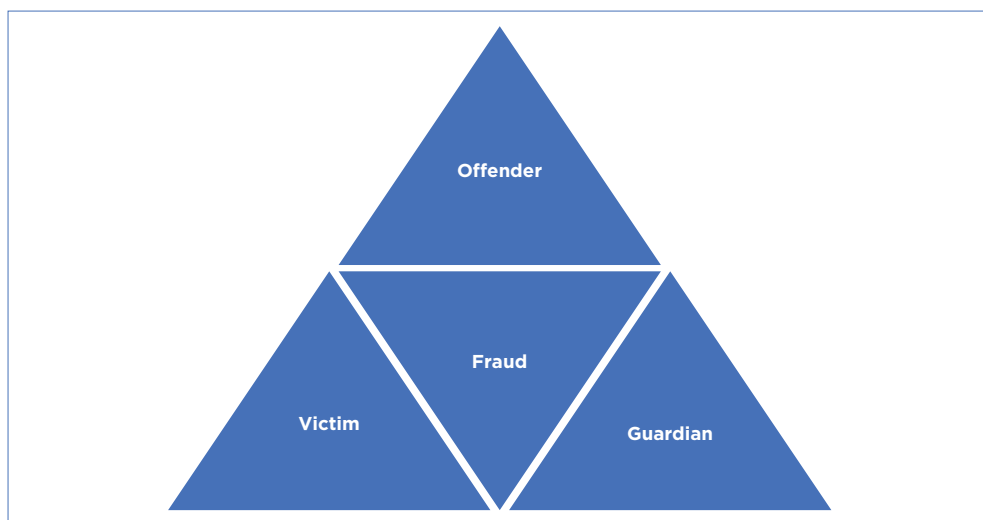
- **Forensic accounting and transaction analysis:** During the investigation, forensic accountants are expected and required to calculate the losses and damages resulting from deliberately falsified accounting records and prepare insurance claims.
- **Investigative intelligence and analysis:** This involves obtaining relevant information from the public about the persons or entities suspected to be engaged in fraud.
- **Computer forensics:** This is an integral part of modern fraud investigation. It involves searching and analysing the electronic evidence, often found on personal computers and modern-day electronic devices.
- **Fieldwork and interviews:** This is the crucial part of most investigations, and it involves an interview with the suspects and witnesses who are vital to fraud investigation. Statements made during an interview can only qualify as admissible evidence suitable for litigation support in a court of law if obtained appropriately.

The FMLT can be adopted as part of the management control systems (MCSs) strategy for fraud mitigation. The mitigation phase of the FMLT can be designed to stop the system's hacking or unauthorised access to sensitive customers or organisational information. It can also be designed

to flag suspicious transactions through a management dashboard. As part of the MCSs, the FMLT can be automated to prevent illegal transactions relating to payments, online fraud, purchases, money laundering, reimbursement or chargebacks. This can be achieved through identity validation and transaction authentication. With the aid of the FMLT, the fraud detection process is a vital tool for a forensic accountant. According to Wilhelm (2004), an effectively deployed and managed FMLT can assist in minimising fraud losses and its impact on the shareholders considerably. The FMLT comprises eight phases, which can increase the understanding and awareness of fraud. With the understanding and awareness of fraud, experts saddled with fraud management will likely communicate and mitigate fraud effectively.

■ Routine activity theory

The RAT was developed by Cohen and Felson (1979). It is an established and widely used theory for the analysis of crimes (Rice & Csmith 2002; Yar 2005). The theory boasts straightforward hints on clear cues for policy formulation and crime-prevention strategies. The theory has three major components, namely, the offender, guardian and victim, as shown in Figure 3.7. Routine activity theory considers crime from the offender's perspective. The theory posited that a crime will only be committed if a likely offender thinks a target is vulnerable and a capable guardian is absent. The likely offender assesses the situation and



Source: Adapted from Nasser and Al-Dosari (2020).

FIGURE 3.7: Routine activity theory.

determines whether a crime will occur (Holt & Bossler 2009). All three are necessary for the analysis of a crime. Routine activity theory relies on the same rational methodology as situational crime-prevention techniques. One of the major criticisms of the RAT is that criminals are rational in their decision-making (Leukfeldt & Yar 2016).

In the context of cyberfraud, the potential offenders are the threat actors (cyberfraudsters). At the same time, the primary targets are the direct object of the offence, resulting directly from the offender's motive for committing the crime. These may include an object, place or person. For instance, the victims may be the customers or the business organisation. The victim may be chosen because of the accessibility of the offender to the victim and the victim's vulnerability to the cyberattack method. The location or activities could also be used to choose the victim. This refers to the victim's locality or activities. Likely, offenders target sensitive information and the digital infrastructure of customers and business organisations to steal information and syphon money. The absent guardians are the stakeholders involved in fraud mitigation and the digital technologies or software employed for cyberfraud mitigation. Cyberfraud may be prevented by altering the three primary factors (likely offender, victim or absent guardian), as these three must come together before fraud can be perpetrated. Business organisations may target any of the three elements to combat cyberfraud effectively. For instance, business organisations may consider tracking the likely offenders and bringing them to book or disrupting their network or infrastructure. In terms of the victims, business organisations can also embark on potential victims' sensitisation, awareness creation or development of strategies for the safety of the likely victims against cyberattacks. The guardian business organisations must ensure that the guardians are present and effectively deployed. Cyber and network securities, internal control implementation, digital technologies and anti-fraud software deployment, and security apparatus synergy can promote fraud mitigation.

Figure 3.7 presents the RAT.

■ The self-control theory

Gottfredson and Hirschi first proposed SCT in 1990 (Diksha & Hirschi 1990). The theory suggests that people with low self-control are more liable to impulsive conduct and have a tendency to commit fraud. Low self-control is perceived as the preference to focus on the short-term rather than the long-term (Hirschi & Gottfredson 1983). This agrees with the assumption that 'everybody is capable of crime' (Diksha & Hirschi 1990). This implies that a significant factor causing fraud is a lack of focus on long-term costs associated with behaviours that provide immediate gains, such as fraud.

Kotabe and Hofmann (2015) indicate seven significant components of the SCT:

- **Desire:** This is the driving force for fraud perpetration (Diksha & Hirschi 1990). This is followed by cognitive elaboration, which directs the perpetrator towards immediate gain.
- **Higher-order goals:** This relates to the perpetrator's cognitive, affective and behavioural activity. Unlike desires, higher-order goals are usually pursued deliberately, linked with expectations of long-term benefits.
- **D-G conflict:** This turns desire into temptation and the higher-order goals into self-control goals.
- **Control motivation:** The aim is to control desire. As such, control motivation is determined by the self-control goal.
- **Control capacity:** All the potential cognitive resources that a person can employ to facilitate the control of temptation.
- **Control effort:** The effective use of control capacity.
- **Enactment constraints:** This relates to the environmental factors limiting a person's behavioural options.

■ Akers' social learning theory

Akers (2009) reviews the differential association-reinforcement theory as a social learning theory of crime and deviance. Akers (2009) argues that criminal behaviours are learned, changed or maintained via social interaction and modelling. This theory includes four major components, namely, differential association, definitions, differential reinforcements and imitation (Akers 2009):

- **Differential association:** This refers to the process by which a person is exposed to things that are either favourable or unfavourable to deviant and criminal behaviour. It considers the value of various sources of definitions and their effects on people. Associations in intimate or social groups can influence the character or conduct of a person. The frequency, intensity or duration of interaction with social groups, such as friends, family and church, significantly impact how people define and perceive things.
- **Definitions:** This refers to the attitudes or personal meanings attached to a particular behaviour. Events are perceived and interpreted differently by people depending on their orientation. An event may be right or wrong, and definitions can be specific or general. The more a person perceives and interprets an event as inappropriate or negative, the lower the probability that such a person will engage in such an act. On the contrary, the more a person perceives and interprets an event as proper or positive, the higher the likelihood that such a person will engage in such an act. Neutral definitions recognise that an action is wrong or

negative yet justify its involvement, probably because of prevailing circumstances.

- **Differential reinforcement:** This balances the actual or anticipated reward and the punishment for a given behaviour. There is positive reinforcement when there is an increased chance that a person will engage in criminal behaviour because of reward or other forms of inducement. The more a person perceives and interprets an event as wrong or negative, the lower the probability that such a person will engage in such an act. On the contrary, there is a negative reinforcement when there are increased chances that a person will engage in criminal behaviour with impunity (without consequences or penalties such as conviction, exposure, or fines).
- **Imitation:** This refers to engagement in behaviour by learning or observing the same or similar behaviour by another. The personality, behaviour and nature of observed consequences determine whether the observer will replicate the behaviour.

Akers (2009) also proposed a four-dimensional social structure learning model. These are differential social organisation, differential location in the social structure, theoretically defined structural variables and differential social locations in groups:

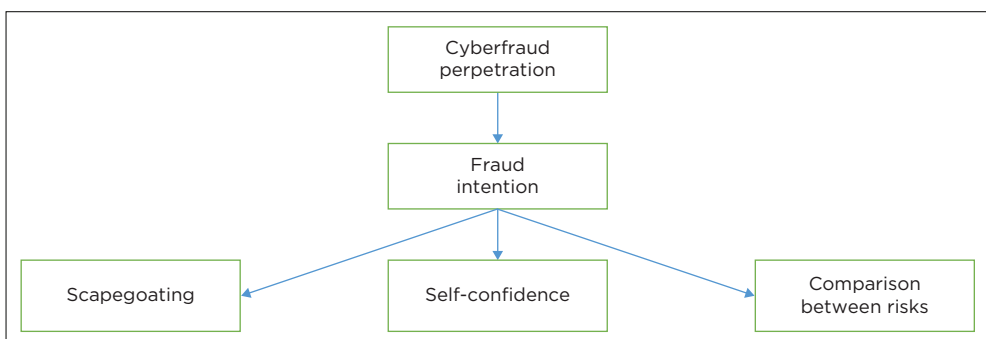
- **Differential social organisation:** This refers to the attributes that propel a particular society to high or low crime rates. It could be the age composition, population density, or unemployment.
- **Differential location in the social structure:** This refers to the socio-demographic features of an individual or social group, such as race, gender, age, marital status, employment status and social categories. These features may contribute directly or indirectly to high or low crime rates.
- **Theoretically defined structural variables:** This refers to the factors influencing a society's criminogenic status or groups. It could be class, anomie, oppression, group conflict or disorganisation.
- **Differential social locations in groups:** This refers to the membership or affiliation of people concerning primary, secondary and reference groups such as family, friendships, peer groups, leisure groups, colleagues and work groups.

■ Denial of risk theory

The DRT discusses the rational ways people adapt to uncertain behaviours by declining the probability of suffering the consequences (Peretti-Watel 2003). This theory postulates that a person may repel the risk level by relating the crime to a satisfactory action. The DRT comprises three

significant constructs: scapegoating, self-confidence and comparing risk (Figure 3.8). Scapegoating is when a person stereotypes the actions of others to justify their behaviour. The scapegoat construct of the DRT deals with the tendency to tag a recognisable group as taking steps that are considered riskier than the one committed by the threat actors (Lazarus 2017). The essence is to provide the basis for the threat actor to repel any risk from their actions to have a positive self-image (Harris & Dumas 2009, Lazarus 2017). For example, fraudsters may justify their involvement in cyberfraud by making the victims (customers, organisations) or the government scapegoats. Some justification for cyberfraud may include unfavourable government or banking policies, unemployment and revenge. Cyberfraudsters may also believe they are causing less evil than ATM or bank robbers who rob customers and banks at gun points. In some emerging economies, cyberfraudsters may also think the involvement of advanced or Western economies in emerging economies has caused more harm than the fraud they perpetrate online (Hutchings 2013). Such rationalisation or justification for committing fraud is an attempt to transfer the blame and absolve themselves of the criminal behaviour (Sugiura 2018). Thus, the intention of the threat actors to commit cyberfraud may be directly or indirectly influenced by scapegoating.

The second component of the DRT is self-confidence. This occurs when threat actors reject the risk of a crime by differentiating themselves from unidentified groups of people. For example, the threat actors who commit cyberfraud defend their actions by indicating they have superior skills to earn a living compared with law-abiding citizens. Some cyberfraudsters believe that cyberfraud is one of the ways to put their digital skills to profitable use.



Source: Adapted from Offei et al. (2020).

FIGURE 3.8: The constructs of the denial of risk theory.

The higher the self-confidence and capacity of a threat actor, the higher the likelihood of committing fraud (Jegede, Olowookere & Elegbeleye 2016; Sigala 2017). Although some cyberfraudsters understand that their acts are criminal and punishable by law, they show confidence that their actions can be performed with impunity. Sometimes, cyberfraudsters increase their confidence in committing fraud by drawing solidarity among themselves (Jegede et al. 2016, Koay 2017). Thus, the intention of the threat actors to commit cyberfraud may be directly or indirectly influenced by self-confidence.

The third component of the DRT is a comparison between risks. People who compare risks consider the crime they perpetrate as a lesser evil than others (Choo 2011). Some threat actors believe that some crimes are riskier than others. Some people committing cyberfraud compare the crime to armed robbery and ATM or bank robbers (McMullan & Rege 2010; Meesters & Behagel 2017; Mekonnen, Padayachee & Meshesha 2015). Thus, the intention of the threat actors to commit cyberfraud may also be directly or indirectly influenced by risk comparison.

■ General strain theory

The GST is a criminology theory developed by Robert Agnew in 1992 (Moon et al. 2017). The theory emphasises that society places a premium on specific socially desirable and approved goals without provision for the opportunity or legitimate means to achieve these goals (Aseltine, Gore & Gordon 2020; Broidy 2001; Froggio 2007; Paternoster & Mazerolle 1994).

In other words, people can be strained and resort to committing crimes to achieve socially desirable goals when there is no legitimate means to achieve such goals. The GST posits that perpetrators commit criminal acts to cope with societal or emotional strains such as depression, anxiety, and anger (Agnew 1992). Agnew (1992) provides four features of GST that can lead to crime:

- Strains are perceived as unjustified.
- Strains are perceived as high in degree.
- Strains are linked to low social control.
- Strains create some incentives or pressure to involve criminal coping.

The strain theory finds application in the various forms of cyberfraud, such as hacking, piracy, online scams and cyberstalking, harassment or bullying (Chism & Steinmetz 2017; Hay & Meldrum 2010; Hay Meldrum & Mann 2010; Hinduja 2006, 2012; Patchin & Hinduja 2011; Wright & Li 2012).

■ Agency fraud theory

Agency fraud theory posits a significant challenge in certain circumstances with a principal-agent relationship (Dalton 2007). The theory suggests that internal governance can reduce information asymmetry between insiders and outsiders, thus minimising the chances of fraud (Dalton et al. 2007).

■ Control fraud theory

The control fraud theory holds that the organisation's structure in specific scenarios may be designed to easily enable fraud perpetration by definite agents, such as employees or managers (Davia et al. 2001).

■ Eclectic theory

The eclectic theory integrates several ecological, transmission and anomie theories to identify scenarios or red flags where fraud is most likely to occur (Riahi-Belkaoui & Picur 2000).

■ Probable causes of fraud from theoretical perspectives

The basic fraud theory is the theory of differential association (Sutherland 1940), while a refined form of the FTT is the fraud scale (Albrecht et al. 1984), where the scale replaces rationalisation for integrity. An extension of the fraud triangle is the fraud diamond, which includes the capability of the threat actor to commit the fraud (Wolfe & Hermanson 2004). Table 3.1 presents the probable causes of fraud from the fraud theories reviewed.

■ Management control systems theories for fraud mitigation

The MCSs ensure resource acquisition and effective utilisation to achieve the organisation's objectives (Anthony 1965). Langfield-Smith (1997, p. 215) defines MCS as 'a process by which managers ensure that resources are obtained and used effectively and efficiently to accomplish the organisation's objectives'. Thus, MCS encompasses management practices and rules that direct employees' activities. The MCS can be broken down into management control and control systems. Management control exists as a process that ensures that organisations achieve their objectives regarding the quality and quantity of available resources (Kloot 1997, p. 49).

TABLE 3.1: Probable causes of fraud from the fraud theories reviewed.

No.	Probable causes of fraud	Applicable theory
1.	Opportunity (absence of fraud mitigation personnel, strategies or technologies or weak internal controls, vulnerable customers or organisations)	Fraud triangle, fraud diamond, fraud box key model, routine activity, fraud management lifecycle
2.	Pressure or incentive	Fraud triangle, fraud diamond, fraud box key model, self-control, general strain
3.	Capacity	Fraud diamond, denial of risk
4.	Lack of good corporate governance	Fraud box key model
5.	Lack of ethics	Fraud box key model
6.	Lack of self-control	Self-control theory
7.	Social interaction and modelling, social structure and location	Akers' social learning
8.	Negative influence	Akers' social learning
9.	Lifestyle, belief or behaviour	Akers' social learning
10.	Adaptation to criminal behaviour or tendencies	Denial of risk
11.	Society and strain	General strain
12.	Lack of deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution frameworks	Fraud management lifecycle, Akers' social learning
13.	Both external and internal sources and conditions. Weaknesses in financial institutions and regulations are major determinants of the prevailing occurrences of cyberfraud	Eclectic theory

Source: Authors' own work.

On the other hand, the essence of the control system is to assist management in directing the organisation towards its goals. Pfister (2014, p. 145) states that the word 'control' in this context means directing, guiding, enabling and supporting the employee to give room for innovation and creativity. Armesh, Salarzahi and Kord (2010, p. 193) explain that information can be gathered through MCS to evaluate an organisation's performance in relation to the human, physical, financial and time resources and set objectives. For an organisation to effectively achieve set goals, there is a need to monitor both the internal and external environments through well-defined management controls (Armesh et al. 2010, p. 198). Thus, a well-developed MCS can effectively utilise resources to influence an organisation's performance. It can also drive an organisation towards the realisation of set goals.

Noorein (2012, p. 120) states that by monitoring and evaluating an organisation's performance and employees' activities through MCS, corrective measures can quickly be taken where there are deviations from the organisation's goals or standard practices. Shurafa and Mohamed (2016, p. 79) indicate the need for effective design of MCS to stimulate organisational learning and enhance organisational performance. In the design of the MCS, Bashir, Zarifah and Sheikh (2013, p. 3) stated that MCS should be integrated into the organisation's social structure; otherwise,

the tool may become complex to implement. A properly developed and implemented MCS can also assist organisations in adapting to the dynamics of the business environment and provide the necessary feedback on organisational performances. It also provides an update on the profit evaluation from products and clients to decide on capital investment (Carenys 2012). Thus, MCS comprises accounting- and non-accounting-based controls, which provide direction to the overall business process or undertakings and motivate the employees towards realising set goals (Yau 2000, p. 92). From the description of MCS, it is a tool suitable for evaluating the employee and organisation's performance about the set goals.

The conventional MCS limitation is that they only aim at ensuring operational efficiency but may not ensure a good competitive advantage (Armash et al. 2010, p. 194). Thus, there is a need for a sustainable MCSs that incorporate managerial values to invite employee collaboration and creativity towards innovation and development of business opportunities. In the context of this chapter, the MCS is aimed at fraud mitigation. Management control systems can foster information gathering and promote communication at the different levels within the organisation on the effectiveness of the strategies employed for cyberfraud mitigation. With the dynamics of cyberspace and the emerging technologies in tackling cyberfraud, MCSs can encourage training and other forms of human capacity development that may aid the effective deployment of anti-fraud technologies or other forms of countermeasure. Furthermore, financial organisations can have a fraud prevention and detection blueprint through an adequately designed MCS. Evaluating the milestone with the actual performance will aid decision-making related to cyberfraud mitigation. In addition, MSCs can also help prevent and detect fraud by evaluating the performance of different departments and the organisation concerning the deployed resources and specific goals of cyberfraud mitigation.

The MCS is a system of information processes that validates and verifies the physical process in an organisation. It can be divided into two categories, which will be discussed in the following sections.

■ Closed-end management control system

This system type of MCS uses a receptor and corrector mode of operation in which the organisation's internal sub-units do not interact with the external units. The flow of information is through the activity, result, matching of the standard pre-set, analysis of the variation and taking corrective steps to mitigate the error. This system uses a receptor and corrector mode of operation.

According to Carenys (2012, p. 13), closed-end MCSs are formal and mechanistic systems with classic and contingency control theories. The classic theory, the classical management theory, believes that employees are highly motivated by meeting their physical needs and other forms of incentives (whether monetary or non-monetary). This theory assumes that employees require a formal mechanism for motivation and control before effective performance can be achieved in line with the organisation's objectives. Thus, organisations implementing this management style often integrate consistent opportunities for employees to be rewarded with incentives based on their productivity. The formulation of the classic theory is based on the rational and scientific perspectives of organisations and management systems.

On the contrary, the contingency theory assumes that no single control system suits all organisations in all situations. In other words, this theory assumes there is no best way to lead or direct an organisation or make decisions. Thus, there is a need to develop control systems to suit an organisation's objective, management structure and style, situation and business environment. From the definitions mentioned, it can be stated that the classic theory is based on clearly identified objectives and measurable outputs. In contrast, the contingency theory is a more flexible form of control developed to adapt to the organisation's current situation. For the closed-end MCS, the overall output of the organisation is usually compared with the identified objectives, and corrective actions will be taken once the output falls short of the benchmark. The lack of flexibility of the closed-ended MCS rooted in the mechanistic and formal control systems makes it more suitable for organisations that perform monotonous activities rather than those that engage in different operations. This type of control does not consider the psychosocial aspects of the employee (that is, the combined effect that psychological factors and the social environment have on the physical and mental wellness of the employees as well as their ability to function in the assigned tasks). Thus, the closed-end MCS is usually difficult to adapt to in a dynamic business environment.

An open-end MCS, like the closed-end MCS, also uses a receptor and corrector mode of operation. However, there is an interaction between the organisation's internal sub-units and external units. Furthermore, the feedback mechanism is continuous in every phase of the activity. This implies that this control has several receptors interacting with several correctors in the system. Carenys (2012, pp. 13-14) explains that open-end MCSs consider the employee's psychosocial aspects, human relations and human information processing to rectify the limitations of closed-end MCSs. With consideration for the psychosocial factors of the employee, the passiveness, rational behaviour and performance of an employee can be stimulated. In addition, this control system also considers the business

environment and the need to adapt to its dynamic nature. Employees' behaviour is essential in developing this control system, as people can be motivated monetarily and non-monetarily.

The limitation of closed and open-ended control systems is that both controls do not affect the organisation's anthropological and cultural factors (Carenys 2012, pp. 10-11). The cultural and anthropological factors can also influence the employees' behaviour, ideology performance and relationship with others (Omar, Johari & Hasnan 2015, p. 367). As cultural factors can affect employees' behaviour, it is necessary to consider this as one of the variables for the control system designed for fraud mitigation. Considering the cultural and human factors in the control systems may enable the understanding of employees' beliefs, moral values and behaviours. This can assist in identifying the rationale and root causes of fraud perpetration and possible ways to mitigate its occurrence. As part of considering cultural factors, Omar et al. (2015, p. 371) further suggest that an organisation can train employees on ethical and cultural values. Carenys (2012, p. 14) explains that a cultural factor is a significant factor that can promote the efficiency of control systems as it is vital in identifying individual and corporate objectives.

By comparing the closed and open-end MCSs, it is clear that the system comprises the organisation's internal sub-units, which do not interact with external systems. In contrast, the MCS includes the organisation's internal sub-units interacting with external systems. However, for fraud mitigation, there is a need for effective communication with other departments and stakeholders, as well as inputs from the environment, such as customers and anti-fraud agencies, as in the case of the open-end MCS.

The MCS theory can assist in achieving sustainability in performance measurement and management via the proper definition of various forms of controls in the organisation and its internal systems. Barrows and Neely (2012) state that the MCS theory specifies that the actions of all the organisation's systems must be integrated and aligned with the organisation's overall objectives. As such, control mechanisms such as performance measurement, organisational structure and behavioural controls, including norms and policies, should be implemented at all levels of an organisation. Behavioural control, which evaluates the employees' actions regularly concerning the organisation's standards, might be valuable in probing the motivating factors for cyberfraud perpetration.

An employee's training can form part of the input control system so that the employee possesses the required expertise needed for growth and development (Krausert 2009). The output control, which measures the employees' performance, may be influenced by incentives, motivation,

rewards or sanctions after regular evaluation. The input and output control systems can be used to investigate the level of human capital development and its performance in a financial institution. This will determine, to a large extent, the employees' capacity to implement some digital anti-fraud technologies for cyberfraud mitigation. The input and output control systems can also influence the effectiveness of the deployed anti-fraud technologies. However, any control mechanism's outcome must be aligned with the organisation's objectives (Barrows & Neely 2012).

Following the review of some articles on the effect of MCS on the organisation's performance, there is a consensus among the authors that a properly designed and implemented MCS could enhance the performance of an organisation, including fraud mitigation (Carenys 2012, p. 12; Henri & Journeault 2010, p. 63; Mohammed & Knapkova 2016, pp. 276 & 277; Slavoljub, Srdjan & Predrag 2015, p. 48; Tekavčič & Peljhan 2003, p. 94).

▣ Corporate social responsibility theory

Corporate social responsibility (CSR) is a voluntary idea in which organisations integrate the social and environmental needs of the employees, customers and the host environment into their business model and budget to impact them positively (EU 2002). The EU (2002) report defines CSR as a model in which an organisation resolves willingly to improve the quality of life and the environment in the host society. Gherghina and Vintilă (2016, p. 23) indicated that an organisation responds to societal needs and social pressures, including social and environmental requirements, through CSR. According to Obalola, Omotoso and Adelopo (2009, p. 199), CSR is a model in which an organisation takes responsibility for the impact of its activities on the host environment while taking necessary steps to alleviate the pressures on the host environment (Obalola et al. 2009, p. 199).

In situations where social values change rapidly, the concept of CSR can promote organisational and stakeholder values. A strong relationship with the shareholders can support competitiveness and improve the organisation's status directly through the correct perception of the shareholders (Andrija 2017, p. 135). Godfrey, Merrill and Hansen (2009, p. 425) asserted that there is a connection between the execution of CSR activities and the perception of the shareholders. Implementing CSR activities can bring considerable benefits such as risk management, human resource management, customer relations and business innovation (Akinbowale, Klingelhöfer & Zerihun 2022b). There exists a link between

MCS and CSR. The connection between MCS and CSR is that MCS can assist in the planning and implementation of CSR activities (Arjaliès & Mundy 2013; Jamali & Neville 2011; Khojastehpour & Johns 2014; Kornfeldova 2011; Kornfeldova & Myskova 2012; Uvaneswaran, Zemen & Ahmed 2019). Rodgers, Söderbom and Guiral (2014) indicate that CSR and enhanced control systems can reduce the likelihood of fraud.

Good corporate governance, CSR and compliance with relevant regulations (an organisation's ability to adhere strictly to the rules and regulations guiding its establishment) are key to a successful organisation. They are directly related to both FA and MCSs. Corporate governance refers to how an organisation's affairs are directed and controlled. At the same time, CSR is a model in which business organisations consider societal interest by taking responsibility for the effect of their production or business on the host and business environment. The business environment encompasses the suppliers, customers, employees, shareholders, communities and other stakeholders (Ismail 2009, p. 199).

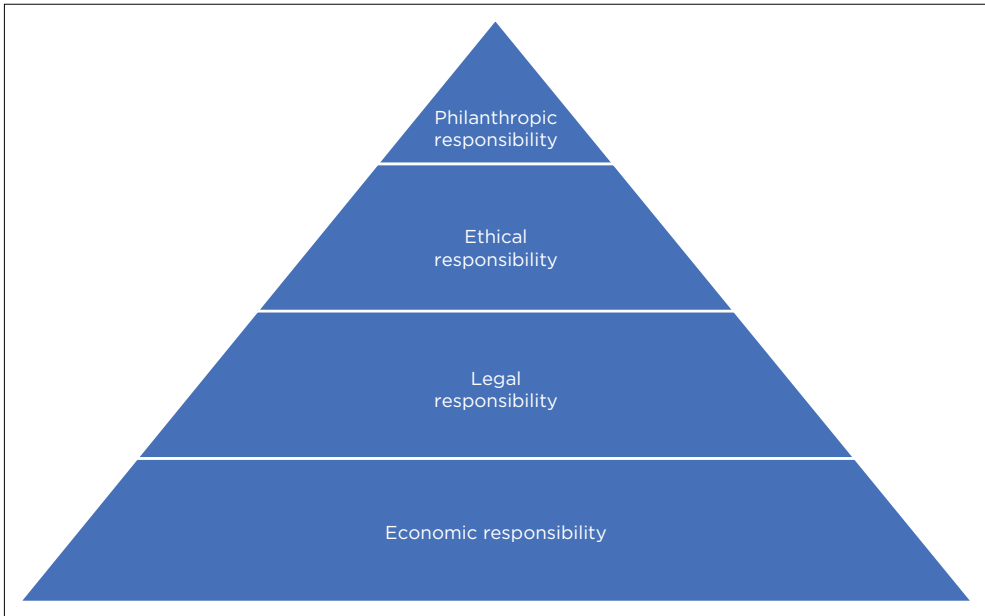
Forensic accounting involves investigating suspected fraud cases and detecting and preventing fraudulent activities to ensure proper information security. At the same time, MCSs focus on ensuring that an organisation's resources are effectively and efficiently employed to achieve organisational goals. However, while ensuring the goals are accomplished, MCS considers various functions such as risk assessments and control, transaction monitoring, supervision of resource allocation within the organisation (this is to avoid wastage and enable effectiveness and efficiency) and evaluation of managerial performance towards the accomplishment of organisation goal. The practical application of FA and MCSs in an organisation could bring about good corporate governance, promote CSR (with reputation as a significant subset), ensure compliance to relevant regulatory frameworks and minimise loss of revenue to cyberfraud threat, thereby uprooting reputation jeopardy.

Three significant theories of CSR include the Carroll theory, the triple bottom-line theory and the stakeholder theory.

■ The Carroll theory

This theory was proposed by Archie Carroll (1991, 2016). It emphasises four business organisation obligations, represented by a pyramid (Figure 3.9). These are economic, legal, ethical and philanthropic responsibilities.

As shown in Figure 3.9, economic responsibility occupied the baseline of the pyramid. This is because any business organisation's bottom-line is necessary for business survival and to reward the stakeholders. Next to



Source: Adapted from Carroll (1991, 2016).

FIGURE 3.9: Carroll's theory of corporate social responsibility.

this, in order of importance, is the legal responsibility. According to Carroll (1991), business organisations must comply with the laws and regulations guiding their operations. A responsible business organisation must be good citizens. They should imbibe the principles of fair business dealings as this will positively impact society and the economy. Next in the hierarchy of importance is ethical responsibility, which stresses that business organisations must abide by ethical standards so that their activities will not harm society. Business organisations must be fair in their dealings with the host community.

Finally, philanthropic responsibility is a voluntary activity guided by the organisation's desire to contribute to meeting society's needs. Although the law may not mandate this, it is a way of giving back to society and alleviating societal pressures. This can promote the image and reputation of the organisation. The Carroll pyramid theory of CSR emphasises that business organisations must first achieve their economic objective and commit to laws and ethical regulations before contributing meaningfully to society. Visser (2012) indicates that in developing countries, emphasis is usually placed on economic responsibility followed by philanthropic responsibility before legal and ethical obligations. Thus, the nature of the host environment and its needs must be adequately identified and defined before the Carroll theory of CSR can be successfully implemented.

□ Triple bottom-line theory

This theory was propounded by John Elkington (1997). It specifies that achieving effective balance among three CSR dimensions – specifically, the economic, social and environmental – is necessary for achieving an organisation’s sustainability. The theory further advocates that the organisation’s financial status may not necessarily be high but must be continuous and sustainable. Furthermore, regarding the social dimension, business organisations must consider societal needs while considering their financial capability. For the environmental dimension, the theory emphasises the need for business organisations to pay attention to the environment and obey environmental laws to enhance people’s quality of life. This theory emphasises that the three CSR dimensions can be achieved simultaneously (not achieving one at the detriment of the other). However, the major limitation of this theory lies in the fact that it may be challenging to balance the three dimensions and each dimension’s contribution to the overall organisation’s sustainability may be difficult to measure.

□ Stakeholders’ theory

This theory was propounded by Freeman (2010). The theory proposes that an organisation’s objective can be achieved effectively by protecting the stakeholders’ interests. The theory stresses the need for the inclusion and participation of the stakeholders in an organisation’s strategic decision-making processes relating to CSR implementation. The theory connects the stakeholders to the management and the CSR approach used by the organisation.

Table 3.2 summarises the three major CSR theories’ strengths, weaknesses and benefits.

□ Forensic accounting

The increasing rates of fraud-related cases in many countries necessitate increased demand for FA (Okoye & Akamobi 2009, p. 39). Forensic accounting is a field that links the traditional accounting system to the legal framework for fraud investigation. Okoye and Gbegi (2013, p. 4) state that FA can be considered ‘investigative accounting’ or ‘fraud audit’ as it integrates accounting and forensic science for fraud investigation. Forensic experts are investigators and interpreters of evidence and facts in fraud-related matters. The FA field has been widely used for detecting fraud and providing litigation support for the prosecution of the culprits (Gerson, Brolly & Skalak 2011, p. 38). Bassegy and Ahonkhai (2017, p. 57) define it as a combination of accounting principles, investigative techniques, legal procedures and accounting skills in gathering financial information that

TABLE 3.2: Strength, weaknesses and benefits of the three major corporate social responsibility theories.

CSR theory	Strength	Weaknesses	Benefits
Carroll theory	It highlights four critical responsibilities of a business organisation, namely, economic, legal ethics and philanthropic responsibilities	The external environment and its needs must first be identified and defined before adopting this theory	It could promote organisations' profitability, as well as trust and reputation in society
Triple bottom-line theory	It highlights three critical CSR dimensions of a business organisation, namely, economic, social and environmental dimensions	Achieving a balance among these three dimensions and the measurement of the contribution of each dimension to organisation's overall sustainability might be a challenge	It could promote the organisation's sustainability, as well as trust and reputation in society
Stakeholders' theory	Protects the interests of the stakeholders and links the stakeholders to management	Participation of the stakeholders in the strategic decision-making processes relating to CSR may make the decision-making processes complex and time-consuming. Furthermore, harmonising the interests of all the stakeholders could also be challenging	It could promote the trust and loyalty of the stakeholders in the organisation and society

Source: Authors' own work.

Key: CSR, Corporate Social Responsibility.

would serve as evidence and will be acceptable in a court of law (Bassey & Ahonkhai 2017, p. 57). Kasap (2013, p. 124) defined the FA as a field that uses the accounting system as a suitable approach for fraud investigation and deterrence.

Forensic accounting is a division of the accounting field involving accounting principles, auditing, criminology and law. Existing authors have termed FA a scientific method suitable for fraud investigation. It can be used to uncover, analyse and present the outcome of investigated fraud-related matters in an acceptable way to the court of law. Thus, it integrates the principles of accounting, investigation, auditing, and litigation skills for fraud detection (Akabom-Ita 2012, p. 26; Pedneault et al. 2012, p. 3; Yadav & Yadav 2013, p. 1). Howard and Sheetz (2006) and Bhasin (2014, p. 4) argue that an FA process includes the preliminary analysis, acquisition of information or data relating to fraud perpetration, data analysis and interpretation, presentation of the outcome of the investigation, expert opinion and litigation support. During the investigative phase, the rule of evidence is usually followed so that the outcome of the investigation can be acceptable in the court. According to Security and Forensic Studies in Nigeria (2010), addressing the loopholes exploited by the threat actors to commit fraud could be useful if FA is well implemented. Forensic accounting can be employed for fraud mitigation (fraud detection, examination, investigation or analysis and prosecution) (Shimoli 2015, p. 63). Forensic accountants are trained to look beyond the numbers and

deal with the business realities and situations at hand to uncover fraud. By doing this, evidence relating to a suspected fraud case can be gathered, and fraud patterns can be traced (Shimoli 2015, p. 63). Furthermore, FA uses accounting analysis, capable of uncovering fraud cases or the basis for the resolution of fraud disputes (Effiong et al. 2017, p. 787; Hecht & Redmond 2012; Stanbury & Parley-Menzies 2010).

Thus, FA, as a division of the accounting field, has its framework, methodologies and procedures for fraud investigation to obtain a comprehensible and credible result for legal support (Modugu & Anyaduba 2013, p. 287). Houck et al. (2006, p. 68) explain that a forensic accountant critically needs accounting principles and fact-finding skills to detect suspected fraud cases. Smith, Sagafi-Nejad and Wang (2008, p. 18) explained that auditing is limited to identifying errors or omissions, which may sometimes lead to fraud detection. Olaoye and Olanipekun (2018, p. 28) stated that an auditor must examine the accuracy of financial reports, detect misstatements in financial statements and ascertain whether any detected misstatement is an act of error or fraud. Grubor, Ristić and Simeunović (2013, p. 1) explained that FA differs from conventional financial auditing. According to Grubor et al. (2013, p. 1), the auditing process can be used to determine the accuracy and reliability of the financial statement from a sample of transactions by detecting deviations or falsifications. Conversely, the FA process deals with the investigation of suspicious financial reports or transactions using digital forensic tools and techniques (Nigrini 2011, p. 11). However, the emergence of FA addresses the limitation of the auditing process through data acquisition, data analytics, trends of perpetration, identification of the perpetrators and their motivation, as well as provision of experts' opinions and litigation support (Akinbowale, Klingelhöfer & Zerihun 2020). Bhasin (2013, p. 1) supports this notion by stressing that the increase in the demand for forensic accountants is because of widespread financial fraud and the limitation of the scope of the auditing process. Özkul and Pamukçu (2012, p. 19) supported the claim that the increasing number of fraudulent cases is a major cause for FA for in-depth investigation of fraud cases and the analysis of the root causes. It is noteworthy to mention that the field of fraud examination is a subdivision of FA. However, they are somehow related but different. While fraud examinations are strictly related to fraud-related cases and can be carried out by either accountants or nonaccountants, FA encompasses fraud investigation, fraud detection, litigation support and other professional services (Wells 2003, p. 76).

Essentially, the nature and adequacy of the financial information acquired determines the outcome of the fraud investigation process. Other factors that determine the success of a forensic accountant during

fraud investigation include the knowledge, experience and expertise of the forensic accountant. The knowledge of the forensic accountant cuts across the means of evidence gathering and handling processes, the nature of the tools used for the investigation and the legal understanding, among others (Hamdan 2017, p. 1). Some crucial areas where forensic accountants are expected to demonstrate comprehensive knowledge and skills include general accounting principles, the law, criminal behaviour, fraud and computerised systems (Hitchcock 2017, p. 1). Financial institutions can also support FA implementation in their organisation through a well-structured framework or policies for its performance (Olaoye & Olanipekun 2018, p. 28).

Hence, a well-structured system of FA can aid fraud minimisation. Akinbowale et al. (2020, p. 163) mention that the tasks of a forensic accountant when dealing with fraud-related cases can be summarised as accounting, investigation, experts' opinion and litigation support roles (Akinbowale et al. 2020, p. 1263). Forensic accountants can use quantitative and qualitative approaches, digital technologies and data analytics tools to resolve fraud-related matters. However, the choice of the techniques to be employed by a forensic accountant is a function of the investigator's expertise, the organisation's needs and capacity, and the nature of the cases to be resolved.

Forensic accounting has been linked to litigation; this can be seen as an intersection of accounting and law (Özcan 2019, p. 1744). This is because the outcome of a fraud investigation using accounting principles can be taken to court for litigation (Özcan 2019, p. 1744). Part of the litigation support offered by a forensic accountant includes the provision of expert opinions about the outcome of the investigation. Hao (2010, p. 185) explains that FA integrates the legal and accounting frameworks. At the same time, Chattopadhyay (2014, p. 22) agrees that FA principles include all accounting and financial analyses that can assist legal counsel during an investigation. Kwok (2007) and Akinbowale et al. (2020) explain that the process of FA consists of several phases such as fraud identification, evidence gathering, investigation, evidence recording, extraction and sorting of evidence, data analysis, inference deduction, reporting, and verification of financial information, presentation of evidence and litigation support.

Golden et al. (2006, p. 3) state that a forensic accountant's core requirements include a comprehensive understanding of financial, accounting, and legal frameworks. The understanding and expertise are employed for fraud prevention, detection, investigation and litigation. A forensic accountant usually specialises in dispute resolution, including fraud cases, through investigation and analysis of evidence (Golden et al. 2006, p. 3). Forensic accounting may also perform cross-examination and third-party inquiries where necessary (Golden et al. 2006, p. 3).

Hence, the roles of FA in fraud resolution have been identified as detection, investigation and litigation (Curtis 2007, p. 538; Golden et al. 2006, p. 22).

Furthermore, the investigative role of FA includes data gathering, interviews, report writing, provision of expert opinions, expert witness in the court and provision of comprehensive information regarding financial fraud cases (Efosa & Kingsley 2016, p. 245; Eliezer & Emmanuel 2015, p. 17; Singleton & Singleton 2010). This means that the FA investigative role involves using financial and accounting information and other expertise to uncover fraud and provide evidence for litigation. The aspect of fraud examination in FA is broad. It comprises fraud examination, comprehensive reviews, risk assessment, detection of financial statement misstatements and reporting (Smith & Crumbley 2009, p. 66).

Okoye and Gbegi (2013, p. 135) emphasised that forensic accountants are professionals in fraud detection, investigation, and documentation of the evidence necessary to prosecute the culprits. Forensic accountants can also perform essential roles relating to fraud or insurance claims, using their financial inclinations (Hassan & Morteza 2012, p. 1). However, according to Shaheen et al. (2014, p. 172), the following components constitute the roles of forensic accountants as they relate to fraud-related matters:

- legal support
- administrative support
- expert witness
- investigation of professional negligence
- mediation and arbitration
- criminal investigation
- fraud investigation.

■ Forensic accounting theory

According to Ozili (2020, p. 5), the theory of FA deals with how accounting and nonaccounting decisions are made during all the phases of the fraud investigation process. It also probes how the accounting and nonaccounting decisions influence the choice of forensic techniques or tools used and the outcome of the investigation (Ozili 2020).

The theory explains the methods, tools and techniques used to detect fraud. The theory states that the accounting and nonaccounting decisions before, during and after a fraud investigation consider the forensic techniques and methods employed.

In other words, selecting the proper forensic detection technique is a function of the forensic accountant's knowledge, experience and expertise, as well as accounting and nonaccounting considerations during the various phases of fraud detection. The core principle of this selection

process is that for a forensic accountant to select the investigation techniques, such an investigator must consider their expertise in accounting and nonaccounting issues during the fraud investigation processes (Ozili 2020, p. 5). The theory further suggests that the outcome of the FA investigation is partly a function of the considerations. The theory is premised on the following assumptions: the forensic investigation's main objective is fraud detection with corrective measures, not retaliatory measures taken against the culprit. The theory also indicates that recommendations on deterrent actions to forestall future occurrences, based on the outcome of a forensic investigation, should be provided, which will not lead to the ruin of the organisation or the culprit (Ozili 2020, pp. 5-6).

One of the benefits of this theory is that it eliminates the forensic accountant's personal sentiments or biases from affecting the investigation's outcome (Ozili 2020, pp. 5-6). Existing works such as Clayton et al. (2006, p. 385) and Gbegi and Adebisi (2014, p. 243) also support this theory that the selection of the right FA tool or technique is a function of the forensic investigator's skills and expertise and may affect the outcome of the investigation process. The process of uncovering fraud in financial institutions partly depends on the expertise of the forensic accountant. The dynamic nature of fraud schemes and accounting methods and policies often makes fraud detection processes challenging (Ozili 2020, p. 2). Thus, the combination of the forensic accountant's knowledge, experience, skill, and expertise plays a significant role in fraud detection. Hamdan (2017, pp. 1-2) states that the success of FA investigation depends on the investigator's expertise and knowledge, the nature of the tools employed and the evidence gathered. Hitchcock (2017, p. 1) indicates that forensic investigators must be skillful in fraud, accounting principles, data analysis, investigation, and litigation processes. This theory can be used to identify the required skills needed by a forensic accountant for cyberfraud investigation. It can also be used to determine the proper technique or tool for cyberfraud based on the nature of the fraud case and the investigator's expertise.

In addition, implementing FA requires good quality and control measures. Hauser (2006, p. 512) indicates that an organisation can achieve significant assurance via quality control. This control includes regulatory compliance, standards adherence and ethical codes of conduct. According to Magrath and Weld (2002, p. 53), quality standards present facts to third parties that the proper steps have been observed to accomplish a robust investigation. Whenever there is a breach in the legal or ethical code of conduct of FA, the admissibility of the outcome of the investigation or evidence provided may suffer a setback in the court.

■ Conclusion

The general fraud and cyberfraud theories discussed in this chapter identify and examine the significant factors influencing fraud perpetration under different circumstances. The theoretical assumptions can further enhance the understanding of various concepts of fraud management to devise sustainable measures to mitigate the identified fraud causes. The theoretical frameworks discussed in this chapter assist in fraud profiling. It provides an in-depth understanding of the characteristics of fraud, the fraudsters and their fraud. This chapter addresses three main areas that relate to fraud profiling. First is the methods employed by the fraudsters, and the second is the characteristics of the fraudsters, including the rationale, motivation and justification for fraud perpetration. Finally, the probable causes of fraud were also addressed. The theoretical concepts discussed can assist in profiling the fraud perpetrators and the mitigation measures the target organisations might implement. This chapter's significant contributions include the definition of fraud profiling and an in-depth explanation of the theoretical framework's main elements, relationships and application to fraud profiling. The theoretical frameworks may be helpful to the target organisation and law enforcement agencies in fraud mitigation.

Cyberfraud mitigation decision-making: From theory to application

■ Introduction

In their quest to mitigate cyberfraud, financial institutions may employ a few approaches. Determining the impact of the cyberfraud mitigating approaches represents a multicriteria decision (MCD) problem requiring a scientific approach to justify. This chapter aims to evaluate the effect of the organisation's cyberfraud mitigation approaches in the order of priorities. To achieve this, the fuzzy analytical hierarchy process (FAHP) is employed for the expression of the elements of the pairwise comparison matrices by triangular fuzzy elements. In addition, calculating the weights of the fuzzy comparison matrices was carried out using classical nonfuzzy methods such as the eigenvectors and the geometric approach. Three hypothetical companies are considered with their cyberfraud mitigating strategies in the order of their priorities. The findings indicated that the mitigation approaches considered by Companies 1 and 2 in the order of their priorities reflect positively in their efforts against cyberfraud, although to a varying

degree compared to Company 3. One of the limitations of this study is that the mitigation approaches considered as the criteria and their order of priorities for the three hypothetical firms are based on the authors' thoughts grounded on the information from the literature. However, this chapter provides a procedural step for implementing the FAHP methodology for evaluating the impact of organisations' cyberfraud mitigation approaches in the order of priorities. This may assist financial institutions in resolving MCD problems relating to cyberfraud mitigation.

Determining the impact of cyberfraud mitigating approaches in the financial sector represents an MCD problem requiring a scientific approach. An MCD problem aims to identify the best alternative amid feasible solutions and competing criteria (Akinbowale, Klingelhöfer & Zerihun 2022a). Many approaches can be deployed to mitigate cyberfraud. Based on the peculiarity of the business environment and the overall organisation's goal of cyberfraud mitigation, an MCD analysis can assist an organisation in selecting the most feasible approach. Sometimes, MCD analysis can identify some factors requiring trade-offs so an organisation can make an informed decision. Given this, the chapter demonstrates the use of the FAHP to assist financial institutions in making an informed decision about mitigating cyberfraud. The selection of the FAHP was informed by the fact that it employs a range of values known as fuzzy numbers to address the ambiguity, bias, imprecision uncertainty and subjectivity in the decision-making process relating to the allocation of weights (Alyamani & Long 2020; Li et al. 2016). Thus, the subjectivity, bias and inconsistency in the judgement of the decision-makers as it relates to the allocation of weights to the competing factors and criteria are reduced.

Furthermore, the FAHP technique offers a scientific and mathematical approach to structuring and solving multicriteria problems. In addition, FAHP also allows for the comparative analysis of the alternatives to make an informed decision.

■ Cyberfraud mitigating approaches from the theoretical perspectives

Table 4.1 presents the suggested approaches for mitigating cyberfraud. These approaches or strategies are obtained from synthesising some existing studies and reports. The strategies are grouped into five categories, as presented in Table 4.1.

TABLE 4.1: Suggested approaches for mitigating cyberfraud.

Cyberfraud mitigating approaches	Description	References
Development of a robust internal control	Close monitoring and supervision of transactions and system control. Creating alert systems on different forms of systems; awareness and sensitisation of the customers, employees and public; human capacity development geared towards fraud mitigation; effective design and implementation of cyberfraud risk mitigation; and response plans, multi-factor authentication, implementation of transaction limits, use of threat detection tools, robust real-time incidence response and use of third-party risk management, among others.	Shahabuddin, Alam and Azad (2011); Prabowo (2011); Dellaportas (2013); Schuchter and Levi (2013); Oguda, Odhiambo and Byaruhanga (2015); Mohd-Sanusi et al. (2015); Zakaria, Nawawi and Salin (2016); Andoh, Quaye and Akomea-Frimpong (2017); Kamande et al. (2017)
Cyber, system and information security	Encryption, use of security or anti-cyberfraud software such as firewalls and data protection software, network access control, security and network monitoring	Lebanidze (2011); Primer (2016); Sutherland (2017); Tariq (2018); Plier (2020)
Synergy among anti-fraud capacities at all levels (local, national, regional, continental and international)	Working with other companies, such as network-providing companies. Reinforcement and collaboration among all existing security apparatus, intelligent systems, regulators and anti-fraud capacities.	Dlamini and Modise (2012); Cassim (2011); Obeng-Adjei (2017); UK Finance (2018); Gumbi (2017)
Use of digital technologies and data analytics	Use of real-time technologies such as artificial intelligence and blockchain technologies	Herselman and Warren (2004); Kenyon and Tilton (2011); Decker et al. (2011); Akinbowale et al. (2020); Lombardi et al. (2021)

Source: Authors' own work.

Methodology: Cyberfraud mitigation using the fuzzy analytical hierarchy process

This chapter employs the FAHP, having a pairwise comparison matrix whose elements are expressed by triangular fuzzy elements. This approach represents a fuzzified form of the analytic hierarchy process (AHP) developed by Saaty (1980).

Moreover, in this chapter, the weights of the fuzzy comparison matrices were calculated using classical nonfuzzy methods such as the eigenvectors and the geometric approach.

Like the AHP, the FAHP is also an MCD technique but with reduced probability for bias and subjectivity. The FAHP was applied to evaluate the impact of an organisation's cyberfraud mitigation approaches.

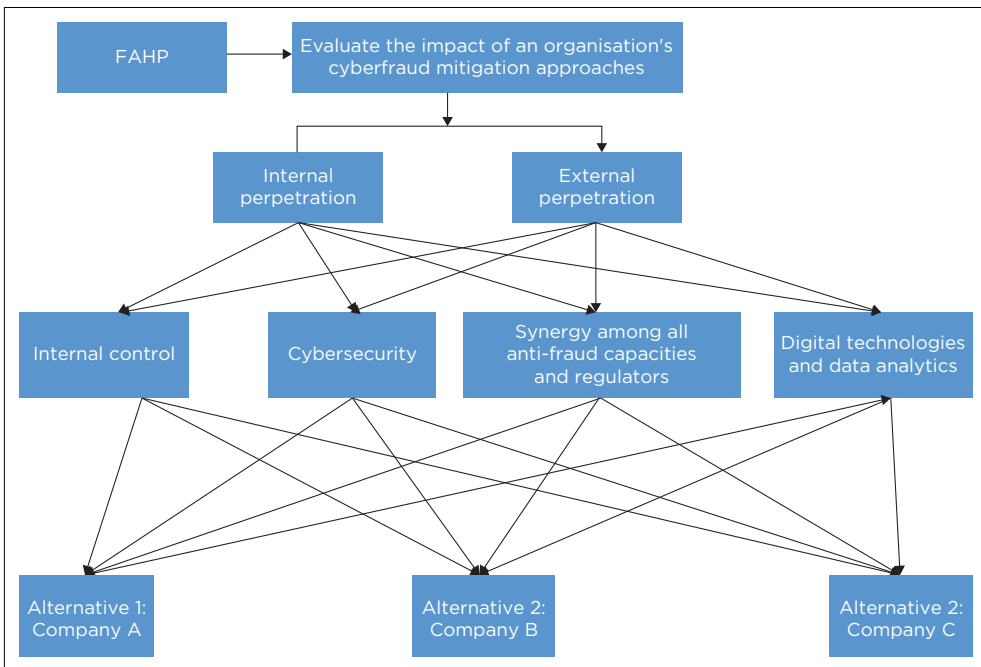
The FAHP allows pairwise comparisons of the competing factors, enhancing effective decision-making by comparing alternatives to facilitate decision.

The FAHP has a triangular fuzzy number (TFN) of three variables (l, m, u). Equation 4.1 defines the membership function ($\mu_A(x)$) of these three variables (Alyamani & Long 2020):

$$\mu_A(x) = \begin{cases} 0 & x < l \\ \frac{x-l}{m-l} & l \leq x \leq m \\ \frac{x-u}{m-u} & m \leq x \leq u \\ 0 & x > u \end{cases} \quad \text{[Eqn 4.1]}$$

where l represents the lowest value, m represents the middle value and u depicts the highest possible value. The following are the procedural steps for the FAHP implementation for decision-making relating to cyberfraud mitigation.

Step 1: The first step is defining the MCD to be solved and establishing the goal and criteria for the FAHP goal model. This encompasses identifying the overall goal, criteria or factors, as shown in Figure 4.1. The criteria are extracted from the various theories and literature presented in Table 4.1. Through the FAHP, this chapter evaluates the impacts of cyberfraud



Key: FAHP, fuzzy analytical hierarchy process.

FIGURE 4.1: Fuzzy analytical hierarchy process hierarchy structure.

mitigation approaches from the internal and external perspectives using three organisations (alternatives) as an example. Cyberfraud can take place internally by internal employees because of ethical breaches. Internal employees can take undue advantage of the knowledge of the internal control structure and access to customers' and organisation information to perpetrate cyberfraud. Internal employees may also collude with external perpetrators by supplying the confidential information external threat actors need to commit cyberfraud. Conversely, cyberfraud perpetration can be purely an external affair without any input from internal employees.

Step 2: Decomposition of the MCD problem into a structure. After that, the pairwise comparison of the weights of the criteria or factors is carried out. The structuring displays the set of alternatives.

This is followed by the pairwise comparison of the weights allocated to the competing factors or criteria using the linguistic scale having three variables l , m and u . This is presented in Table 4.2.

Table 4.3 presents the competing criteria. Criterion 1 (internal control) is considered to be of weak importance compared to Criteria 2 and 3 (cybersecurity and synergy among all anti-fraud capacities and regulators). Thus, Criterion 1 is assigned a TFN value of (2 3 4). Criteria 2 and 3 are considered less critical than Criterion 4. Take the reciprocal (1/4 1/3 1/2) under the column for the first criterion. Criterion 1 is also considered extremely important over Criterion 4 (digital technologies and data analytics). It is assigned a TFN value of (6 7 8). At the same time, Criterion 4 (digital technologies and data analytics) takes the reciprocal (1/8 1/7 1/6) under the column for the first criterion.

Criterion 2 is considered equally important to Criterion 3. It is assigned a TFN value of (1 1 1), with both having a reciprocal of (1) under the column for the second criterion. Criterion 2 is also considered to be of weak importance over Criterion 4. It is assigned a TFN value of (2 3 4) while Criterion 4 takes the reciprocal (1/4 1/3 1/2) under the column for the second criterion. Furthermore, Criterion 3 is of weak importance over Criterion 4. It is assigned

TABLE 4.2: Fuzzy linguistic scale.

Importance	Linguistic definition	TFN	TFN reciprocal
1	Equal importance	(1 1 1)	(1 1 1)
3	Weak importance	(2 3 4)	(1/4 1/3 1/2)
5	Strong importance	(4 5 6)	(1/6 1/5 1/4)
7	Very strong importance	(6 7 8)	(1/8 1/7 1/6)
9	Absolute importance	(9 9 9)	(1/9 1/9 1/9)
2, 4, 6, 8	Intermediate scales	(1 2 3) (3 4 5) (5 6 7) (7 8 9)	(1/3 1/2 1) (1/5 1/4 1/3) (1/7 1/6 1/5) (1/9 1/8 1/7)

Source: Saaty (1980).

Key: TFN, triangular fuzzy number.

a TFN value of (2 3 4), while Criterion 4 takes the reciprocal (1/4 1/3 1/2) under the column for the third criterion.

Table 4.3 presents the impact of the criteria and the assigned TFNs.

There are three options (alternatives): Company 1, 2 and y. Table 4.4 shows the assigned TFNs for assessing Criterion 1 (internal control) concerning the three options (Companies 1, 2 and 3, respectively), while Tables 4.5–4.8 present the assessment of each criterion with the options.

For Criterion 1 (internal control), Company 1 is considered weak to Company 2 but extremely important to Company 3. Company 2 is deemed to be of substantial importance to Company 3. Their assigned TFNs and their reciprocals are highlighted in Table 4.4.

For cybersecurity, Company 1 is of weak importance to Company 2 but of strong importance to Company 3. Company 2 is also considered to be of weak importance to Company 3. Their assigned TFNs and their reciprocals are highlighted in Table 4.5.

For the third criterion (synergy among all anti-fraud capacities and regulators), Company 1 is equally essential to Company 2 but weak to Company 3. Conversely, Company 2 is of very strong importance to Company 3. Their assigned TFNs and their reciprocals are highlighted in Table 4.6.

For the fourth criterion (use of digital technologies and data analytics), Company 1 is considered to be of weak importance to Company 2 but of strong importance to Company 3. Conversely, Company 2 is deemed

TABLE 4.3: Impact of the criteria and the assigned triangular fuzzy numbers.

Criteria	Internal control	Cybersecurity	Synergy among all anti-fraud capacities and regulators	Digital technologies and data analytics
Criterion 1: Internal control	1	2 3 4	2 3 4	6 7 8
Criterion 2: Cybersecurity	1/4 1/3 1/2	1	1	2 3 4
Criterion 3: Synergy among all anti-fraud capacities and regulators	1/4 1/3 1/2	1	1	2 3 4
Criterion 4: Digital technologies and data analytics	1/8 1/7 1/6	1/4 1/3 1/2	1/4 1/3 1/2	1

TABLE 4.4: Assessment of Criterion 1 (internal control) with respect to the three options (alternatives).

Companies	Company 1	Company 2	Company 3
Company 1	1	2 3 4	6 7 8
Company 2	1/4 1/3 1/2	1	4 5 6
Company 3	1/8 1/7 1/6	1/6 1/5 1/4	1

TABLE 4.5: Assessment of Criterion 2 (cybersecurity) with respect to the three options (alternatives).

Companies	Company 1	Company 2	Company 3
Company 1	1	2 3 4	4 5 6
Company 2	1/4 1/3 1/2	1	2 3 4
Company 3	1/6 1/5 1/4	1/4 1/3 1/2	1

TABLE 4.6: Assessment of Criterion 3 (synergy among all anti-fraud capacities and regulators) with respect to the three options (alternatives).

Companies	Company 1	Company 2	Company 3
Company 1	1	1	2 3 4
Company 2	1	1	6 7 8
Company 3	1/4 1/3 1/2	1/8 1/7 1/6	1

TABLE 4.7: Assessment of Criterion 4 (use of digital technologies and data analytics) with respect to the three options (alternatives).

Companies	Company 1	Company 2	Company 3
Company 1	1	2 3 4	4 5 6
Company 2	1/4 1/3 1/2	1	1
Company 3	1/6 1/5 1/4	1	1

equally significant to Company 3 as presented in their assigned TFNs and their reciprocals in Table 4.7.

Step 3: Determination of the geometric mean (\tilde{r}) value (Equation 4.2) (Burney & Ali 2019).

$$\tilde{r} = \left(\prod_{i=1}^n m_{ij} \right)^{\frac{1}{n}}, i = 1, 2, \dots, n \quad [\text{Eqn 4.2}]$$

Step 4: Computation of the weight of each criterion (Equation 4.3) (Burney & Ali 2019).

$$\tilde{w} = \tilde{r} \times \left(\sum_{i=1}^n \tilde{r} \right)^{-1}, i = 1, 2, \dots, n \quad [\text{Eqn 4.3}]$$

Step 5: Defuzzification of the calculated weight in Step 2 above (Equation 4.4) (Khan et al. 2017).

$$w = \frac{w_{lij} + w_{mij} + w_{uij}}{3} \quad [\text{Eqn 4.4}]$$

Step 6: Normalisation of the defuzzified weight (Equation 4.5) (Khan et al. 2017).

$$w_n = \frac{w}{\sum_{i=1}^n w} \quad [\text{Eqn 4.5}]$$

■ Results and discussion

Table 4.8 presents the eigenvector and geometric mean of the various criteria instead of the options (alternatives). The results indicated a significant agreement between the eigenvector values and the geometric mean. This justifies that the weight allocation and the pairwise comparison are reliable.

Table 4.9 displays the maximum eigenvector (λ_{max}), consistency index (CI), random index (RI) and consistency ratio (CR). The table also indicates that the pairwise comparison is reliable. This is justified by the high consistency level, as evidenced by the CR that is less than 10% (CR < 10%) (Saaty 2008). When the CR exceeds 10%, there is a need to re-assign the weights and re-calculate the CR (Akinbowale, Klingelhöfer & Zerihun 2022b).

Figure 4.2 shows the triangular fuzzy elements computation for the criteria. Figure 4.2 shows that Criterion 1 (internal controls) takes precedence over other criteria, followed by Criteria 2 and 3 (cybersecurity and synergy

TABLE 4.8: The values of the eigenvector and geometric mean for the criteria.

Criteria	Eigenvector	Geometric mean
Criterion 1 (Internal control)	0.545	0.545
Criterion 2 (Cybersecurity)	0.193	0.193
Criterion 3 (Synergy among all anti-fraud capacities and regulators)	0.193	0.193
Criterion 4 (Digital technologies and data analytics)	0.069	0.069
Criterion 1 with respect to the three alternatives, respectively (1)	0.649	0.649
-2	0.279	0.279
-3	0.072	0.072
Criterion 2 with respect to the three alternatives, respectively (1)	0.637	0.637
-2	0.258	0.258
-3	0.105	0.105
Criterion 3 with respect to the three alternatives, respectively (1)	0.488	0.388
-2	0.575	0.575
-3	0.097	0.097
Criterion 4 with respect to the three alternatives respectively (1)	0.659	0.659
-2	0.185	0.185
-3	0.156	0.156

TABLE 4.9: Consistency indices for the pairwise comparison process.

Criteria	λ_{max}	CI	RI	CR	Remarks
Four criteria	4.008	0.003	0.089	0.003	Consistency is high
Criterion 1 with respect to the alternatives	3.065	0.032	0.520	0.062	Consistency is high
Criterion 2 with respect to the alternatives	3.039	0.019	0.520	0.037	Consistency is high
Criterion 3 with respect to the alternatives	3.080	0.050	0.520	0.077	Consistency is high
Criterion 4 with respect to the alternatives	3.029	0.015	0.520	0.028	Consistency is high

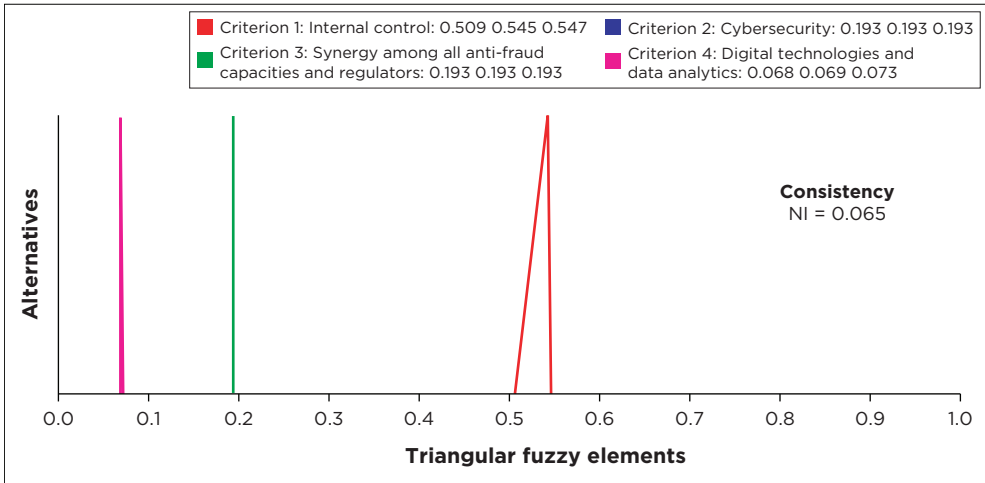
Key: CI, consistency index; RI, random index; CR, consistency ratio.

among all anti-fraud capacities and regulators, respectively). In contrast, Criterion 4 (digital technologies and data analytics) has the lowest triangular weight assigned. The reason for the high triangular weight of Criterion 1 (internal controls) was that in the hypothetical companies used as an example in this chapter, preference was given to the allocation of weights in the order of importance compared to other weights. The reason is that it is believed that the primary responsibility of cyberfraud mitigation rests on the organisation's internal control structure. Concerning fraud mitigation, existing studies have indicated that an organisation's internal control structure is saddled with the following activities (Andoh et al. 2017; Dellaportas 2013; Kamande et al. 2017; Mohd-Sanusi et al. 2015; Oguda et al. 2015; Prabowo 2011; Schuchter & Levi 2013; Shahabuddin et al. 2011; Zakaria et al. 2016):

- gathering of intelligence reports
- periodic auditing and performance measurement
- close supervision and monitoring of staff and transactions
- implementation of anti-fraud programs and control of fraud risk management
- sensitisation and education of the employees, customers and public
- promotion of a good organisation's culture to mitigate the potential causes of fraud
- effective risk assessment, proper information and communication controls
- information control
- human capacity development
- collaboration with stakeholders.

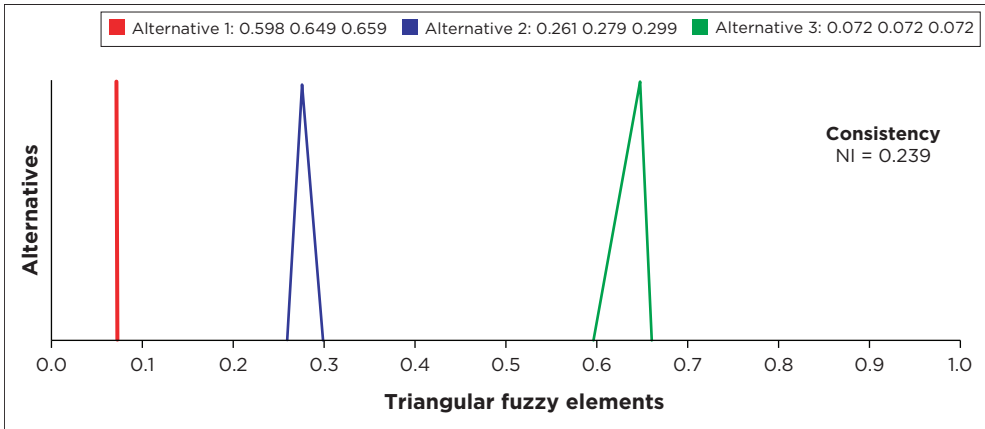
Cybersecurity's triangular weight comes second in the hierarchy. Dlamini and Modise (2012) explained that the South African banking industry must prioritise cybersecurity to combat cyberfraud effectively. The emergence and implementation of a national cybersecurity policy in South Africa will further promote cybersecurity awareness. The Association of Certified Fraud Examiners (2012a) also explained that cybersecurity is the first defence against cyberfraud. Drawing from the literature, it was established that fraud-related cases could be minimised with effective cybersecurity (Lebanidze 2011; Tariq 2018).

Figures 4.3–4.6 show the triangular fuzzy elements evaluation of each criterion in relation to the options (alternatives). The figures indicate the priorities of the hypothetical companies concerning the four criteria (internal control, cybersecurity, synergy among all anti-fraud capacities and use of digital technologies and data analytics). Table 4.10 presents the summary of the companies with respect to these four criteria.



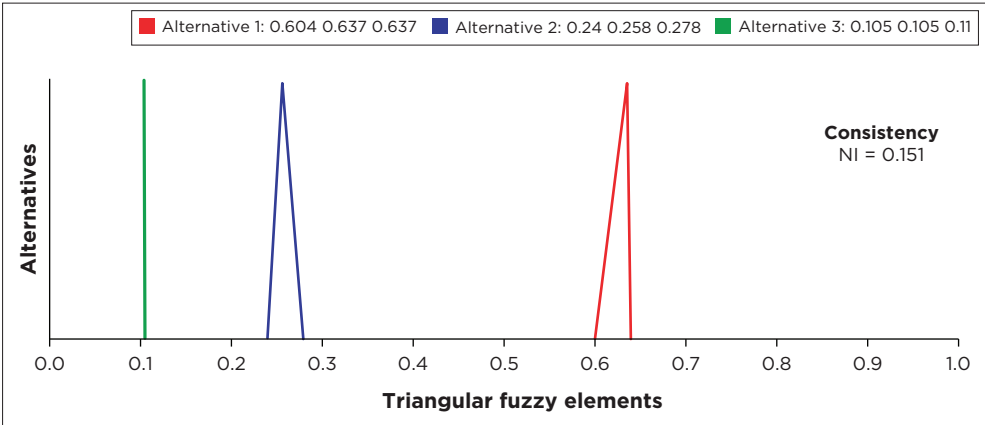
Source: Authors' own work.

FIGURE 4.2: Triangular fuzzy elements computation for the criteria.



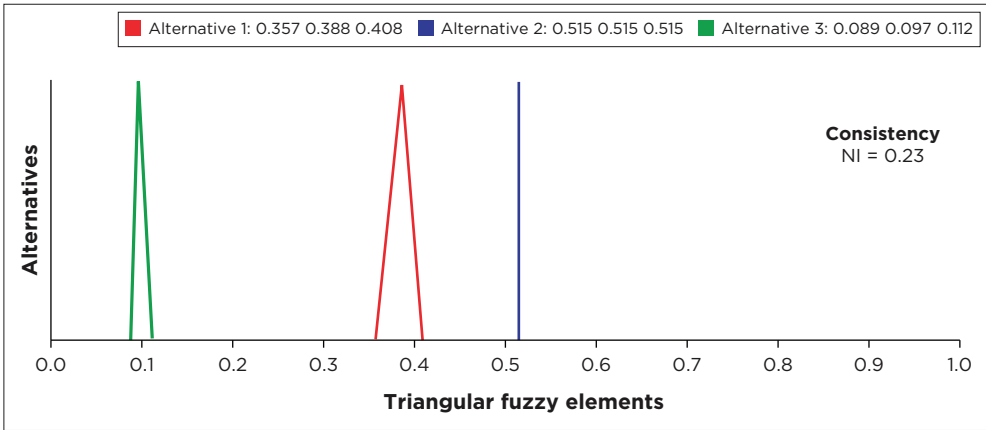
Source: Authors' own work.

FIGURE 4.3: Criterion 1 triangular fuzzy elements (internal control) with respect to the options (alternatives).



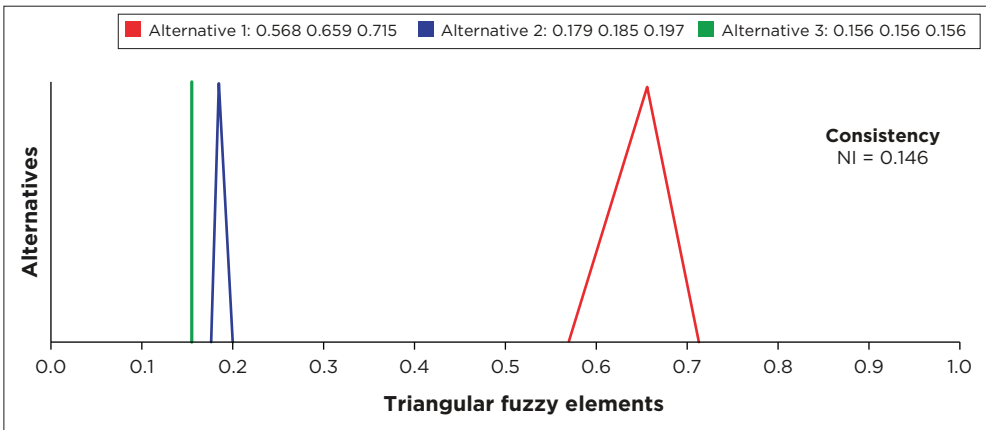
Source: Authors' own work.

FIGURE 4.4: Criterion 2 triangular fuzzy elements (cybersecurity) with respect to the options (alternatives).



Source: Authors' own work.

FIGURE 4.5: Criterion 3 triangular fuzzy elements (synergy among all anti-fraud capacities and regulators) with respect to the options (alternatives).



Source: Authors' own work.

FIGURE 4.6: Criterion 4 triangular fuzzy elements (digital technologies and data analytics) in relation to the alternatives.

TABLE 4.10: Summary of the companies with respect to the four criteria.

Company	1st priority	2nd priority	3rd priority	4th priority
Alternative 1	Internal control	Cybersecurity	Use of digital technologies and data analytics	Synergy among all anti-fraud capacities
Alternative 2	Synergy among all anti-fraud capacities	Internal control	Cybersecurity	Use of digital technologies and data analytics
Alternative 3	Use of digital technologies and data analytics	Cybersecurity	Synergy among all anti-fraud capacities	Internal control

Careful consideration and balance among these four criteria are needed to combat and sustain the fight against cyberfraud effectively. From the perceived importance and the weights allocated to the criteria in this example, Company 1 seems to have a better approach to combatting cyberfraud, as reflected in the defuzzified and normalised weights of the company compared to other companies. This is followed by Company 2, and the priorities of Company 3 seem to have a lesser impact on the fight against cyberfraud than Companies 1 and 2.

Table 4.11 highlights the defuzzified and normalised weights of the criteria. In contrast, the defuzzified and normalised weights of the options are highlighted in Table 4.12.

Figure 4.7 shows the normalised weights of the options (alternatives) in relation to the criteria. The result indicates that for option 1 (Company 1), the influence of the combination of the criteria in the order of their priorities has the highest impact on the fight against cyberfraud, followed by Company 2. On the contrary, the effect of the combination of the criteria in the order of their priorities has the most negligible impact on the fight against cyberfraud for Company 3.

TABLE 4.11: Defuzzified and normalised weights of the criteria.

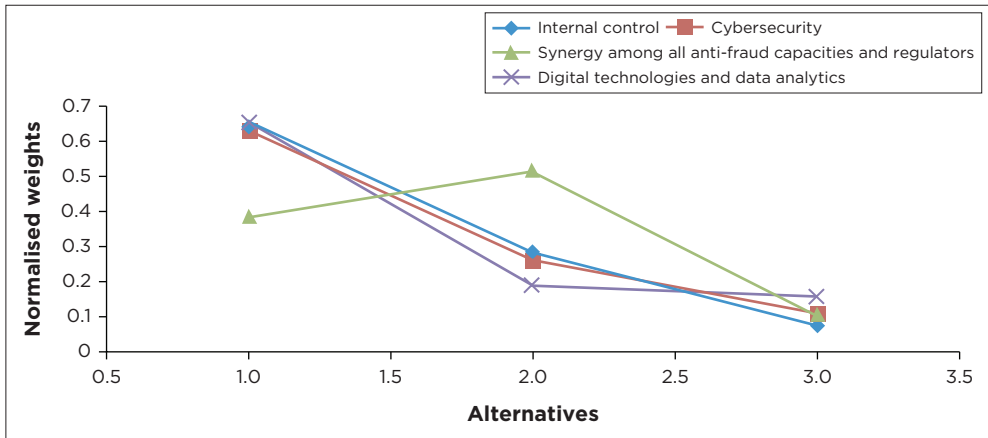
Cyberfraud mitigation approaches	Lowest possible value (<i>l</i>)	Modal value (<i>m</i>)	Highest possible value (<i>u</i>)	Defuzzified weight	Normalised weight
Internal control	0.509	0.545	0.547	0.525	0.535
Cybersecurity	0.193	0.193	0.193	0.193	0.197
Synergy among all anti-fraud capacities and regulators	0.193	0.193	0.193	0.193	0.197
Digital technologies and data analytics	0.068	0.069	0.073	0.07	0.071

Source: Authors' own work.

TABLE 4.12: Defuzzified and normalised weights of the alternatives.

Criteria	Alternatives	Lowest possible value (<i>l</i>)	Modal value (<i>m</i>)	Highest possible value (<i>u</i>)	Defuzzified weight	Normalised weight
Internal control	1	0.598	0.649	0.659	0.635	0.645
	2	0.261	0.279	0.299	0.280	0.283
	3	0.072	0.072	0.072	0.072	0.073
Cybersecurity	1	0.604	0.637	0.637	0.626	0.631
	2	0.240	0.258	0.278	0.259	0.261
	3	0.105	0.105	0.111	0.107	0.108
Synergy among all anti-fraud capacities and regulators	1	0.357	0.388	0.408	0.384	0.385
	2	0.515	0.515	0.515	0.515	0.516
	3	0.089	0.097	0.112	0.099	0.099
Digital technologies and data analytics	1	0.568	0.659	0.715	0.647	0.654
	2	0.179	0.185	0.197	0.187	0.189
	3	0.156	0.156	0.156	0.156	0.158

Source: Authors' own work.



Source: Authors' own work.

FIGURE 4.7: Normalised weights of the options (alternatives) in relation to the identified criteria.

Concerning the question: How do an organisation's cyberfraud mitigation approaches impact the fight against cyberfraud? From the example provided in this chapter, the mitigation approaches considered by Companies 1 and 2 in the order of their priorities reflect positively in their efforts against cyberfraud, although to a varying degree compared to Company 3. The findings in this study can provide valuable insights to organisations on the combination of the proper mitigation approaches in the correct order of priorities to promote an effective and sustainable fight against cyberfraud. The study identifies the order of importance of the three companies used as an example. This study can assist organisations in identifying the areas that need to be prioritised for effective cyberfraud mitigation. The results obtained agree with the literature to a certain extent.

■ Conclusion

This chapter ranked the impact of organisation's cyberfraud mitigation approaches in their order of priorities. The FAHP was used as an MCD technique to achieve this. The expression of the elements of the pairwise comparison matrices by triangular fuzzy elements was first carried out, followed by the calculation of the weights of the fuzzy comparison matrices using the classical nonfuzzy methods such as the eigenvectors and the geometric approach. The outcome of this chapter indicated that the mitigation approaches considered by Companies 1 and 2 in the order of their priorities reflect positively in their efforts against cyberfraud, although to a varying degree compared to Company 3. One of the limitations of this study is that the mitigation approaches considered as the criteria and their order of priorities for the three hypothetical firms are based on the authors'

thoughts grounded on the information from the literature. Nevertheless, this chapter provides a procedural step for implementing the FAHP methodology for ranking competing criteria and factors in the order of their priorities. This may assist organisations in resolving MCD problems relating to cyberfraud mitigation. Further study can use quantitative data sets to evaluate the developed FAHP framework.

Combatting cyberfraud in the digital era: The machine learning approach²

■ Introduction

For effective cyberfraud mitigation in this digital era, machine learning is necessary for data analytics to draw proper inferences from high volumes of data gathered from different sources. Thus, this chapter demonstrates the use of the machine learning approach in solving classification and clustering problems related to cyberfraud mitigation. Firstly, the prevalent forms of cyberfraud were identified from the literature, and fraud risk scores on a probability scale are allocated to them based on their prevalence. For the classifier model, the output target variable denoted as 't' has two rows with the ten values having either [1; 0] for the classification of the identified form of cyberfraud as a high-risk occurrence or [0; 1] for the classification of the identified form of cyberfraud as low-risk occurrences. The training was done under a supervised learning environment with labelled data for the input and target data sets. The input factors were grouped based on their similarities and risk factors for

2. Aspects in some sections in this chapter are based on the author's (and co-authors') reworked article, Oluwatoyin, Mashigo and Zerihun (2023).

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Combatting cyberfraud in the digital era: The machine learning approach', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 93-109. <https://doi.org/10.4102/aosis.2024.BK485.05>

the clustering analysis. The clustering analysis architecture comprises ten input factors and 100 output factors carried out under unsupervised learning to identify some trends or patterns that can lead to cyberfraud. The results indicate that 50% of the identified forms of cyberfraud are classified as high-risk occurrences. These include phishing, online payment fraud, identity theft, credit card fraud and technical support scams. On the contrary, 50% of the identified forms of cyberfraud are classified as low-risk occurrences. These include spoofing, impersonation, ransomware, malware and denial-of-service (DoS) attacks. The clustering analysis indicated the suitability of the unsupervised machine learning approach to detect hidden patterns that may not be visible or detected by manual or other examination techniques. Thus, this chapter demonstrates an implementable real-world approach for applying machine learning under the supervised and unsupervised learning approach for cyberfraud analysis.

Machine learning (ML) combines different computer algorithms that allow computers to understand the relationship inherent in a data set to accomplish a specific task without complex coding (Raghavan & Gayar 2019). Mitchell (1997) states that ML is a field that deals with understanding and building models that 'learn' by leveraging data to improve performance on some set of tasks. Machine learning is essential to the growing field of data technology, whereby specialised algorithms are used to train data sets to make classifications or predictions to uncover hidden relationships and draw critical insights (Alpaydin 2020; Zhang et al. 2011). Machine learning is a division of artificial intelligence and computer science that uses specialised algorithms to train data sets to imitate how humans learn for classification, pattern recognition and prediction tasks. It finds various applications in medicine, engineering, science and social sciences. It is usually suitable for processing vast amounts of big data. Ngai et al. (2011) state that big data can drive the ML approach towards detecting hidden trends, patterns and relationships in large amounts of raw data for effective decision-making (Ngai et al. 2011).

Bishop (2006) and Bengio, Courville and Vincent (2013) indicate that ML is suitable for pattern recognition and analysis. As there are peculiar trends or patterns attributable to fraud and cyberfraud occurrences, using the ML approach in fraud investigation and mitigation may play a decisive role. Thus, ML plays a vital role in fraud investigation. Lack of required skills and expertise around fraud investigation coupled with the use of the wrong ML approach can jeopardise the success of fraud investigation and mitigation. With the emerging digital technologies and the increasingly complex nature of cyberfraud, combining traditional data analytics with ML is necessary. In conventional data analytics, data are acquired and

stored in a centralised database in a fixed format. On the contrary, big data technology is the technology whereby a large amount of data are collected at high velocity and from different sources for analysis to obtain valuable information (De Dott 2020). Fraud investigators need to be kept updated about the recent advances in data analytics to improve the quality of investigation in this digital era. The traditional data analytics techniques are laborious, time-consuming and less effective with big data. A high volume of data from different types gathered from various sources might be difficult to manage effectively with traditional data analytic techniques (McKinsey 2011; Warren, Moffitt & Byrnes 2015). Traditional data analytics is suitable for visualising a limited data set, but ML can handle vast amounts of data. The ML approach can eliminate the rigour of manual work and human error during data analysis. Furthermore, it can detect hidden trends and patterns in data sets and effectively establish relationships between the variables in the data set. Fraud and its investigation are dynamic and complex. With the emerging technologies and increasing digital banking platforms, fraudsters are inventing new schemes to beat the mitigating measures put in place by financial institutions. Thus, this necessitates using a versatile algorithm capable of studying vast amounts of data collected from different sources and identifying anomalies in the data set. Fraud investigators can employ ML in the investigative framework to assist fraud investigators in quickly and effectively identifying and investigating the root causes of fraud incidences and preventing future occurrences. This chapter aims to demonstrate the use of the ML approach for the classification and clustering analysis of the identified forms of cyberfraud.

■ The machine learning approach³

Machine learning is a fusion of various computer algorithms that allows a computer to learn and execute a task without difficulty coding (Raghavan & Gayar 2019). In ML, algorithms are used to train the data sets so that the machine can learn the patterns and relationships in the data set. Based on this, decisions or predictions can be made (Bzdok, Altman & Krzywinski 2017). A rules-based system approach is a knowledge-based approach that uses 'if-then' statements to draw conclusions and decisions based on certain logic (Liu & Cocea 2015). Compared to the rules-based system, the ML approach can quickly identify trends and patterns in multidimensional and multivariate data. It can study historical data, establish variables' relationships and make future predictions. It is also time-effective and

3. Aspects of this chapter are based on the article by Oluwatoyin, Mashigo and Zerihun (2023).

can accelerate the process of fraud detection. In addition, it can be used for clustering and classifying suspected fraud cases as either standard or fraudulent. The ML algorithms can trace or detect hidden transactions and update detected patterns in real time.

Under ML, a data set can be trained under supervised, unsupervised, reinforcement or deep learning environments. For a supervised learning environment, the machine is trained by specialised algorithms to understudy the data set, learn, recognise hidden patterns and make predictions using a labelled data set. A labelled data set is one with input and outputs. Conversely, for the unsupervised learning environment, the machine is trained to understudy the data set, learn, recognise hidden patterns and make predictions using an unlabelled data set (the input data set only). For the reinforcement learning environment, the machine is trained to learn, recognise patterns and make predictions from the unfamiliar data set using a trial and error approach (Van Otterlo & Wiering 2012). Deep learning is a subset of ML, having advanced neural networks inspired by biological neural networks. The neural network has nodes with interconnected layers that communicate with each other to analyse high-volume input data set.

■ Application of the machine learning approach for classification problem⁴

Table 5.1 presents the prevalent form of cybercrime, the average loss, number of victims and total loss for 2021 (AAG 2022a, 2022b). In this example, fraud risk scores on a probability scale are allocated to the identified forms of cybercrime based on their prevalence. The prevalence is expressed by the number of victims affected, presented in the table.

TABLE 5.1: Prevalent forms of cybercrime, the average loss, number of victims and total loss for 2021.

Prevalent forms of cybercrime	Average loss (US\$)	Number of victims (in thousands)	Total loss (millions US\$)	Fraud risk score
Online payment fraud	4,665.0	93.5	436.2	0.7
Identity theft	5.4	51.6	278.3	0.6
Credit card fraud	10,328.0	16.8	173.0	0.5
Impersonation	12,584.0	11.3	142.6	0.3
Spoofing	4,436.0	18.5	82.2	0.4
Ransomware	13,196.0	3.7	49.2	0.3
Phishing	136.0	324	44.2	0.8
Malware	6,910.0	0.6	5.6	0.1
Denial-of-service	197.0	1.1	0.2	0.2
Technical support scams	1,454.0	23.9	347.7	0.5

Source: Adapted from AAG (2022b).

4. Aspects in this section of the chapter are based on Oluwatoyin et al. (2023).

The output target variable denoted as 't' has two rows, with the ten values having either [1; 0] for the classification of the identified form of cyberfraud as a high-risk occurrence or [0; 1] for the classification of the specified form of cyberfraud as low-risk occurrences. This is depicted in Table 5.2.

The neural pattern recognition application employed in this chapter will enable the data selection, network creation and training, and performance evaluation of the trained network using cross-entropy and confusion matrices. For data classification, a two-layer feed-forward network with sigmoid hidden and softmax output neurons can classify vectors once enough neurons are in the network's hidden layer. The network was trained iteratively with the scaled conjugate gradient backpropagation. It comprises inputs (10×10 matrix) representing the data of ten samples of ten elements. The target output is a 2×10 matrix.

Three significant phases characterise implementing the ML approach for data classification in this study. These include the training, validation and testing phases. The training phase enables the network to understand the features and relationships inherent in the data. This is usually carried out to fit the model so that the model can learn from the input data to make the correct classification. The training phase teaches the neural network, and the training continues until the performance goal is met. It is an iterative process that is carried out until the performance goal is met. When the performance goal is not met, the weights and bias can be adjusted until the network is adequately trained for predictive purposes. A negligible mean square error usually indicates an adequately trained neural network.

The validation phase measures network generalisation and training when there is no more improvement in the generalisation. The validation can also be used for the optimisation of the model. The testing phase measures the performance of the trained network and the classifier model. The test data set provides an independent measure of the network accuracy.

Training automatically stops when there is no improvement in the generalisation as indicated by an increase in the cross-entropy error of the validation samples. There is a need to minimise the cross-entropy results to obtain good classification results. Lower values are better, while zero

TABLE 5.2: Output factors and the allocated values.

Factors	1	2	3	4	5	6	7	8	9	10
A	1	0	0	1	0	1	1	0	0	1
B	0	1	1	0	1	0	0	1	1	0

Source: Authors' own work.

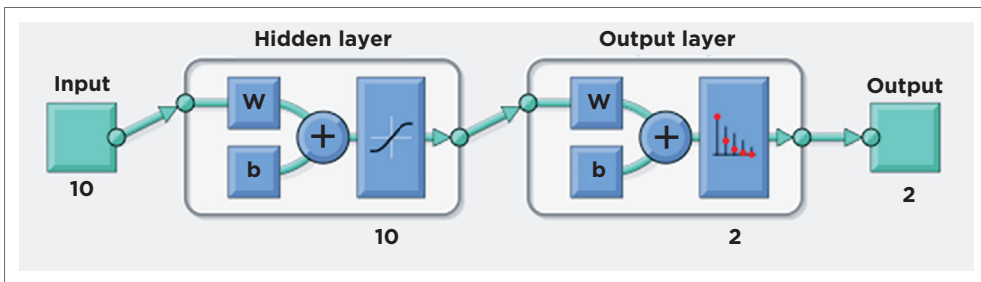
indicates the absence of error. The per cent error indicates the sample fractions that have been misclassified. A value of 100 implies that there is maximum misclassification, while 0 means there are no misclassifications.

The training was done under a supervised learning environment with labelled data for the input and target data sets. As shown in Figure 5.1, the network comprises ten input and ten hidden layers with two output layers. This is done to classify the forms of cyberfraud into two: high-risk and low-risk activities. The input and output of the data set are routinely divided into training, validation and test data sets. After that, the confusion matrix was employed to evaluate the percentages of the correctly and incorrectly classified outputs.

The simulation data set, obtained from the literature, considered the top ten prevalent forms of cybercrime. Scores on a probability scale (0.1-0.9) are allocated to the factors based on the frequency of perpetration (Table 5.1). The first aim is to build a classifier that can differentiate a high-risk from a low-risk form of cyberfraud based on the example used in this study. This classification analysis is supervised learning with input and output variables where the classifier learns how to weigh multiple features and produces a generalised, not over-fitted, mapping. One of the significant limitations of this approach is that it may misclassify activities that are not included in the historical or input data fed into the network. Having identified the factors, the information is fed into the neural network application in a MATLAB (2020b) environment to classify high-risk from low-risk cyberfraud.

The neural network is initialised with random initial weights, and a single-hidden layer feed-forward neural network with ten hidden layer neurons is created and trained using a scaled conjugate gradient backpropagation.

Figure 5.1 presents the neural network architecture for the high- and low-risk cyberfraud classification problems. The network comprises ten input factor, ten hidden layers and two output layers. The input factors are



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

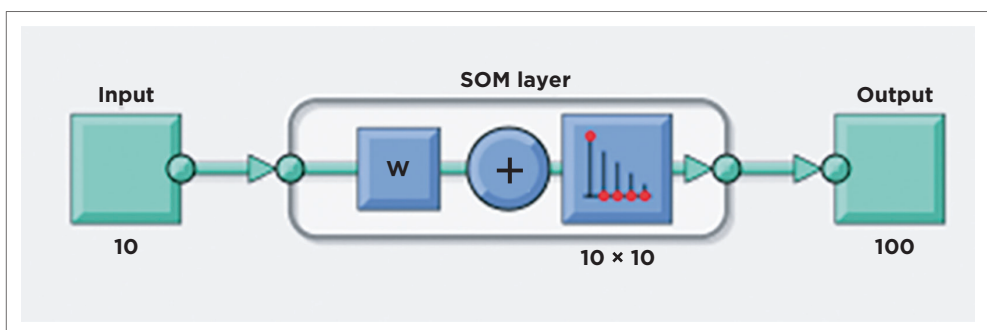
FIGURE 5.1: Neural network architecture for fraud detection.

the risk scores allocated to each cyberfraud form. In contrast, the output factor represents the model's results: a high and low-risk form of cyberfraud. The hidden layer is a layer between the input and output layers, which performs a nonlinear transformation of the inputs where the neurons take in a set of weighted inputs to produce an output through an activation function.

■ Procedure for the clustering analysis

The clustering of the forms of cyberfraud in Table 5.2 was also performed to classify the input factors according to their similarities and risk factors. The clustering analysis under unsupervised learning can be used to identify some trends or patterns that can lead to cyberfraud. The clustering model can continuously process and update new data and patterns automatically.

The architecture for the clustering analysis is presented in Figure 5.2. This is unsupervised learning comprising ten input factors and 100 output factors. The aim is to group the risk scores of the identified forms of cyberfraud based on their prevalence. The architecture is a self-organising map consisting of a competitive layer that classifies the data set of vectors with any number of dimensions into the classes as the layers of the neurons. The neurons are arranged in a 2D topology. This permits the layer to form a representation of the distribution and a two-dimensional approximation of the topology of the data set. The risk factors are input factors fed into MATLAB (2020b) as a matrix. The developed neural network is iteratively trained with the self-organising map (SOM) batch algorithm. The SOM algorithm is a good clustering algorithm and was considered for use in this study because its classifications can retain topological information about group similarities.



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).
Key: SOM, self-organising map.

FIGURE 5.2: Neural network architecture for the clustering analysis.

■ Results and discussion

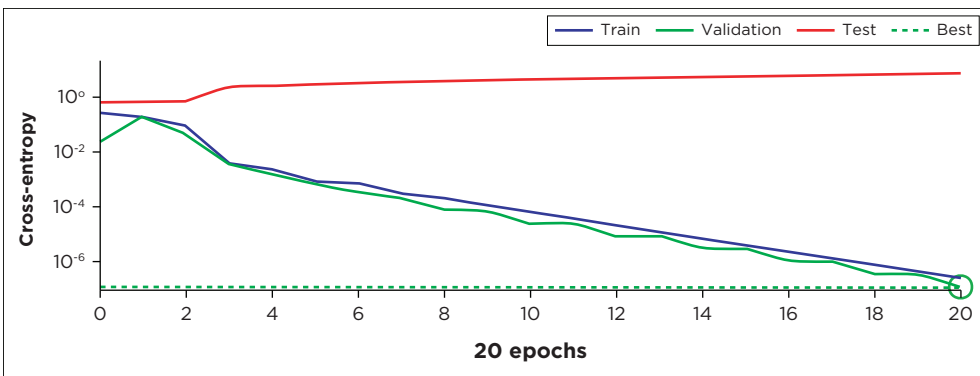
This section reports on the classification and clustering analysis outcomes, respectively.

■ Results obtained for the classification analysis

Figure 5.3 shows the network performance measured in terms of mean squared error on a logarithmic scale. The performance is shown for the training, validation and test data sets. The results indicated that cross-entropy's magnitude decreases as the network is trained. The performance goal was met at the 20th iteration (epoch) with a negligible mean square error value of 1.2213×10^{-7} . The epoch is the number of times the iteration was performed before the performance goal was met. The negligible value of the mean square error shows that the network has been adequately trained for the classification problem.

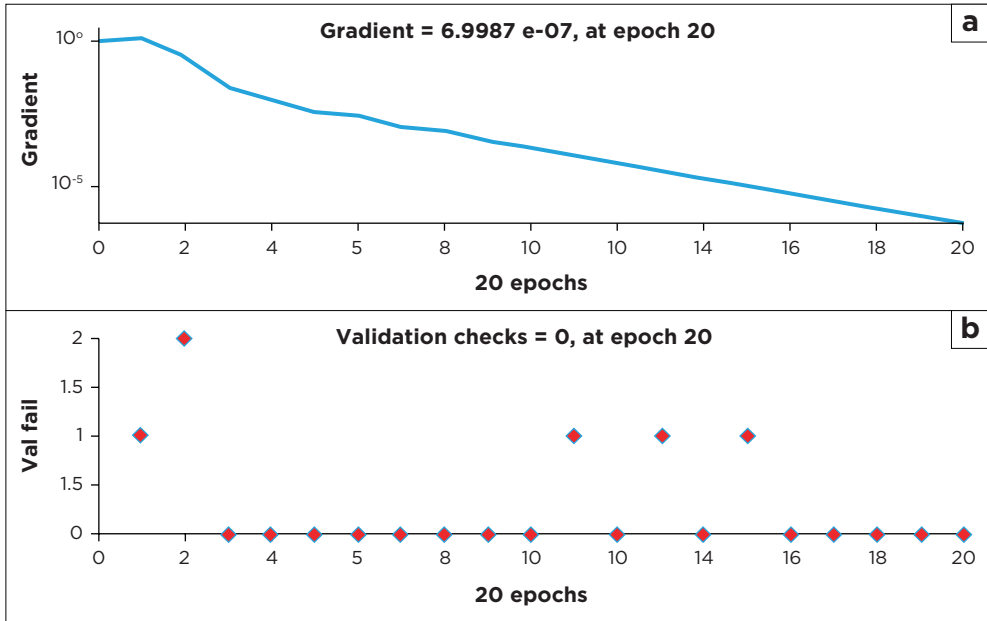
Figure 5.4 shows the plot of the gradient and validation check after the neural network training. The gradient is 6.9987×10^{-7} at 20 epochs. The training stopped at the 20th iteration as the data began to overfit. The best validation performance shows zero validation failure at the 20th iteration. The small values of the gradient (6.9987×10^{-7}) indicate that the error is negligible and that there is a high degree of agreement between the target and the output from the network.

Figure 5.5 shows the error histogram. The error is obtained by finding the difference between the targets and outputs from the network. Small error margins indicate that the network is adequately trained for the classification problem. In contrast, a significant error means the network is not sufficiently trained and liable for misclassification. The figure shows



Source: Authors' own work.

FIGURE 5.3: Validation performance goal.



Source: Authors' own work.

FIGURE 5.4: The gradient and validation check.

that the error values were negligibly small (not up to 1). The bins represent the number of vertical bars, and each of the bars depicts the number of samples from the data set. In this figure, the error histogram comprises 20 bins. The error range is between -0.95 and 0.95 . This was divided into 20 smaller bins, and the error is calculated as follows:

$$\begin{aligned} \text{Error range} &= \frac{(0.95 - (-0.95))}{20} \\ \text{Error range} &= 0.095 \end{aligned}$$

The width of the error corresponds to 0.0950. Furthermore, the error at the left-hand side of the plot was -0.05 when the vertical height of the bin for the data validation was eight. This means eight samples from the validation data set have errors, which fall within such range. The error range is, therefore, calculated thus:

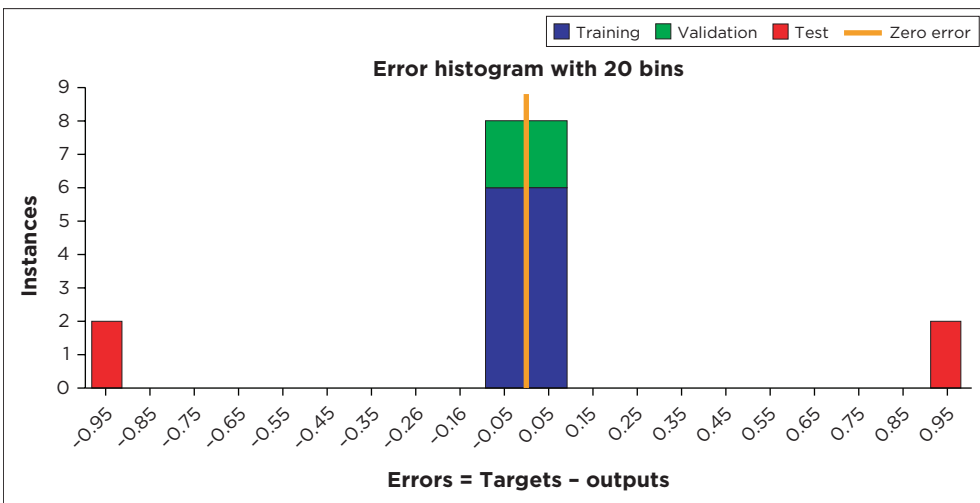
$$\begin{aligned} \text{Error range} &= \frac{-0.05 - 0.095}{2}; \frac{-0.05 + 0.095}{2} \\ \text{Error range} &= 0.0725; 0.0225 \end{aligned}$$

As illustrated in Figure 5.5, the small error range indicates a high degree of agreement between the targets and the neural network outputs (Daniyan et al. 2020). This implies a high probability that the neural network can classify the forms of cyberfraud as high and low-risk occurrences.

In addition, Figure 5.6 shows the confusion matrix, which measures the neural network’s performance in data fitting and classifications. The matrix indicates the percentages of correct and incorrect classifications. The green squares on the matrix diagonal indicate the correct classifications. In contrast, the red squares represent the incorrect classifications. The confusion matrix demonstrates that for the training, validation and testing processes, there are 100% correct classifications. For the confusion matrix, 80% of the forms of cyberfraud are correctly classified as either high- or low-risk cases, while 20% are misclassified. The few misclassifications indicate the accuracy of the developed network for classifying the identified forms of cyberfraud as either high- or low-risk cases.

The results obtained for the classification analysis of the identified forms of cyberfraud demonstrated the feasibility of the developed neural network model for the classification analysis. This is evidenced in the forms of cyberfraud correctly classified (95%) and the negligible percentages of misclassification (5%) obtained from the confusion matrix.

From Figure 5.6, 50% of the identified forms of cyberfraud are classified as high-risk occurrences. These include phishing, online payment fraud, identity theft, credit card fraud and technical support scams. Conversely, 50% of the identified forms of cyberfraud are classified as



Source: Authors’ own work.

FIGURE 5.5: Error histogram.

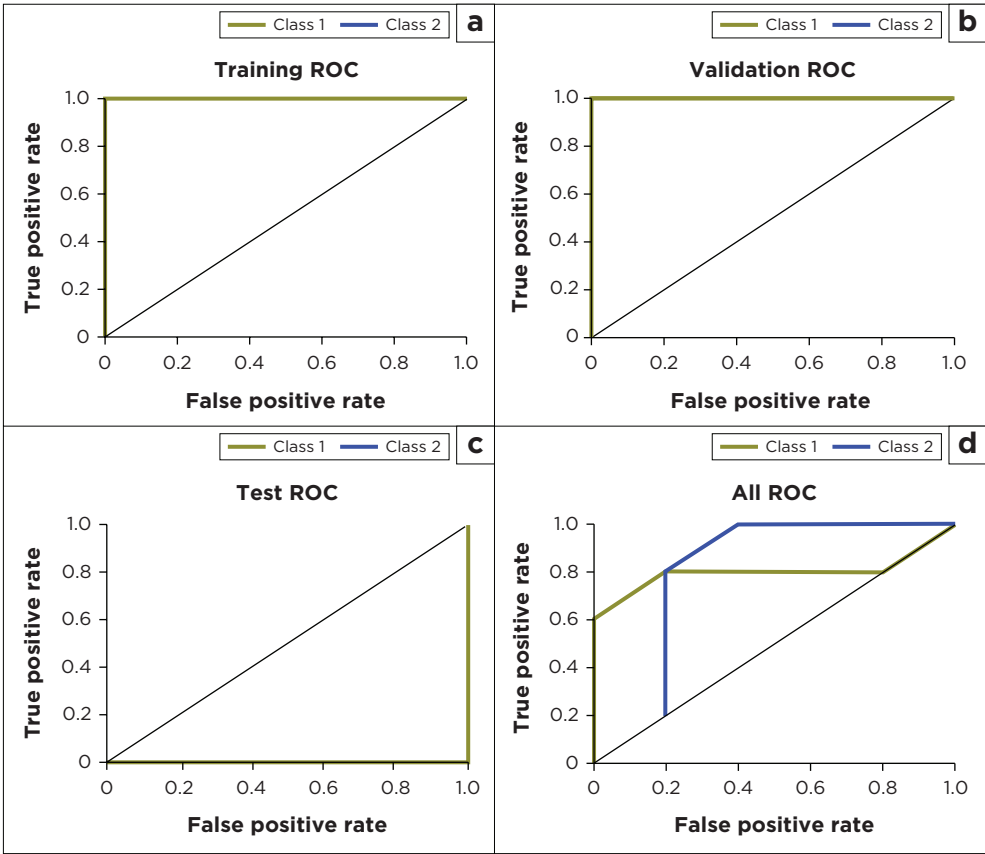


Source: Authors' own work.

FIGURE 5.6: Confusion matrix.

low-risk occurrences. These include spoofing, impersonation, ransomware, malware and DoS attacks.

Figure 5.7 presents the receiver operating characteristic plot. This is another measure of how well the neural network fits the data set. Class 1 shows the high-risk cyberfraud cases, while Class 2 indicates the low-risk cases. Figure 5.7 also shows how the false positive and true positive rates relate to the threshold of the outputs that are varied from 0 to 1. The farther left and up the line, the fewer the false positives. The best classifiers have a line from the bottom left corner to the top right corner, as shown in Figure 5.7. The confusion matrix classifies its output as 'True positive' when the model classifies the output correctly as positive. In other words, when there is an agreement between the prediction from the neural network model and the actual situation, the activities are not high-risk. 'True negative' is a situation whereby the model classifies the output correctly as negative. In other words, when the prediction from the neural network agrees with the actual position, the activities are high-risk cases. 'False positive' is a situation whereby the model predicts that the activities are high-risk and low-risk cases. Finally, a 'false negative' is a situation whereby the model prediction states that they are low-risk cases, whereas they are high-risk cases in the actual condition.

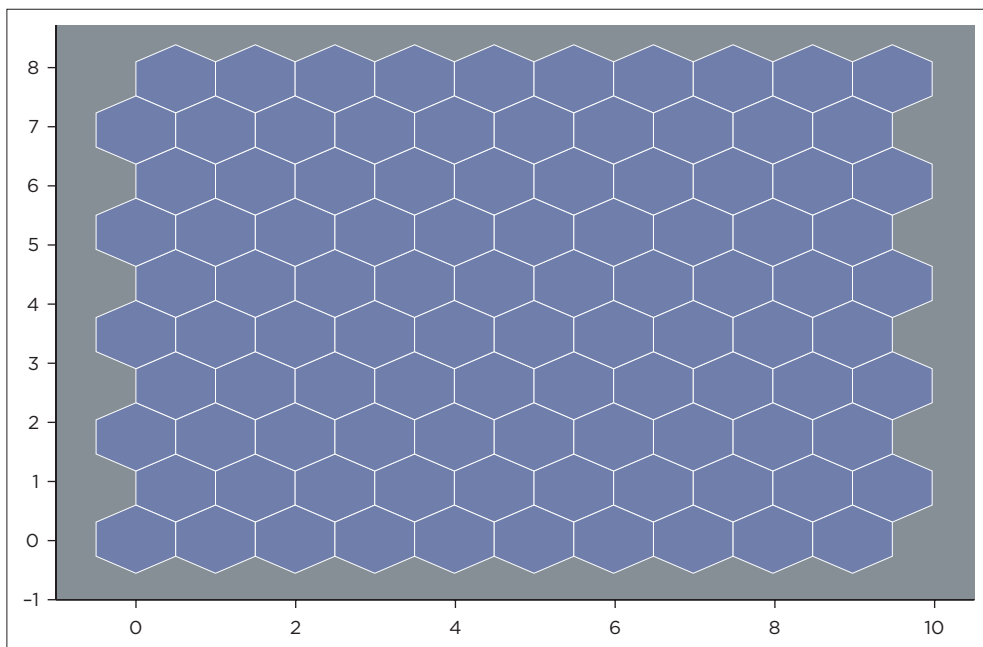


Source: Authors' own work.

FIGURE 5.7: Receiver operating characteristics.

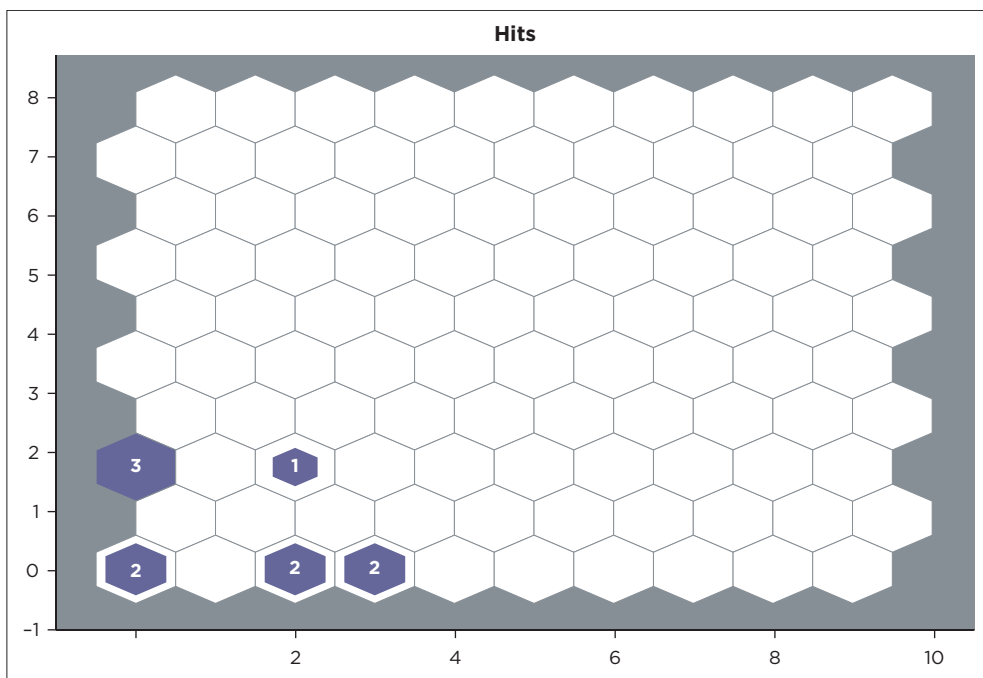
■ Results obtained for the clustering analysis

Figure 5.8 presents the SOM topology having 100 neurons positioned in a 10 x 10 decagonal grid. Each of the neurons represents the peculiarities of the different forms of cyberfraud identified, while the adjacent neurons represent similar classes. This means that the trends of the identified forms of cyberfraud can be recognised with the aid of neural network architecture. Hence, fraud investigators can use this to detect cases of cyberfraud. Figure 5.9 shows the SOM hits, which calculates the classes for each attribute of the identified forms of cyberfraud. The areas of neurons with significant hits represent the classes with similar highly populated feature space regions, whereas the areas with few hits indicate sparsely populated regions of the feature space. Figure 5.8 and Figure 5.9 can assist fraud investigators in understanding the identified forms of cyberfraud with the same or similar attributes. The forms of cyberfraud with the same cluster



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

FIGURE 5.8: Self-organising map topography.

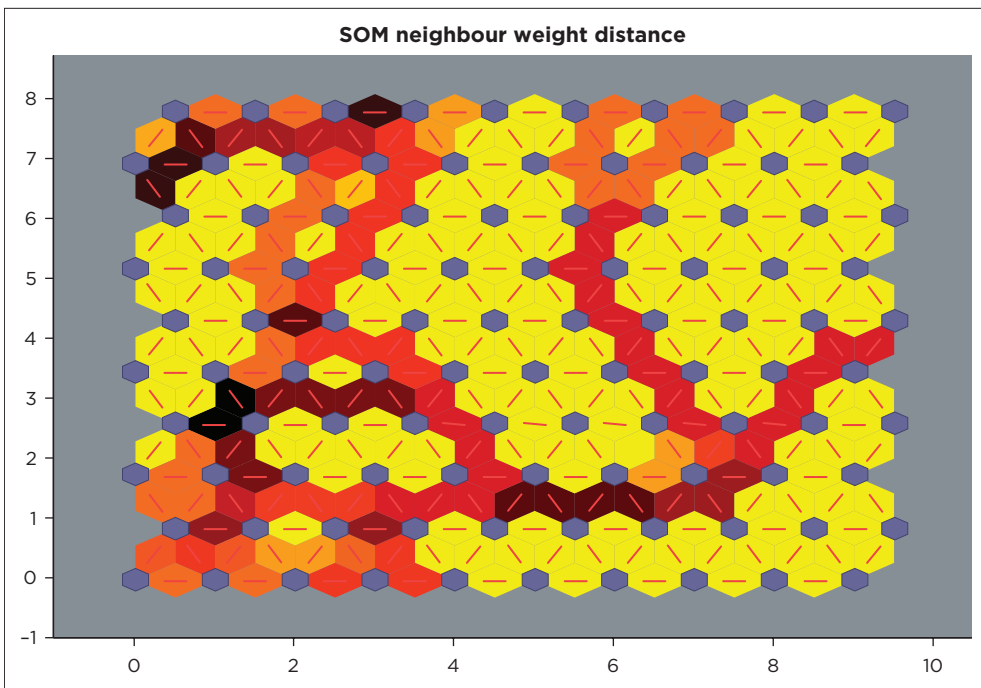


Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

FIGURE 5.9: Self-organising map hits.

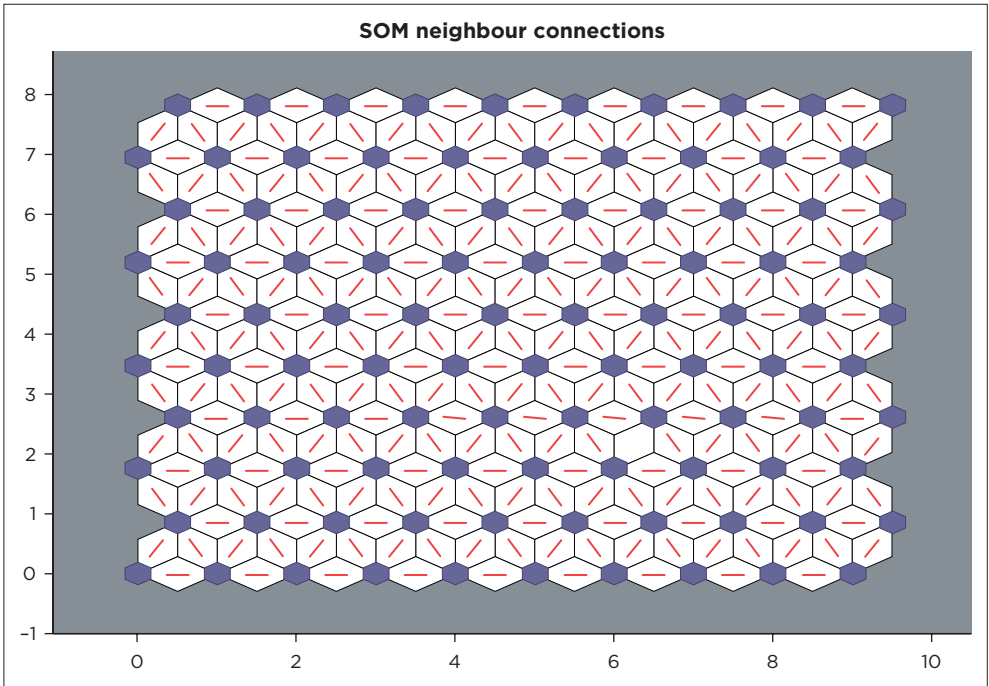
have the same or similar features. This implies that there exists a relationship between the identified forms of cyberfraud. In other words, one form of the identified cyberfraud could lead to the other. Hence, the clustering will enable a proper understanding of the existing relationship between the recognised forms of cyberfraud and how to mitigate them. For instance, when a fraud investigator detects a cyberfraud cluster, all the cyberfraud indicators in the cluster may lead to a cyberfraud case and must be investigated and mitigated.

Figure 5.10 shows the distance between a neuron's class and its neighbours. The parts indicated with bright connections show the highly connected areas of the input space. On the contrary, the areas marked with dark connections show the classes representing the regions of the feature space, which are distant apart. For instance, the bright connections in the figure may indicate the presence of possible connections among the identified forms of cyberfraud. For example, it may reveal the presence of high-risk cyberfraud cases. In contrast, the areas marked with dark connections, which are distant apart, may indicate the presence of instances of low-risk cyberfraud. Figure 5.11 shows the neuron neighbour connections, typically used to classify similar samples. This figure indicates the suitability of the unsupervised ML approach to detect hidden patterns that may not be visible or detected by manual or other examination techniques.



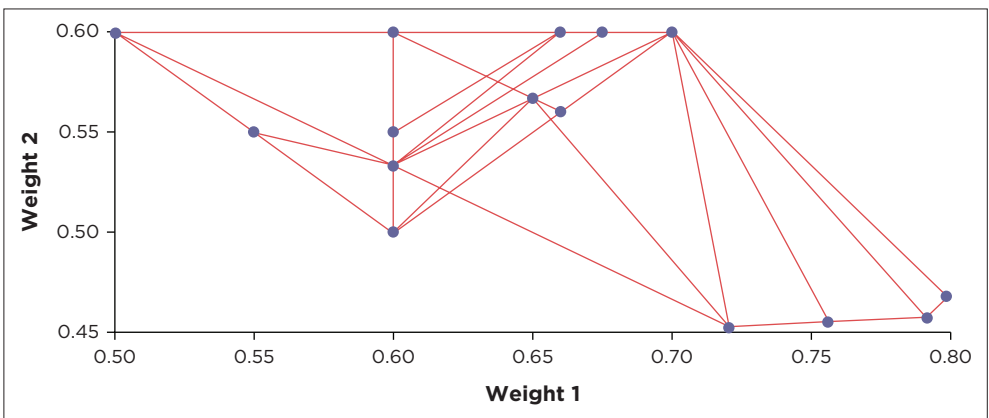
Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

FIGURE 5.10: Self-organising map neighbour weight distance.



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

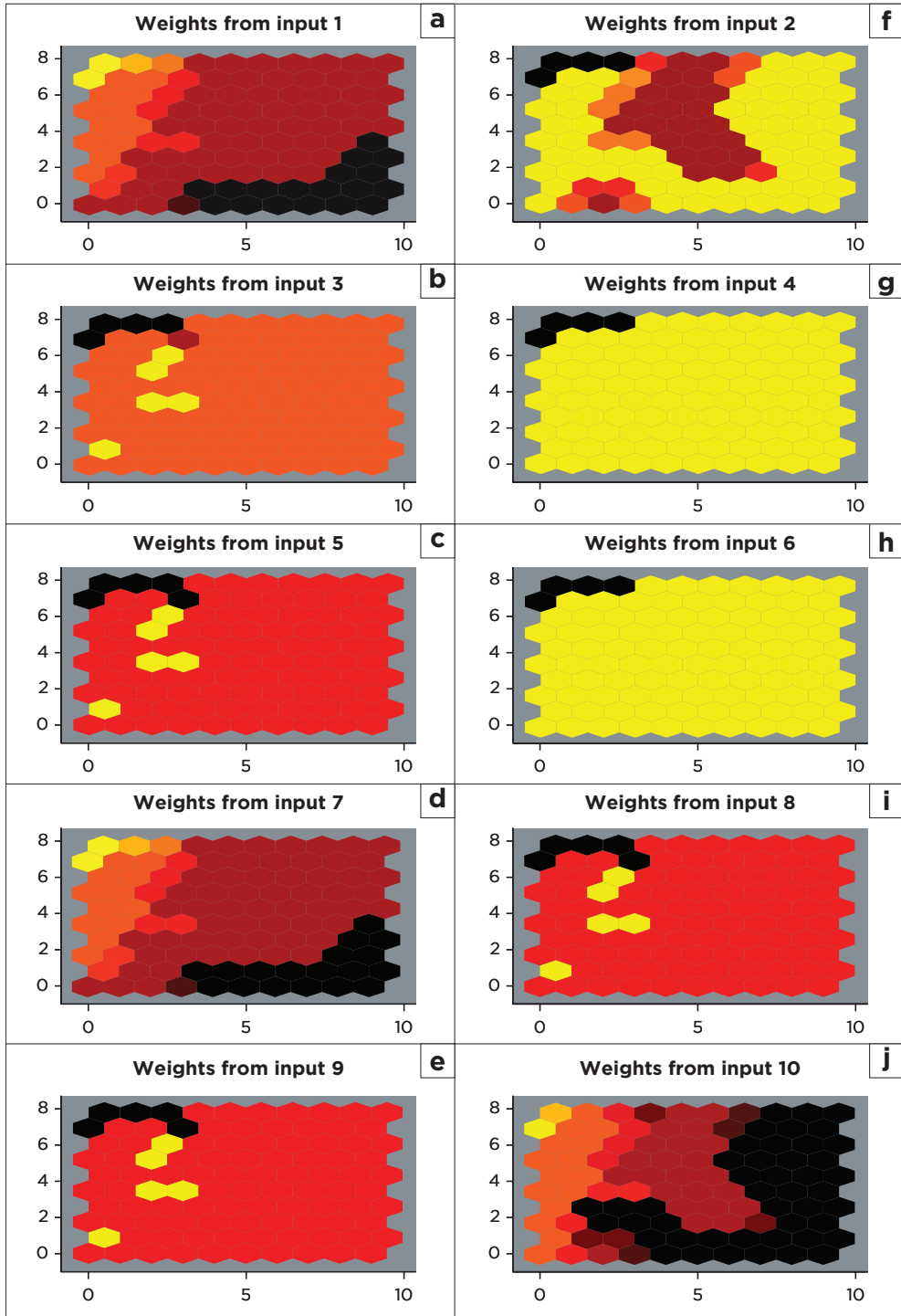
FIGURE 5.11: Self-organising map neighbour connections.



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

FIGURE 5.12: Self-organising map weight positions.

Figure 5.12 presents the SOM weight positions. It can be seen from the figure that the weights cover all parts of the data. Thus, whenever new data are fed as an input, it can easily be assigned to the exact cluster. The position of the data points implies a good representation of the data set.



Source: Authors' own work, generated using MATLAB (2020b) (2020 version, MathWorks).

FIGURE 5.13: The weights of the eleven potential red flags.

Figure 5.13 shows the weight plane for each of the eleven input attributes. The figure displays the weights that connect each input for 100 neurons in the 10×10 decagonal grid. The area with dark patches depicts larger weights. The presence of similar weight planes signals the correlation between the inputs.

■ Conclusion

Machine learning is a division of artificial intelligence and computer science that uses specialised algorithms to train data sets to imitate how humans learn for classification, pattern recognition and prediction tasks. This chapter aims to demonstrate the use of the ML approach for the classification and clustering analysis of the identified forms of cyberfraud. This was achieved under the supervised and unsupervised learning environment implemented in MATLAB (2020b). Firstly, the prevalent forms of cyberfraud were identified from the literature and fraud risk scores on a probability scale are allocated to them based on their prevalence. For the classification analysis, the neural pattern recognition application was employed in this chapter to enable the data selection, network creation and training, and performance evaluation of the trained network using cross-entropy and confusion matrices. For data classification, a two-layer feed-forward network, with sigmoid hidden and softmax output neurons, was employed to classify the vectors. The network was trained iteratively with the scaled conjugate gradient backpropagation. The clustering analysis architecture comprises ten input factors and 100 output factors carried out under unsupervised learning to identify some trends or patterns that can lead to cyberfraud. The results indicate that 50% of the identified forms of cyberfraud are classified as high-risk occurrences. These include phishing, online payment fraud, identity theft, credit card fraud and technical support scams. On the contrary, 50% of the identified forms of cyberfraud are classified as low-risk occurrences. These include spoofing, impersonation, ransomware, malware and DoS attacks. The clustering analysis indicated the suitability of the unsupervised ML approach to detect hidden patterns that may not be visible or detected by manual or other examination techniques. Thus, this chapter demonstrates a practical guided approach for implementing ML under the supervised and unsupervised learning approach for cyberfraud analysis.

Machine learning works best when big data (high volume of data) is employed. Thus, it is recommended that financial institutions develop ML capabilities by developing a suitable approach for gathering big data and developing the required expertise in implementing the ML approach geared towards cyberfraud analysis and mitigation.

The role of big data technology in fraud mitigation

■ Introduction

In this digital era, many transactions are carried out online. As a result, data of different structural levels, sizes and varieties are gathered. There is a need to analyse the data gathered to make an informed decision effectively. The traditional method of data analysis may be time-consuming and ineffective in processing the large amount of data collected from different sources. Thus, there is a need for big data analytics (BDA) to effectively process such data and solve specific organisational challenges such as fraud detection. This chapter presents a systematic literature review on the role of big data technology in fraud mitigation in this digital era. Articles which provided theoretical, conceptual or empirical results of BDA were selected. After the elimination process, a total of 90 articles were systematically reviewed. The findings from the existing works indicated the suitability of big data analytic techniques, such as data-mining and ML, for detecting frauds such as cyberfraud, money laundering, insurance fraud, financial statement fraud, management fraud and fraud in the health sector, among others. Furthermore, the literature synthesis provides conceptual guidelines for implementing the big data technology geared towards fraud mitigation. The use of big data technology for fraud

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'The role of big data technology in fraud mitigation', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 111-125. <https://doi.org/10.4102/aosis.2024.BK485.06>

mitigation is still emerging; thus, developing the human capacity to upskill personnel to effectively implement some of the identified big data tools and technologies will promote sustainability in using big data technology to combat fraud.

■ The role of big data technology

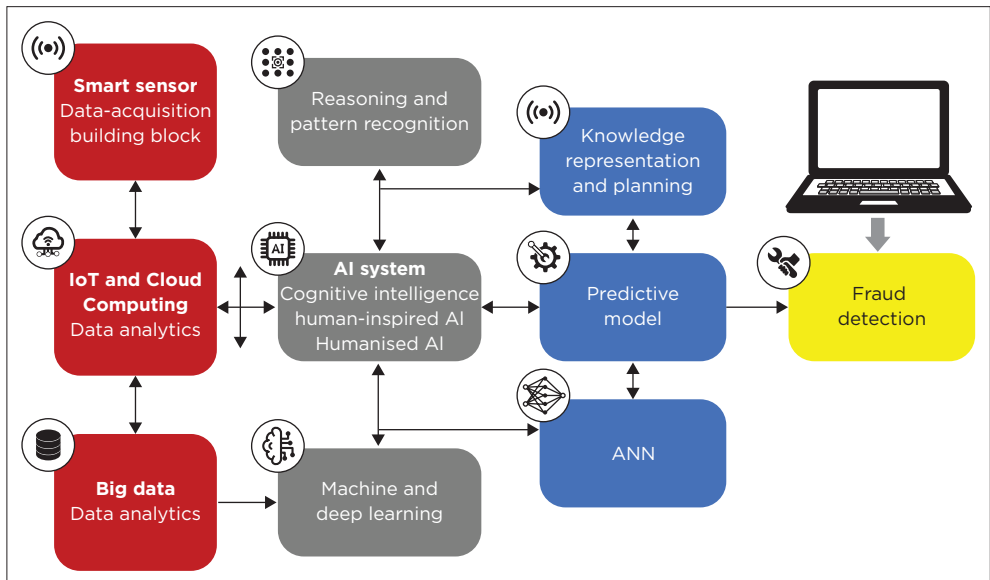
The term big data technology refers to the technology whereby a large amount of data are collected at high velocity and from different sources for analysis to obtain valuable information (De Dott 2020; George, Haas & Pentland 2014). Three key attributes are commonly used to describe the 'big data'. These are high-volume (vast size or amount of data garnered, which may range from terabytes to tens of petabytes), high velocity (the high speed at which the data was collected, which may range from 30 kilobytes to 30 gigabytes per second) and wide variety (the diverse sources from which the data were garnered and the form of the data captured) (Arnaboldi, Busco & Cuganesan 2017; De Dott 2020; Moffitt & Vasarhelyi 2013; Vasarhelyi, Kogan & Tuttle 2015; Yoon, Hoogduin & Zhang 2015; Zhang et al. 2015). Some examples of data sources include organisational data (data captured by the organisation's system and stored in the database, including customer information and transaction-related information as in the case of financial institutions), experimental data (data created by digital machine sensors, devices, satellite and digital cameras) and social media data (data created by people in the form of text messages, blogs and posts). In terms of data forms, Moffitt and Vasarhelyi (2013) explain that data could be in structured, unstructured, semi-structured and multistructured forms. Structured data are a form of data presented in tables with fixed attributes, as in the case of relational data. At the same time, people usually generate data in an unstructured form via text, video, audio, or natural languages. The data are generally presented in tags, but this changes with documents for semi-structured data - for instance, HTML, XML, JSON files and server logs. Multistructured data are an integrated form of different types and structural levels. Thus, big data is a collection of different kinds of high-volume data collected at high speed and from various sources. Examining, pre-processing and analysing big data to obtain valuable information, such as detecting specific trends or patterns to make an informed decision, is usually called BDA (Cao, Chychyla & Stewart 2015).

Using statistical or ML techniques, BDA uses an exploratory approach to study voluminous data to infer knowledge. The programming of the BDA could be at a low level, involving the use of Java and Python or, at a high level, including the use of SQL and its derivatives or domain-specific

languages such as Cypher or PigLatin. The heterogeneous and voluminous data set extracted in this digital age from diverse sources is unlikely to fit into the main memory of a cluster. In other words, big data exceeds the commonly used hardware and software capacity to capture or manage (Moffitt & Vasarhelyi 2013). This is coupled with the need to process the data chunk by chunk to obtain condensed, useful and insightful information. There is a consensus among the authors that the use of big data technology can assist in the process of fraud investigation and mitigation (Baader & Krcmar 2017; Balios et al. 2020; Cao et al. 2015; Chiu, Wang & Vasarhelyi 2020; Dagilienė & Klovienė 2019; Jans, Alles & Vasarhelyi 2011; Rahmawati, Yaqin & Sarno 2016; Tang & Karim 2019; Vasarhelyi et al. 2015; Werner 2016; Yoon et al. 2015).

The digital world that is driven by data technology is gradually emerging. Many organisations leverage the power of data to transform the enterprise, although some without the ‘data-driven’ culture still struggle to implement big data technology. Some challenges to the evolution of big data technology in organisations could also relate to organisational alignment, resistance or lack of understanding and change management, among others.

Figure 6.1 presents a conceptual framework for big data analysis for fraud detection.



Source: Authors' own work.

Key: IoT, Internet of Things; AI, artificial intelligence; ANN, artificial neural network.

FIGURE 6.1: Conceptual framework for big data analysis for fraud detection.

■ **Methodology: Systematic literature review on big data technology**

This chapter employs a systematic literature review involving the preferred reporting items for systematic reviews and meta-analysis (PRISMA) approach. Preferred reporting items for systematic reviews and meta-analysis are evidence-based approaches researchers use to report various systemic reviews and meta-analyses (Liberati et al. 2009).

The PRISMA approach was chosen as the best method for conducting the literature review in this investigation because it is a detailed approach suitable for literature synthesis that ensures transparent and complete reporting (Liberati et al. 2009). The literature reviewed was found using a variety of major search engines, such as Google Scholar, Wiley, Emerald, ScienceDirect, ResearchGate, Sage Publications, ACM Digital Library, Google Books, IEEE, UK Routledge, ERIC, ProQuest and Springers. The relevance of the articles selected for review was determined by publications published in the field of 'big data' and its associated applications in fraud mitigation or financial investigation.

To streamline the study, relevant inclusion and exclusion criteria, such as the year of publication and relevance of the keywords to the subject matter, were considered (Daniyan et al. 2021, 2022). This guideline was followed to facilitate a carefully planned and documented systematic review that promotes consistency, transparency, accountability and the integrity of review articles.

■ **Data sources**

The quality of a systematic review partly depends on the sources from where the data are garnered (Abdulrahaman et al. 2020). A systematic search of literature aligned with the study's focus was carried out from academic and research databases. The articles gathered were screened, and the relevant ones were selected for review.

■ **Keywords search**

The search utilised key phrases including 'big data', 'big data analytics', 'big data technology', 'big data in fraud mitigation' and 'big data in financial investigation'. The literature was also categorised using keywords, and the systematic review was employed, followed by the procedural checklist outlined as a guideline by the existing works (Abdulrahaman et al. 2020; Kitchenham et al. 2009).

TABLE 6.1: Search strategy adopted in the present systematic review and meta-analysis.

Search strategy items	Details
Keywords	'big data', 'big data analytics', 'big data technology' and 'big data in fraud mitigation'
Popular search engines	MDPI, Springer, Taylor & Francis, ScienceDirect, John Wiley & Sons, Citeseer, ResearchGate, Sage Publications, ACM Digital Library, Google Books, ResearchGate
Inclusion criteria	Relevance and year of publication
Exclusion criteria	Content outside of BDA
Time-lines filter	1990–2022
Language filter	Only articles written in English

Key: BDA, big data analytics.

■ Inclusion and exclusion criteria

Some inclusion criteria include the year of publication, the relevance of the articles to the study, the availability of empirical findings, and the conceptual or theoretical framework of big data technology as it relates to fraud or financial investigation. The year of publication only applies to conference and journal articles. Articles published between the years 2000 and 2022 were selected. The publication year was not a criterion for seminar works and textbooks.

The total number of articles obtained from the database after the search was 9,654. Afterwards, unrelated and duplicate papers were eliminated, bringing the total number of articles to 1,250. Subsequently, the content of the articles was perused, and some articles were dropped based on the contents. Articles which provided theoretical, conceptual, or empirical results of BDA were selected. After the elimination process, a total number of 90 articles were reviewed. The 90 peer-reviewed articles are published in reputable journals and conference proceedings and written in English. The framework for the inclusion and exclusion of the articles is presented in Table 6.1.

■ Review of the role of big data technology in combatting fraud

Corporate fraud involves using one's profession for personal benefit through deliberately misappropriating an organisation's resources (Association of Certified Fraud Examiners [ACFE] 2012a, 2012b). The AICPA (2002) defines fraud as deceiving an individual or organisation to exploit its resources for personal gains.

Ramamoorti, Morrison and Koletar (2014) indicated that fraud involves deception, purposeful intent, intensity of desire, possibility of apprehension,

breach of trust and rationalisation. In the context of financial reporting, Rezaee (2005) defined fraud as an intended attempt by an organisation to trick, cheat or misinform the users of financial statements, most notably the stakeholders, through the preparation and dissemination of misstated financial statements.

One of the subsets of general fraud is cyberfraud. Cyberfraud is a broad term comprising a multitude of offences. It can be summarised as a criminal act involving IT infrastructure to gain unauthorised access to personal or organisational confidential information or to illegally interfere with or intercept personal or organisational data or systems to commit fraud (Tiwari, Bhalla & Rawat 2016). It comprises computer-enabled actions complemented with global networks, either by definite entities or otherwise, and has become a significant global challenge for law enforcement agencies (Meephlam 2017; Monni & Sultana 2016).

It can be categorised into cyber-dependent crime and cyber-enabled crime. Cyber-dependent crimes, or pure cyberfraud, are perpetrated using a computer, computer networks or other ICT. These acts include spreading viruses or other malware, hacking and distributed denial-of-service (DDoS) attacks. At the same time, cyber-enabled crimes are traditional crimes that can be increased in scale or reach using computers, computer networks or other forms of ICT. Unlike cyber-dependent crimes, which rely solely on ICT, the underlying crimes of cyber-enabled crimes can be perpetrated without ICT. The most common types of cyber-enabled crimes are fraud and theft. A typical example is scam emails that deceive recipients into transferring money to an unidentified sender (McGuire & Dowling 2013).

■ Theoretical literature review on the role of big data in fraud mitigation

Big data is described as a vast and ever-increasing volume of data (Ur Rehman et al. 2016). Among others, it has five characteristics, usually referred to as the 'five V's': volume, velocity, variety, veracity and valence (Ahmed et al. 2021). Big data analysis may be applied to detect transaction inconsistencies resulting in fraud. The analysis could also be performed in a discrete environment where there is a restriction on data transfer. Data can be stored in different locations and systems; hence, thorough research is usually required to locate it in hidden places. Additionally, data-mining and statistical analysis can also be helpful for the analysis of voluminous data sets (Gai, Qiu & Zhao 2016).

Through big data technology and analytics, voluminous data related to fraud incidences can be managed (acquired, processed and analysed) to

achieve a reliable outcome. Big data analytics combines numerous data processing techniques. Thus, organisations' collective use of these techniques can enable them to obtain valuable outcomes or results. Hence, big data plays a significant role in cyberfraud mitigation as it can assist organisations in gaining access to a pool of data and with the analytical concept, the data can be processed to discover hidden trends, patterns or relationships or used to perform predictive functions, thus, enhancing good decision-making in real time (Thhaduri et al. 2015). McAfee and Brynjolfsson (2012) indicated that big data technology boasts high processing power and storage capacity. Traditional data analytics is structured and limited in size and information. This is because information exists on other nontraditional platforms, such as social media, email, posts and blogs, which can provide helpful information for fraud investigation and legal requirements (Moffitt & Vasarhelyi 2013). Big data analytics can assist financial organisations to avoid or mitigate risks by visualising and analysing possible scenarios. Big data analytics can be divided into four categories, namely descriptive analytics (which answers the questions 'what happened, where and how did it happen?'), diagnostics analytics (which reveals the root cause and may answer the question 'why it happened, the perpetrators involved, the scope of perpetration and the reason for perpetration and the perpetrators?'), predictive analytics (which will forecast what will happen because of the perpetration) and prescriptive (which will indicate what is to be done to minimise the impact of the occurrence and forestall possible future occurrences).

Existing studies have indicated the feasibility of the BDA technologies for service innovation (Lehrer et al. 2018; Yoo et al. 2012).

The authors explain and highlight the capability of the BDA technologies for data sourcing, storage, event recognition or prediction, behaviour recognition and prediction, among others. Thus, the authors developed a framework for service automation and BDA-enabled human-material service practices. There are two key primary roles of BDA in the context of service innovation. These include automation of customer-sensitive service provision and human-material customer-sensitive service practices. Service innovation can improve customers' relationships and how employees and management respond to cyber threats from customers.

Big data analytics finds application in business analytics (Chen, Chiang & Storey 2012). For instance, it can provide helpful insights and valuable information to fraud investigators in detecting hidden patterns, trends, or anomalies in a data set (Clayton 2011; Decker et al. 2011; Kenyon & Tilton 2011; Miller & Martson 2011). Mittal, Kaur and Gupta (2021) indicate that big data can play the 'mediating role' in influencing experts to employ FA for fraud detection. Ngai et al. (2011) show the suitability of the data-mining

approach (data analytics) for detecting financial fraud. Moffitt and Vasarhelyi (2013) suggested that the traditional way of information security is no longer sufficient in this digital age with the evolution of big data technology. Hence, many organisations are currently exploring the concept of big data technology, including finance and insurance, for fraud detection and risk analysis. For instance, through the 'click path', the source of fraud can be traced in connection with the websites and webpages visited by the threat actors, including the transactions carried out. Thus, the path of fraudulent behaviours and the threat actors can be identified.

In terms of the efficiency of accounting measurements, Vasarhelyi (2012) and Moffitt and Vasarhelyi (2013) state that big data can significantly impact certain areas, such as real-time provisioning of transaction data, provisioning of information data and breaking reports into divisions. However, some authors have suggested the need for substantive formalisation of BDA with a proper description of its data processing mechanics, classification structures, taxonomies and hierarchies in this digital age (Geerts & McCarthy 2002; Vasarhelyi 2012).

Regarding the accuracy of financial reporting, Vasarhelyi (2012) states that big data integrates semantic data from many sources. Thus, this may influence the quality and correctness of the information in financial reports.

In auditing, Vasarhelyi (2012) states that many auditing activities are obsoletely performed manually or semi-automatically in a digital age where database-to-database verification can be carried out with the aid of big data technology. Ambalavanan (2020) suggests using safety systems and other approaches to identify cyber pressures effectively. One of the significant drawbacks of the safety system is that the computer resources decide the safety dependability levels of ordinary users without any input from technical safety experts. Furthermore, spam, junk messages and other undesired or unsolicited communications pose a significant risk to the organisation's systems and will consume network and system resources, including Internet resources, computer memory and speed.

■ Empirical review on the role of big data in cyberfraud mitigation

In their study, Kantarcioglu and Shaon (2019) develop a system to protect data and ensure information confidentiality. The system considers various data administration systems by conforming to safety standards using innovative SECURED.L software. Organisations can use their systems to monitor confidential information or communications, such as audit logs.

The developed system can also sort and accumulate personal data depending on the needs or requirements and identify unauthorised access.

Chan et al. (1999) indicate that the data-mining technique of integrating multiple algorithms such as C4.5, Classification and Regression Tree (CART), Ripper and Bayes learning algorithms is suitable for effective intrusion and credit card fraud detection. The results indicated that the integrated machine model effectively computes meta-classifiers and detects credit card fraud and unauthorised access. Chen, Chen and Lin (2006) demonstrate the feasibility of employing a binary support vector system and genetic algorithm to detect credit card fraud with few input data having skewed distribution. Dorronsoro et al. (1997) present an online system installed in a transactional hub to identify credit card fraud based on a neural classifier. They report that the online fraud detector is fully operational and can handle more than 12 million operations annually with high efficiency in credit card fraud detection.

To curb money laundering, Gao and Ye (2007) successfully demonstrate the use of the data-mining approach. The money laundering network generation analysis results, which involve link analysis, community generation and network destabilisation, indicated that the proposed methodology could serve as an anti-money laundering technique if effectively deployed. Zaslavsky and Strizhak (2006) and Quah and Sriganesh (2008) proposed a real-time system for detecting credit card fraud using computational intelligence, specifically the SOM and clustering technique to identify, process and analyse customer behaviour for detection. Quah and Sriganesh (2008) stressed the need to develop a system that can adequately model and adapt to dynamic patterns in the digital marketplace with easy convergence of information such as customer and merchant profiles, selling patterns and market policies for effective decision-making. Srivastava et al. (2008) and Bhusari and Patil (2011) employed the Hidden Markov Model (HMM) for the detection of credit card fraud. The studies are based on the HMM to study the transactional profile of a credit card holder in relation to the card holder's incoming transactions and spending behaviour. The results indicated that the approach could identify and classify the transactions on the credit card as fraudulent or non-fraudulent activities. Yeh and Lien (2008) investigated the predictive accuracy of six data-mining techniques - K-nearest neighbour classifier, logical regression, discriminant analysis, naïve Bayesian classifier, artificial neural network (ANN) and classification tree - in predicting the probability of defaulting in credit card users. The results indicate that out of the six techniques, the ANN has the highest accuracy and capability to predict the actual probability of default.

■ Empirical review on the role of big data in general fraud mitigation

Abouelmehdi, Beni-Hessane and Khaloufi (2017) emphasise the importance of big data in the health care sector. In their study on the current security and privacy issues, the authors highlighted the influence of big data in the health care sector. He, Graco and Hawkins (1997) also demonstrate using neural networks involving a multi-layer perception and SOM to detect fraud among general medical practitioners. Many data-mining techniques have been reported in the health sector for uncovering fraud. These include clustering, Bayesian co-clustering, outlier detection, support vector machine, logic regression, neural network, classification tree, genetic algorithm and k-nearest neighbour clustering (Aral et al. 2012; Capelleveen 2013; Copeland et al. 2012; Ekina et al. 2013; Kirlidog & Asuk 2012; Kumar, Ghani & Mei 2010; Liu & Vasarhelyi 2013; Musal 2010; Ngufor & Wojtusiak 2013; Shin et al. 2012; Tang et al. 2011).

Bai, Yen and Yang (2008) compare the CART performance and the Logit regression in detecting false financial statements. The results indicated that the CART outperformed the Logit regression in identifying false financial statements. Other data-mining techniques for the detection of financial statement fraud include neural networks (Cerullo & Cerullo 1999), logistics regression models (Bell & Cerullo 2000) and fuzzy neural networks (Lin, Hwang & Becker 2003). In addition, Artís, Ayuso and Guillén (2002) indicate that automobile insurance fraud can be detected with the use of discrete choice models, while Bermúdez (2008) suggested that the use of an asymmetric link can significantly improve the percentage of insurance fraud case detection that is correctly classified. Other techniques for uncovering automobile insurance fraud include Kononen's self-organising feature map (Brockett, Xia & Derrig 1997), principal component analysis of RIDITS (relative to an identified distribution) (Brockett, Derrig & Golden 2002), fuzzy logic algorithm (Pathak, Vidyarthi & Summers 2005), fuzzy-based algorithm and multinomial Logit model with missing information (Caudill, Ayuso & Guillén 2005), Bayesian learning neural network (Viaene, Dedene & Derrig 2005) and Naïve Bayes (Viaene, Dedene & Derrig 2004).

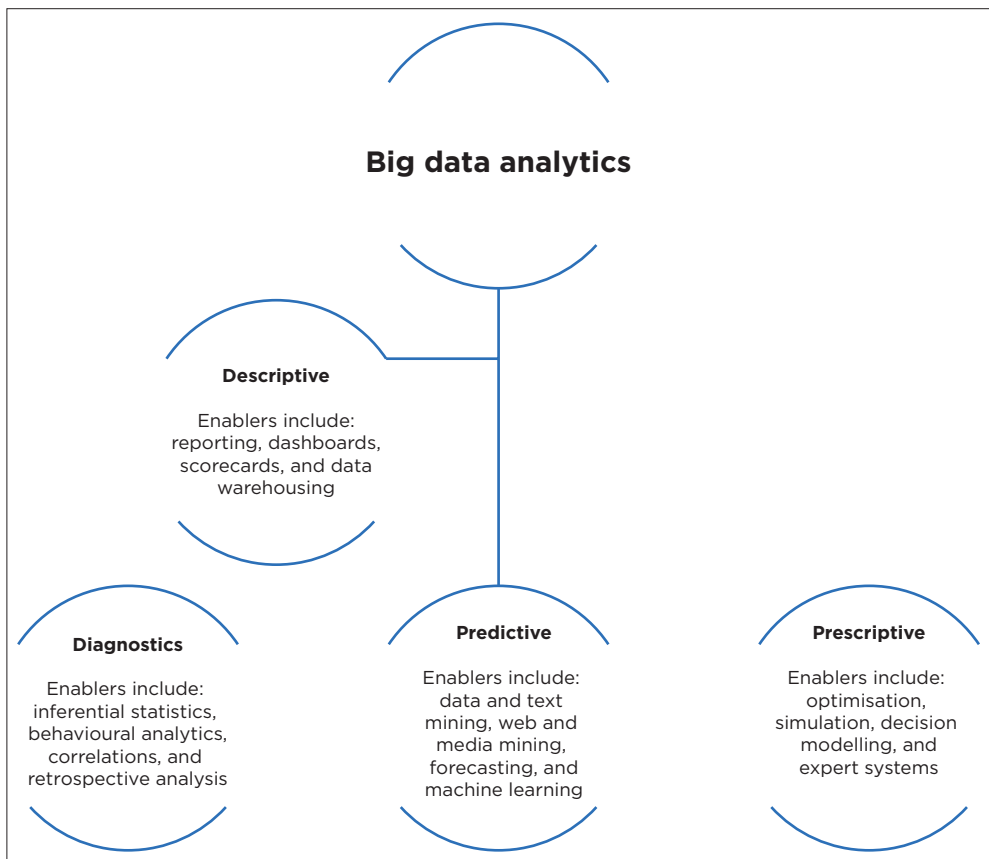
In terms of fraud risk management, Deshmukh, Romine and Siegel (1997) and Deshmukh and Talluru (1997) propose using a fuzzy logic-based reasoning approach to identify fraud potential red flags. Concerning management fraud, Green and Choi (1997) and Fanning and Cogger (1997) propose using the ANN for fraud identification.

■ Conceptual literature review on the role of big data in fraud mitigation

Figure 6.2 presents the value chain of BDA.

Table 6.2 presents the possible sources of data for fraud investigation, the possible measures and indicators, while Table 6.3 presents the stages of BDA for fraud investigation.

For further discussion, Table 6.4 and Table 6.5 are included. Table 6.4 summarises the significant BDA technologies and their functions, while Table 6.5 presents the significant findings on applying big data for fraud mitigation.



Source: Adapted from Delen and Demirkan (2013).

FIGURE 6.2: Big data analytics value chain.

TABLE 6.2: Possible sources of data for fraud investigation, the possible measures and indicators.

Sources	Description	Indicators
Customer service data	Customer information and other information gathered from customers relating to the service provided, causes of fraud and the prevalent ones	Frequency of customers' complaints and the frequency of reported forms of fraud Customer perspectives of the balance scorecard
Operational data	Data from day-to-day organisational activities, including operational efficiency or efficiency of fraud mitigation and risk management strategies	Number of successful and unsuccessful fraud cases and their implications The internal business processes of the balance scorecard
Employee performance data	Employee information Productivity of fraud investigators and personnel saddled with risk management and fraud mitigation	The learning and growth perspective of the balance scorecard
Website	Online activities of customers, employees and threat actors and detection of their browsing, communication or transactional patterns	Anomaly detection through analytics
Mobile	Data logs and sensor data generated by mobile devices to provide useful insights into customers', employees' and threat actors' mobile activities, locations or movements	Anomaly detection through analytics
Social media	Unstructured data gathered about the posts of customers, employees or threat actors to provide insights into their activities, lifestyles and opinions	Detection of negative activities, lifestyles or opinions

Source: Authors' own work.

TABLE 6.3: DBA for fraud investigation.

Stages	Description	Action
Data discovery and acquisition	Access to and collection of big data	Discovery of data sources Collection and storage of heterogeneous data set Creation of an inventory for the data sources and the metadata
Data preparation	Arrangement of data in useful formats for analysis	Data pre-processing Data formatting, indexing, organisation and optimisation Set up data access control
Pre-analysis	Evaluation of the data history and overview of the pre-processed data in preparation for detailed analytics	Identification of possible patterns and relationships Identification of syntax, structure and semantics for each data source
Data integration	Combining or linking all data of different types and sources that relate to the same case together	Establish a common data representation
Detailed analytics	The use of the right analytical tool to analyse the data and retrieve the required information	Carry out descriptive, diagnostics, predictive or prescriptive analytics depending on the requirements or information required Establish a cause-and-effect relationship
Visualisation and reporting	A holistic view of the outcome of the analytics and presentation of the outcome	Use illustrative graphs or tools to summarise and present the outcome of analytics
Decision-making	Review possible scenarios and decide on the necessary steps to undertake	Prescribe and take actions based on the outcome of analytics

Source: Adapted from Stein (2022).

TABLE 6.4: Summary of the major big data analytics technologies and their functions.

Big data analytics tools or technologies	Function	Reference
API	Provide real-time access to data such as social media data	Chen et al. (2012)
Data lake	For data storage in the native format. Data lake can combine data from different sources and of varying types (structured, unstructured, processed or unprocessed data) and conduct future analysis. It can also enable users across multiple platforms to refine, explore and enrich data. Furthermore, its interactive nature permits multiple data access across a shared platform.	Porter and Heppelmann (2015)
Data pre-processing software	For organising and cleaning data into a consistent format in preparation for the main analysis	Kaur (2022)
Data quality software	For cleaning and enriching data set to obtain consistent and reliable outputs from big data processing	King (2021)
Predictive analytics	Uses statistical or machine learning approaches to analyse present or historical data to make predictions about future events or patterns. Useful for avoiding risks in decision-making.	Chen et al. (2012)
NoSQL databases	For efficient data management across a scalable number of storage nodes. Store data as relational database tables, JSON documents or key-value pairings.	Redy (2018)
Knowledge discovery tools	These tools allow businesses to mine big data stored on multiple sources. It enables data analysts to isolate and utilise the information to meet their goals.	Cattermul (2016)
Stream analytics	For filtering, aggregation processing and analysis of data stored on multiple platforms and in various formats. Stream analytics also permit connection to external data sources and their integration into the application flow. As such, it can be used for the analysis of live-streaming data to identify trends or patterns and trends to detect current or future nonconformities from the normalcy.	Watson (2014)
Web analytics	For the analysis of clickstream data logs to provide useful insights into the online activities of customers and to detect their browsing or transactional patterns	Chen et al. (2012)
In-memory data fabric	Allows large quantities of data to be distributed across system resources such as dynamic RAM, flash storage or solid-state storage drives. This is to enable low-latency access and big data analysis on the connected nodes.	Ariwala (2022)
Distributed storage	This is a non-relational database that contains replicated data to prevent loss of data from loss or failure of independent storage or corruption of big data sources and also for quick, low-latency access on large computer networks	Cattermul (2016)
Mobile analytics	For the analysis of clickstream data logs and sensor data generated by mobile devices in order to provide useful insights into customers' mobile activities, location or movement	Chen et al. (2012)
Data virtualisation	Transforms the data analytics results into visually comprehensible and customisable dashboards. Enables data retrievals by other applications. It also enables real-time access to data stored on various platforms.	Chen et al. (2012)
Social media analytics	For media data analysis, such as the posts of customers, employees or threat actors, to provide insights into their activities, lifestyles and opinions	Chen et al. (2012)
Data integration	Enables data to be streamlined across several big data solutions such as Apache Hadoop, Couchbase, Apache Pig, MapReduce, Amazon EMR, Apache Spark, Apache Hive and MongoDB	Ariwala (2022)
Rule-based system	Uses predefined sets of rules to initiate actions based on the interaction between input and the rules	Watson (2014)

Source: Adapted from Stein (2022).

Key: API, application programming interface, RAM, random access memory.

TABLE 6.5: Summary of the major findings on the application of big data for fraud mitigation.

Big data technology applications	Function	Reference
Service innovation	To improve customer relationships and foster real-time response to fraud threats	Yoo et al. (2012); Lehrer et al. (2018)
Web, mobile or social analytics and tracking	To track the purchasing patterns, locations and movement of customers, employees or suspected threat actors. In this scenario, data validity and correctness of analysis must be ensured.	Howison et al. (2011); Chen et al. (2012)
Machine learning	For efficient detection of cyber threats, fraud and mitigation	Dorransoro et al. (1997); Zaslavsky and Strizhak (2006); Quah and Sriganesh (2008); Zaslavsky and Strizhak (2006) as well as Quah and Sriganesh (2008); Ambalavanan (2020)
Data-mining	For effective intrusion and credit card fraud detection, money laundering mitigation and financial statement fraud detection	Chan et al. (1999); Chen et al. (2006); Gao and Ye (2007); Yeh and Lien (2008); Cerullo and Cerullo (1999)

Source: Developed from several sources found in the last column of the table.

■ Conclusion

This chapter presents a systematic literature review on the role of big data technology in fraud mitigation in this digital era. Articles which provided theoretical, conceptual or empirical results of BDA were selected. Ninety articles were systematically reviewed after applying the inclusion and exclusion criteria. The findings from the existing works indicated the suitability of big data analytic techniques, such as data-mining and ML, for detecting fraudulent activity such as cyberfraud, money laundering, insurance fraud, financial statement fraud, management fraud and fraud in the health care sector, among others. Furthermore, the literature synthesis provides conceptual guidelines for implementing big data technology geared towards fraud mitigation. Big data technology is still emerging but highly dynamic and efficient. Fraud investigators can employ some of the big data tools, technologies or analytics discussed in this chapter for data sourcing, storage and data analysis, as well as for detecting and predicting fraud patterns and behaviours. There is, however, a need to ensure that the big data technology employed is compatible with the tools and expertise of the fraud investigators. Furthermore, many authors decry the lack of the required expertise in implementing BDA, especially in resolving complex issues like fraud. Hence, developing human capacity to upskill personnel to effectively implement some of the identified big data tools and technologies will promote sustainability in using big data technology to combat fraud. The findings from the existing

works indicated the suitability of big data analytic techniques, such as data-mining and ML, for detecting cyberfraud, money laundering, insurance fraud, financial statement fraud, management fraud and fraud in the health care sector. Some of the limitations of big data technology in fraud mitigation include lack of supporting digital infrastructure, cost implications, lack of data security, insufficient or unreliable data, lack of the required expertise, the integration of the big data technology into the organisation's framework to replace or complement the traditional data analytics, among others.

Impact of information and communication technology and forensic accounting in fraud mitigation

■ Introduction

Many techniques are involved in fraud mitigation, especially in the current digital world. This chapter conducts a literature review to examine the impact of ICT and FA in fraud mitigation. A total of 108 articles were initially obtained using different search engines, but only 60 articles were reviewed because of their relevance to the topic. The findings from the literature review indicate the need for a sound knowledge of IT for effective FA investigations. There is significant consensus among the authors on the success of FA in fraud control, financial reporting and internal control improvement. However, based on other literature reviewed in this chapter, it was found that fraudulent practices and the provision of forensic services have implications for accounting education and practices. Thus, from the outcome of the literature, it could be established that FA has a relationship with providing more reliable evidence through standardised IT facilities.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Impact of information and communication technology and forensic accounting in fraud mitigation', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 127-153. <https://doi.org/10.4102/aosis.2024.BK485.07>

Furthermore, the use of FA software has a relationship with the fraud investigative process. This finding revealed in this chapter may assist corporate organisations in the quest to mitigate internal and external fraud schemes effectively.

■ Information and communication technology and fraud mitigation

In this digital era, the Internet is considered one of the fastest-growing infrastructural technologies (Ali et al. 2017). Information and communication technology has become the banking industry's asset because it provides incredible support to address banking challenges and requirements. Information and communication technology refers to systems, applications and networking components that allow information acquisition, storage and transfer. Thus, ICT infrastructure and components enable modern computing and interaction in this digital world. Currently, banks cannot think of introducing financial products or digital services without the availability of ICT (Reddy & Bhargavi 2018). UK Finance (2018) reported that banks alone spent US\$360bn on ICT facilities globally in 2016 to improve the banking operation's robustness. With the advent of the Fourth Industrial Revolution (4IR), driven by data and cyber-physical systems, IT has become a vital and integral component of routine operations for most organisations (Ali et al. 2017).

Luka and Frank (2013) indicate that ICT infrastructure is one of the current indices for evaluating a modern business organisation. This underscores the importance of ICT in business. The banking industry employs ICT to achieve operational excellence, customer service improvement, business process improvement and effective decision-making. Turban et al. (2004) indicate that certain factors, such as technology, promote the competitiveness of organisations in a dynamic and unpredictable business environment. Hence, implementing ICT in business may allow the banks to gain a competitive advantage in a rapidly changing environment and economy. Furthermore, ICT can enable business growth, customer retention, productivity improvement, cost reduction, increase in market share and effective organisation control over issues such as fraud. Therefore, using ICT in the banking industry affects the business processes connected to modern-day banking, ranging from routine to strategic activities (Luka & Frank 2012).

Teufel, Subramanian and Pedro (2011) explain that IT provides a means to collect a large amount of data for analytics and decision-making, thereby enhancing banking performance. However, the challenge is that IT devices and processes can also act as a channel to acquire and manipulate data to commit fraud. Kadiri (2014) considers the merits and challenges of IT in the

banking sector and reports that IT promotes the evolution of data technology, enhancing the productivity of banking operations and services.

Modugu and Anyaduba (2013) describe FA as an evolving field linked to financial crime resolution. Many scandals are rocking the corporate world. Typical examples include the commonly cited Enron and WorldCom incidences. These fraud incidences brought the FA field into the limelight (Sarbanes Oxley Act 2002).

Financial crime has merged as a full-fledged problem. It is orchestrated by the development of computer software combined with the availability of Internet infrastructure. Further, detecting or investigating these crimes is becoming increasingly complex because of the lack of adequate cybersecurity measures. In Nigeria, for instance, the structure of accounting services and the limitations of the statutory auditors, further inhibited by specific clauses in the organisation's laws, present a visible and ineffective fight against financial crimes in business organisations (Izedonmi & Ibadin 2012).

Furthermore, financial-related crimes and corruption have assumed increasing dimensions. Insidious resource mismanagement assumes a negative trend in public and private organisations (Akabom-Ita 2012; Ogbi 2013). Moreover, the most disheartening aspect was the legislative investigation of the aviation sector, which revealed scams totalling US\$6.5bn. These fraudulent activities involve the misappropriation of assets and revenue by both employees and the organisation, as well as the mishandling of funds designated for the procurement of goods and services. Furthermore, there are instances of incurring expenses through fraudulent or unlawful means (Azih & Okoli 2015). However, the pressure to commit fraud may result from the different lifestyles of the threat actors and employees' perception that they are insufficiently remunerated, thus resulting in fraud as compensation for their efforts (Gallet 2010).

Omar, Mohamed and Jomitin (2013) investigated the significance of IT and FA. The study shows that IT has been practically a significant tool for halting corruption with the capacity to promote transparency and accountability in various sectors of the economy. Hence, IT is a conduit to assist forensic accountants in the public sector with fraud prevention. This is partly related to the work of Akabom-Ita (2012), who explained the impact of IT on the FA profession. The study showed that accounting professionals need computerised accounting system skills for planning, directing, monitoring and evaluation.

However, protecting the organisation's IT infrastructure and reporting fraud represents only one side of the problem (Dedrick, Gurbaxani & Kraemer 2003). Equally important is to achieve the overall goal of FA for

fraud mitigation (detection, investigation and litigation services). While some literature reports on forensic auditing and skills acquisition for fraud mitigation, little has been reported on the impact of IT on FA practice. This chapter seeks to fill this gap. The purpose of this chapter is to highlight the impact of IT on FA. This is drawn from the fact that FA will be more effective in combatting fraud if IT facilities (forensic software) are introduced, that is, taking into cognisance computer forensics, which involves white hat (legal hacking), key logging, digital surveillance and intrusion detection.

The following are the research questions underlying this chapter:

1. How reliable do forensic accountants get the evidence from IT facilities?
2. To what level can FA software be employed to improve the speed of fraud detection?

This chapter seeks to investigate the impact of IT on FA practices. Specifically, to examine the reliability of IT facilities' use in detecting fraud and tracing economic damages by forensic accountants and the extent to which IT facilities can be used to enhance the speed of fraud detection.

Investment IT is a significant priority despite its deficiency of financial crime risk. However, suppose more financial crimes are perpetrated through the computer system (Internet fraud). In that case, the best way to trace this should be through these IT facilities and not with ephemeral facilities such as paper to promote the accuracy of information investigated and safeguard evidence that might be referred to in the future for court cases.

Therefore, this study evolved because of prevalent fraudulent practices and corruption that have become a usual way of life. However, the broad objective of this study is to investigate the skillful ability of trained accountants in the performance of FA using IT facilities and to examine exactly how effective it is in terms of accuracy, speed and reliability in promoting public confidence. This objective is, therefore, linked with the research hypothesis and research questions, with all being restricted to the impact of IT, which is of significant priority in the practice of FA. Despite its exposure to more crime, it is still regarded as the best way to combat financial crimes, as most crimes are committed online.

■ Fraud, information and communication technology and forensic accounting

This study conducts a systematic literature review to investigate the impact of ICT and FA on fraud mitigation. First, relevant articles were obtained using the search engines and the most relevant ones were systematically reviewed. The systematic review involves the identification of data sources for the search, using keywords for the search and implementing the

exclusion and inclusion criteria (Daniyan et al. 2021). The use of keyword search ensured that only relevant literature was obtained and reviewed. Some keywords employed include 'IT', 'ICT', 'fraud mitigation', 'corporate fraud' and 'computerised forensic investigation'. A total of 108 articles were initially obtained using different search engines, but only 60 articles were reviewed because of their relevance to the topic discussed. The 60 articles selected were based on the relevance of the articles to the study, the year of publication and the results obtained. The systematic review employed in this study followed the procedure outlined in the guidelines provided in the existing works (Abdulrahman et al. 2020; Kitchenham et al. 2009). To streamline the study, the relevant inclusion and exclusion criteria, such as the year of publication and the relevance of the keywords to the subject matter, were considered (Daniyan et al. 2022). Figure 7.1 presents the framework employed for the article's selection during the systematic literature used in this study.

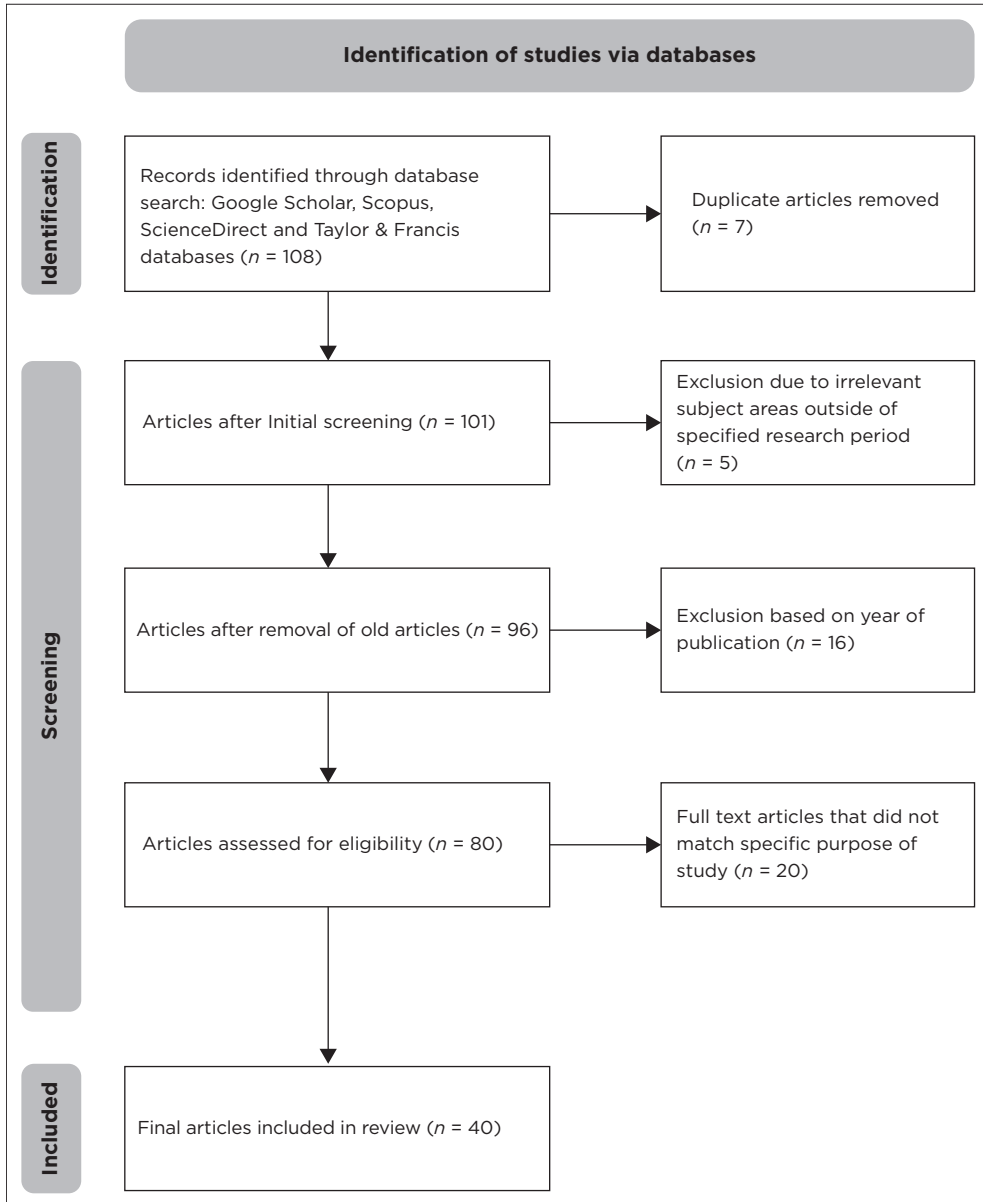
■ Systematic literature review

■ The concept of fraud

Fraud is a deliberate distortion or falsification of financial information by an individual or group, including management, employees or third parties. It consists of deception to obtain sensitive information for illegal advantage. Fraud is different from error. While fraud is intentional, premeditated and carefully executed, error refers to 'accidental misstatements or oversights in the amount or disclosures from individual or corporate accounting records or financial statements' (Efendi, Srivastava & Swanson 2007; Rezaee 2005). Fraud includes all the multifarious means human ingenuity can employ to deceive and conceal the truth. It has unsolicited communications, tricks, craftiness, pretence or other ways by which another person is manipulated (Black, Nolan & Connolly 1979; Okoye & Gbegi 2015). Fraud may be classified into organisational, management and fraud as tort. Organisational or corporate fraud is the fraud perpetrated by, for or against a business corporation (Singleton et al. 2006). Lessambo (2014) defined management fraud as an intentional fraud committed by an organisation's management that injures the stakeholders (creditors and investors). It may be perpetrated through a deliberately false and misleading financial statement or an ethical breach that violates trust.

■ Forensic accounting and information and communication technology

This section comprises various authors' views on FA in relation to ICT expressed conceptually, empirically and theoretically. The conceptual



Source: Authors' own work.

FIGURE 7.1: Framework employed for article selection.

aspect deals with the nature of FA, which has various subtopics discussed under it. In contrast, the empirical aspect gave reports on the findings of the authors' investigation or examination of articles or papers relating to FA and ICT, considering the methodologies and designs adopted or used in the articles. However, the theoretical underpinning, which is this chapter's

final contribution, is to highlight and explain various theories to enhance the understanding of FA concerning ICT.

□ The nature of forensic accounting

Anizoba, Ezugwu and Obumse (2005) stated that FA assumes the form of a three-layer structure. On the bottom layer is the firm background of accounting, while the second, smaller layer translates to the auditing background, risk assessment and fraud detection. The third, even smaller layer represents a legal background - understanding the courtroom and how to testify.

Forensic accounting is a fundamental part of the accounting profession, which aims to detect fraudulent activities within or outside an organisation (Modugu & Anyaduba 2013). Thus, it is the science that deals with applying the knowledge of financial accounting, auditing and litigation to examine and investigate fraud matters within the context of civic and criminal law (Lohana 2013). Forensic accounting is gradually emerging and has its own models, methodologies and investigative procedures for fraud examination (Kramer, Seda & Bobashev 2017). It searches for evidence and critically analyses it to produce legal evidence. Curtis (2008) asserts that forensic accountants can investigate fraud as fraud encompasses the acquisition of money, property or economic advantage through deceit or deliberate misrepresentation and concealment. The aspects of inquiry in FA are broad and include fraud examination, diligence reviews, risk assessment, identification of financial statement misrepresentation, cybercrimes and illegal money transfers (Smith 2005).

Crumbley, Heitger and Smith (2009) differentiated FA from forensic auditing. A forensic auditor is an accountant principally skilled in auditing, while a forensic accountant combines accounting, consulting, auditing and legal skills in the broader sense. Singleton and Singleton (2006) posited that FA provides a detailed approach to fraud investigation. This encompasses the prevention, detection and analysis of anti-fraud controls in line with gathering financial and nonfinancial information.

Dada, Owolabi and Okwu (2013) observed that the primary duty of the forensic accountant is to gather evidence, analyse, interpret, summarise and present financially viable evidence in fraud-related cases. Forensic accountants' activities are significant to the different types of business and personal legal disputes. The bulk of the work of a forensic accountant is connected to the investigation of past or projected financial activities as well as the appraisal and preparation of business valuations (Dada et al. 2013).

Okoye and Gbegi (2013) stressed that forensic accountants are professional fraud investigators specialising in fraud detection

and investigation. They are also versed in the documentation of evidence required for litigation and prosecution of the culprits. They can precisely work in complex regulatory and litigation environments and identify and capture the correct information on missing, altered, destroyed or deceptive accounting records. In addition, Enofe, Utomwen and Danjuma (2015), in their study 'Forensic Accounting and Corporate Mitigation', revealed that corporate crime mitigation could be achieved by strengthening corporate governance through FA. The existence of corporate governance could be attributed to the auditing professional role of being a watchdog rather than a bloodhound.

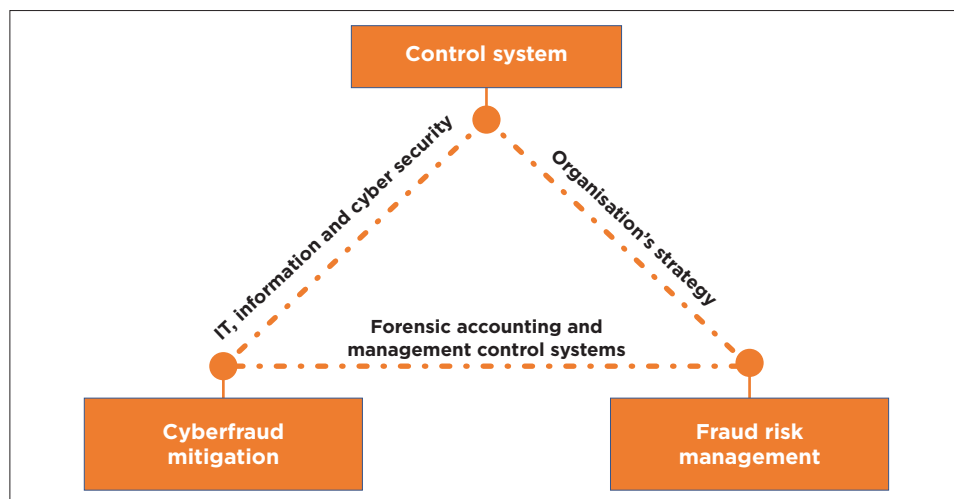
The Centre for Forensic Studies (2010) in Nigeria reported that the proper application of FA could be used to reverse the leakages that cause corporate failure. According to Howard and Sheetz (2006), FA involves interpreting, summarising and presenting multifaceted financial issues in a brief, detailed and factual way for fraud resolution or litigation purposes. Through FA, suspected fraud cases can be investigated with evidence gathered properly without breaching the rule of evidence to gain acceptance in court. Forensic accountants are always taught to investigate the numbers involved in a case and the business realities of the suspected cases. Thus, analysing, interpreting, summarising and presenting complex financial-related issues are the essential characteristics of FA (Bhasin 2007, p. 1005).

According to Punitha et al. (n.d., p. 60), the internal control system aims at ensuring the following: validity, completeness, accuracy of records, authorisation of recorded transactions, classification and valuation of transactions, recording and posting of the transaction as at a due date, as well as compiling a correct summary of transactions in the ledger accounts. Punitha et al. (n.d., p. 60) also stated that the merits of an internal control system include the provision of assurance to management regarding the consistency and accuracy of operating and financial information, minimisation of errors and fraud, security of the organisation's assets against misuse, prevention of wastage, the promotion of operational efficiency, identification of internal weaknesses and the provision of guidelines to ensure strict adherence to the established organisation's policies. Drawing from the earlier definitions, it is clear that internal control functions are not limited to accounting functions in an organisation as they integrate both accounting and administrative controls. While accounting control is concerned with the controls that relate directly to the accounting system (checking transactions according to the prescribed procedures and protection of the assets), administrative control deals with the appraisal of operational performance and holistic performance. The accounting control consists of budgetary control, internal checks and audits, standard costing and deviation analysis, bank reconciliation and self-balancing ledgers. On the other hand, administrative control consists of motion and time studies, quality control, performance appraisal and statistical analysis (Punitha et al. n.d., p. 61).

According to Punitha et al. (n.d., p. 60), the control systems include monitoring and fraud risk management as significant elements. The fraud risk management cycle is an interactive process of risk mitigation (risk identification, assessment of its impact and prioritisation of control actions to reduce risks). According to CIMA (2008, p. 19), steps to reduce risk include the following:

- the setting of risk objectives
- identification of risk areas
- understanding and assessment of the scope of risk
- development of a risk response strategy
- allocation of responsibilities
- implementation of risk plans
- implementation of monitoring and control
- review and process definition
- decision-making.

Cyberfraud can be traced to recent advances in ICT and the vulnerability of the public and organisation's internal control mechanisms (Ali et al. 2017). Therefore, an effective control system must prioritise information and cybersecurity. This is because cyberfraud is an online fraud that compromises an organisation's IT infrastructure to steal confidential information or syphon resources from customers or organisations. In addition, developing the right strategies for fraud risk management is also necessary for fraud mitigation. Incorporating the FA and MCS techniques for cyberfraud mitigation into an organisation's control system and strategy may assist in effective fraud mitigation (Figure 7.2).



Source: Authors' own work.
Key: IT, information technology.

FIGURE 7.2: Forensic accounting and management control systems for cyberfraud mitigation.

Makgatho (2013, p. 97) explained that organisations can achieve a good audit outcome and efficient allocation and monitoring of financial resources only if an effective internal control system is implemented. This agrees significantly with this study's finding concerning developing robust internal controls. The results significantly agree with the position of the AICPA (2012) that the internal control measure is a significant player in the detection and prevention of fraud. However, enforcing internal controls may not be sufficient for fraud mitigation. This is because internal controls can be weakened through collusion, management overrides and technological advances; hence, overreliance on internal controls could jeopardise the fight against cyberfraud. However, adopting other measures was recommended for effective fraud mitigation (AICPA 2012).

Furthermore, Punitha et al. (n.d., p. 62) identify some good internal control system requisites. A sound control system is designed so that the financial and accounting operations are separated. Different entities should handle cash, other transactions and recordings to allow for transparency and checks and balances. A well-designed organisational structure is necessary, with clearly defined job responsibilities. To avoid a collision, the rotating principle, which allows for the movement of an employee from one task to another, should be encouraged as mechanical devices such as counting machines, calculating machines, cash registers and time clocks should be used where necessary. The system should allow for continuous and constant checks of the work done by the employee to uncover errors and fraud. Records involving the work done by each employee should be kept, and a clear rule in terms of cash, ordering, receiving and issuing goods should be provided, if necessary. An efficient internal auditing staff is also critical to an effective internal control system (Punitha et al. n.d., p. 62).

■ Challenges and prospects of computerised forensic investigation

People are increasingly more attracted to and conversant with the digital environment. However, this comes with some benefits and challenges. In terms of fraud, many perpetrators use digital platforms as tools for fraud perpetration. Smith (2005) argues that 'almost every financial fraud incorporates computer and digital equipment'. Volonino, Anzaldúa and Godwin (2006) categorise computer crimes into two, namely, computer crime as a target and as a tool. Computer-related crimes include attacks on networks that cause them to crash or allow intrusions or attacks that tamper with information systems, programs or data. Fortunately, like a double-sided sword, technology is also the investigator's friend in detecting fraud. As computers can be used as both a target and a tool in fraud, data stored in computers is perfect evidence to detect fraud. Suppose an

investigator knows the right way to acquire, preserve and analyse data stored in a computer suspected to be a target of fraud or used as a tool in fraud. In that case, the data will become helpful evidence in the court. Pearson and Singleton (2008) stress the need to obtain, manage and analyse digital evidence as a critical success factor for the accounting profession.

Thus, the benefit of technology, such as computers and other digital equipment, outweighs its negative side. Furthermore, Okoye and Akamobi (2009) comment on the deployment of FA in developing economies like Nigeria, and they opined that it is a suitable tool for fraud mitigation; however, it is confronted with many problems. Crumbley (2009) and Grippo and Ibex (2003) identify some of the challenges underlying the use of FA:

1. The onus of gathering evidence and its admissibility in the court of law.
2. The compliance of the gathered evidence with the laws of evidence. This is important in the prosecutions of the culprits and in processing civil claims.
3. The anonymous nature of cyberspace and the globalisation of the economy. The threat actors can operate from any location worldwide using an anonymous identity. This may lead to the challenge of inter-jurisdiction.

Degboro and Olofinsola (2007) indicated that another critical challenge in mitigating the effective application of FA in financial fraud control in Nigeria is that the law is not compliant with technological advancements. Furthermore, FA is perceived as being expensive and only affordable for big firms. Therefore, most firms may prefer to outsource FA services or opt out of the court settlement to avoid the expenses and the risk of poor publicity and corporate misrepresentation.

■ Techniques involved in forensic accounting for fraud examination

For voluminous data, forensic accountants usually employ big data technology to social representation theory, classify and analyse such data to derive useful information (Chakrabarti 2014). Among others, some of the techniques used in FA for fraud investigation will be discussed in the following sections.

■ Benford's law

Benford's law is an arithmetical tool usually used to determine if a specific variable under investigation is a case of error or fraud. The law states that untrue figures (as in a fraud case) indicate a contradictory pattern from

random figures. Once the field or variable of financial significance is determined, the leftmost variable digit is mined and summarised for the entire population. This is usually done by classifying the first digit field and calculating its observed count percentage. After this, Benford's set is applied. A parametric test known as the z-test is also performed to determine the significance of the variance between the two populations, namely, Benford's percentage numbers for the first digit and the observed percentage of the first digit at a specific confidence level. If the outcome conforms to the percentage of Benford's law, then it implies that the data are Benford's set. In other words, there is a 68% (almost two-thirds) probability of no error or fraud. Notably, the first digit may not always be the only pertinent field. Therefore, Benford's law gives a discrete set for the 2nd, 3rd and up to the last digit. It also applies to mixed numbers, decimal and rounded numbers. The merits of Benford's law are that it is unaffected by scale invariance coupled with the fact that it can assist in a situation where there is insufficient evidence to prove the legitimacy of the transactions (Yadav &Yadav 2013).

■ Computer-assisted auditing tools

These are sets of programs usually employed by the auditors during the auditing procedures to process substantial data in the client's information systems without human involvement. Computer-assisted auditing techniques (CAAT) can assist the auditors in carrying out some auditing procedures given as follows:

- analysis of transaction balances and details
- detecting discrepancies or irregular patterns in the data set
- analysis of general and computer systems application controls.

■ Theory of relative size factor

This theory reveals all bizarre irregularities arising from errors or fraud. Relative size factor (RSF) is calculated as the ratio of the biggest number to the second biggest number of the specified set. In practice, each entity has definite restrictions (e.g. tax to be paid by a taxpayer). These restrictions may be distinguished from the available data (if undefined). When deviations exceed the acceptable range, further investigation will be needed into the probable reasons for such deviations.

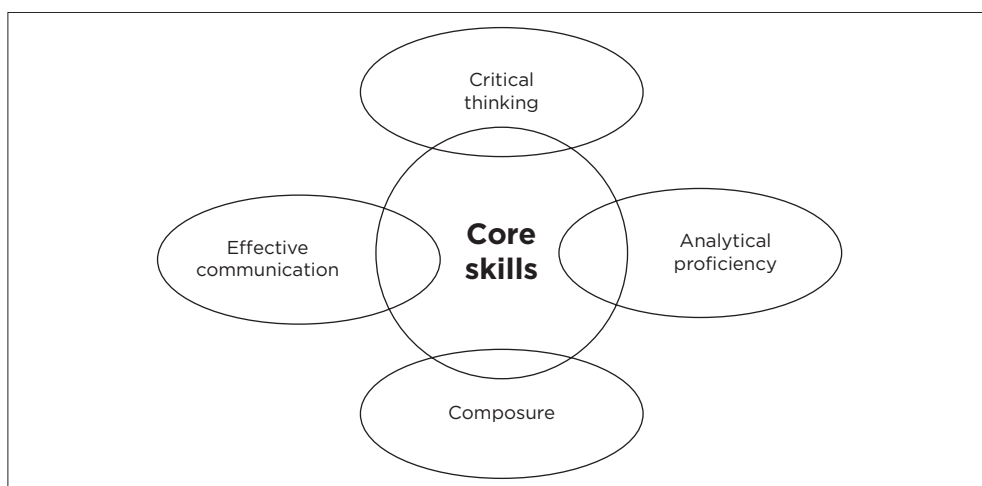
■ Basic skills required by forensic accountants

Davis, Farrell and Ogilby (2010) and Ozili (2015) stated that the skills required by a forensic accountant can be classified into core and enhanced skills.

■ Core skills

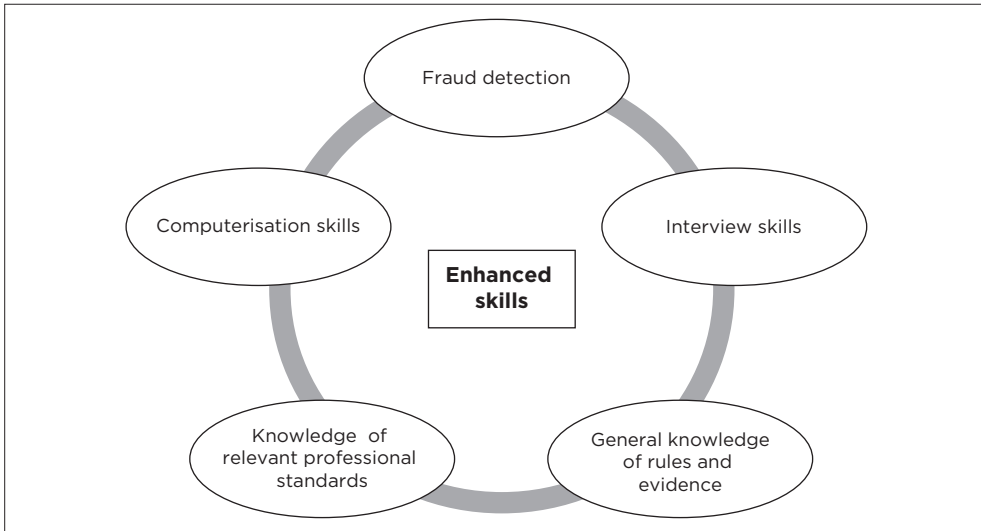
These are skills considered to be fundamental to becoming a forensic investigator. However, the components of the core skills are contained in Figure 7.3:

- **Critical thinking:** This refers to the ability of the forensic accountant to conceptualise, synthesise and analyse information gathered and differentiate between facts and opinions.
- **Deductive analysis:** The forensic accountant uses this to confirm or refute the evidence gathered. The forensic accountant often employs this skill to identify any financial contradiction that does not fit the typical data set pattern or evidence under investigation.
- **Analytical proficiency:** This is a vital skill required of a forensic accountant. It is the ability to investigate and interpret the data set or evidence gathered to conclude. This can also be regarded as a normative thinking rule.
- **Effective communication:** This effectively disseminates informative evidence without redundancy in writing and through charts, graphs or reports. This will form the foundation of opinion.
- **Specific legal knowledge:** The ability to comprehend basic legal requirements, processes and issues, including the rules of evidence. This will form the foundation of evidence admissibility in the court.
- **Composure:** This includes working under pressure and maintaining a calm attitude in stressed or uncertain situations.



Source: Adapted from Ozili (2015).

FIGURE 7.3: Core skills of a forensic accountant.



Source: Adapted from Ozili (2015).

FIGURE 7.4: Enhanced skills of a forensic accountant.

■ Enhanced skills

Enhanced skills are skills developed through years of experience in academia or industry. Examples of improved skills are depicted in Figure 7.4:

- **Fraud detection:** The ability to discover and expose fraudulent practices without favouritism and accepting bribes (Santos Filho, Carlos & Costa 2017).
- **Computerisation skills:** This is the capacity of a forensic accountant to trace economic damages using IT facilities.
- **Knowledge of professional standards:** This is the ability to understand every required professional standard and present them in detail as evidence against violation from accounting entries.
- **General knowledge of rules and evidence:** This is the ability to understand every legal rule guiding the tendering of evidence for litigation purposes as a forensic accountant is also an expert witness.
- **Interviewing skills:** This refers to the skills of approaching any suspected fraudster; it is not always best to approach a suspected offender with annoyance – humour may be more effective.

■ The fraud deterrence cycle

The fraud deterrence cycle is a collaborative process which encompasses the development of corporate governance, incidence response, risk assessment, application of transaction-level control processes, otherwise known as the system of internal accounting controls, reflective examination



Source: Authors' own work.

FIGURE 7.5: Fraud deterrence cycle.

or review of governance and control processes through audit investigation and remediation of suspected or alleged cases. Figure 7.5 presents the fraud deterrence cycle.

■ Empirical review on forensic accounting

Akhidime and Uagbale-Ekatak (2014) and Sule, Ibrahim and Sani (2019) examine the increasing significance of FA for fraud and corruption mitigation using the Nigeria experience as a case study. The outcome of the studies indicated that FA in Nigeria is still in the evolution phase, and there is no clear boundary between the applications of FA and auditing in Nigeria. They further opined that the gradual emergence of FA in Nigeria is because of two main reasons, namely, FA does not form part of the educational curricula of colleges and professional bodies responsible for producing and developing accountants in Nigeria, and there does not exist any statutory backing for FA services in Nigeria compared to the traditional financial audit.

On the current availability of FA education and the state of FA services in Hong Kong and mainland China, Wang, Lee and Crumbley (2016) indicated the need to formally integrate the concept of FA into the academic curriculum and also emphasised the need for the recognition of FA as a professional service.

The specialisation, professionalism and organisation characterise economic crime (Adegbie & Fakile 2012). The more complex the context in which criminals operate, the more professional experience they require, which is why large-scale economic offences need an organisation to achieve their results better and reduce risks. In addition, Modugu and Anyaduba (2013) posited significant consensus among stakeholders on the effectiveness of FA in fraud control and its ability to improve financial reporting and internal control. Therefore, the authors suggested that forensic accountants should be informed about the trends that frauds assume every day and be alert to corporate fraud and other illegal activities around them.

Turvey (2012) studied forensic fraud and evaluated the law enforcement and forensic science cultures within the context of the investigator's misconduct. The result showed that forensic fraud tends to result from cultural, pathological and systemic causes rather than the narrow motives of single individuals, as the circumstances surrounding it must be allowed to develop and persist by those in the immediate forensic environment. It also supports the assertion that although private (e.g. defence) forensic practitioners are routinely characterised as biased or mercenary, those working on behalf of the state (e.g. the police and the prosecution) are responsible for a substantial amount, if not the majority, of known cases of forensic fraud. Additionally, it is fair to say that routine activities theory, differential association theory and role strain theory provided valuable insights into cultural and other environmental influences brought to bear on the forensic examiner (Turvey 2013).

Madumere and Onumah (2013) investigate 'Forensic accounting: A relief to corporate fraud'. They found that corporate fraud is becoming a menace in Africa, and most high-level managers prefer to work for a short while and become owners rather than working for a long tenure. The study also reveals that the lack of a robust internal control unit also leads to corporate failure, where the staff in charge of the internal control is related to the manager and dictates to the staff what should be in the financial report. Similarly, Okunbor and Obaretin (2010) report that the prevalent situation of corporate failure has placed greater responsibility on accountants to be more skilled in identifying and providing a definite solution to fraud cases and critical indicators of poor corporate governance and mismanagement. Accountants at all levels must acquire the necessary skills and knowledge for evidence management. These include the skills for evidence identification, discovery and preservation.

Onuorah and Appah (2012) investigate the fraudulent activities and FA services of banks in Port Harcourt, Nigeria. Their study indicates that banks' application of FA services is a deterrent to threat actors within and outside the corporate organisations. The authors established that FA services can

reduce the level of fraud in banks. This is similar to the submissions of Tarr, Van Akkeren and Buckby (2016).

Relatively, Effiok et al. (2012) examine 'The implication of occupational fraud and financial abuse on the performance of companies in Nigeria'. In addition to the body of knowledge, this study's analysis and empirical results have shed some insight into the effect of occupational fraud and financial abuse on the performance of companies in Nigeria. The study's outcome provides relatively strong support for the existence of a negative impact of occupational fraud and financial abuse on the performance of Nigeria's companies. Generally, this result is broadly consistent with results obtained by Hollinger and Clark (1983) that employees commit fraud mainly because of poor workplace or working conditions. The findings of this study's hypotheses indicated no substantial relationship between financial manipulation and a company's performance.

Davis et al. (2010) and Ekeigwe (2011) stressed that analytical skills remain one of the most important skills a forensic accountant needs. The studies further highlight the diverse nature of the skill sets of FA. These include investigation, communication, accounting, business, auditing, technology, psychology, criminology, litigation and critical thinking skills.

Chukwunedu and Okoye (2011) report that integrating FA techniques into the auditing framework can increase the capability of auditors to detect errors and fraud, thus helping to bridge the gap between auditing and FA. This proposal, however, has implications for both accounting practice and education. Also, Okoye and Gbegi (2015) examine FA as a technique for detecting and preventing fraud in the Nigerian public sector ('A case study of Kogi State, Nigeria'). The result revealed that the professional service of a forensic accountant is different from that of a conventional auditor in terms of the technique and skill applied for fraud investigation and detection. The result further indicates that the stakeholders prefer professional forensic accountants' services to the auditor in terms of the depth of investigation. Hence, the authors established the feasibility of FA to reduce fraud occurrence in the public sector significantly. Although most of the respondents drawn from the top management, senior staff, and middle and lower cadre understand FA concepts, the technique is rarely employed in Kogi State, Nigeria, for fraud mitigation. The authors further concluded that effective fraud mitigation necessitates the professional service of forensic accountants in the public and banking sectors.

Furthermore, in their study, Uket and Udoayang (2012) found that the design of internal control can influence the attitude of members of staff towards fraud perpetration or mitigation. Hence, developing and implementing a robust internal control mechanism can deter staff members

from committing fraud. Conversely, a weak internal control structure can expose the organisational system's vulnerability to fraud and provide loopholes for insiders or outsiders to commit fraud. Unfortunately, most Nigerian financial institutions lack an internal control system that can monitor the lifestyles of their employees. Enofe et al. (2015) reliably draw a correlation between implementing FA techniques and fraud detection using the quoted companies in Nigeria as a case study. The study's outcome indicated that implementing FA services is ineffective in mitigating fraud. This has significant implications for corporate governance. Furthermore, the advent of electronic business (e-business) and its increasing applications have not done much for fraud reduction in Nigeria. Although policies in the form of legislation are enacted, some practical measures taken to curb fraud seem ineffective. However, most of the existing literature found that FA has a strong relationship with fraud detection, which is necessary for increasing public confidence and eradicating crime and corruption in the Nigerian economy. Additionally, Emeh and Obi (2013) investigate the empirical analysis of FA and financial fraud in Nigeria. The study examines the coefficients of correlation for the variables. These variables include 'presence of forensic accountant' (PFA), 'number of accountants with forensic accounting skills' (NAFT), 'extent of forensic accounting practices' (EFAP), 'extent of employee theft' (EET), 'extent of financial fraud' (EFR) and 'extent of top management fraud' (ETMT). The study's outcome indicates a significant negative correlation between EET and PFA ($r = -0.561, p < 0.05$). This implies that the presence of a forensic accountant results in a reduction in the EET. The relationship between EET and NAFT was found to be weak and insignificant ($r = -0.108, p > 0.05$). This implies that the NAFT has negligible influence on the rate of employee theft. This calls for developing human capacity through regular training to improve the expertise of forensic accountants. The results of Spearman's rank correlation coefficient indicate the presence of significant negative correlations between PFA and NAFT as well as EFAP and EFR. The outcome of this study agrees with the findings of Degboro and Olofinsola (2007) and Onuorah and Appah (2011).

Adegbie and Fakile (2012) investigated FA as a solution to economic and financial crime in Nigeria. The study revealed that if FA can help curb economic and financial crime in the economy, this would repair Nigeria's soiled image in the international economic community and enhance foreign direct investment (FDI), thereby leading to improved corporate governance and public confidence. Similarly, Modugu and Anyaduba (2013) examine FA and financial fraud in Nigeria using an empirical approach. The result indicated a significant consensus among the stakeholders that FA effectively controls fraud, improving financial reporting and internal control.

In addition, Osisioma (2012) investigate conceptually the implementation of FA tools for fraud prevention in Nigeria. The outcome of Osisioma revealed

that around the globe, the vital role of corporate accountants has suffered damage to their reputation, facing scorn and mockery because of their careless and sloppy handling of professional responsibilities. This period has undeniably been a challenging one for the field of accountancy. Nevertheless, amid this crisis, opportunities for alternative paths have emerged, and one of these options involves the expansion and advancement of FA. Chakrabarti (2014) studies the challenges and potentials of the FA profession in India. The result revealed that significant challenges in the implementation of FA in India include complex and traditional judicial system and political fancy, information gathering against powerful politicians and bureaucrats that is admissible in a court of law, issues on financial defalcation or fraud involving expert witnesses, cost implications and the risk of negative publicity for the image of corporate organisations, financial scandals involving corporations from other countries, problems of inter-jurisdiction which make the prosecution of fraudsters from other countries outside the Indian jurisdiction difficult, as well as the dynamic world of IT and the exponential growth in the use of computer systems. Similarly, Huber (2012) attempts to conceptualise whether FA in the USA was becoming a profession. It was found that FA fulfilled the majority of the qualities of a profession, education, training and certified fraud examiner (CFE), including the existence of an organisation, certification as a symbol, specialised knowledge, examinations and ethics.

Lalit and Virender (2012) examine conceptually 'forensic accounting and fraud examination in India'. The authors found that 'forensic' services require special training and real-life 'practical' experience. Furthermore, forensic accountants are also expected to play more 'proactive' roles in risk reduction, designing and performing extended procedures as part of the statutory audit, acting as advisers to audit committees and assisting in investment analyst research.

Fradella, O'Neil and Fogarty (2004) investigate the impact of Daubert on forensic science. The results show inconsistencies in how Daubert was (Fradella et al. 2004):

[A]ppplied to forensic sciences in the post-Kumho era. The first [*significant*] inconsistency concerns expert testimony from forensic accountants or economists concerning [*calculating*] damages in civil cases. Some courts prohibit any testimony from forensic accountants or economists on the issue of damages calculations. Other courts welcome such testimony [...] [w]hile other courts permit only general testimony regarding what should be included in a jury's calculations for damages but prevent the expert from [...] [*testifying concerning any particular number of damages*]. The second inconsistency [...] revealed by the qualitative content analysis concerned from whom courts will accept testimony as to the causation of illness is in cases where someone has allegedly been made ill by exposure to a toxic substance [...] [*The third major inconsistency concerns the*] type of testing required before an expert in forensic engineering can testify concerning a design or manufacturing defect. (n.p.)

In like manner, Brennan (2014), in the study of FA in a constitutional parliamentary democracy, the case of Ireland, revealed that all the big-four accounting practices and many smaller accounting practices in Ireland have departments specialising in FA. There are yet no professional practice guides on FA. Only one education and training programme is available, which is not mandatory for FA practitioners.

■ Empirical review on information technology and forensic accounting

Njanike, Dube and Mashayanye (2009) indicate the effectiveness of forensic auditing in detecting, investigating and preventing bank fraud. Bhasin (2013) implies that accounting students and accountants in practice require a sound knowledge of IT in the digital environment for effective investigation. They must also be updated on IT-based schemes to understand the need to engage FA experts to support the accountant's work, auditing or investigating Internet- and computer-based fraud. Similarly, Omar et al. (2013) investigate the relevance of IT and FA. The authors find that IT is a practical and essential instrument for curbing fraud. Proper IT deployment can enhance government administration's transparency, responsibility and accountability. Information technology can help forensic accountants in fraud prevention in the public sector. Furthermore, it can improve the robustness of the organisation's internal control in achieving segregation of duties and budget approvals in real time. This will minimise errors and promote transparency. This study, supported by Ayatollahi, Bath and Goodacre (2009), indicates that the paper-based system is more prone to fraud than the IT-based system. Computerised systems employed for transactional activities can reduce fraud because of real-time checks and balances and the ease of gathering evidence for auditing. Thus, IT can reduce fraud and corruption by promoting good governance, consolidating reform initiatives, reducing the tendency for fraudulent practices and fostering relationships between government administrators and citizens (Shim & Eom 2008). Furthermore, IT can enhance internal and managerial control over fraud and promote government or organisation's accountability and transparency (Shim & Eom 2008). Pearson and Singleton (2008) indicate that knowledge and technological application are increasingly essential in effectively implementing FA, anti-fraud programmes and fraud investigations. Furthermore, Adegbe and Fakile (2012) assert that criminals use the latest technologies to connect with criminals worldwide without physical contact. The authors further stated that the success of many crimes demonstrates how criminal organisations can quickly build international connections to plan and perpetrate crimes using new technical know-how and equipment.

■ Underpinning theories of fraud

Uket and Uduoayang (2012) describe fraud as a deliberate attempt to realise a personal or organisational goal through deceit or other dubious means. The layman's definition of fraud includes deceit in the form of premeditated dishonesty, deliberate misinformation or misrepresentation of a material fact. It could be lying, dishonesty, cheating, gaining an unfair or unjust advantage over another or asset misappropriation. Fraud involves manipulating or coercing people not to act in their best interest.

Scholars have developed the following theories to help explain how and why fraud is conceived in society:

- sociological theory of crime and fraud (or both)
- psychological and physiological theory (or both) of crime
- culture transmission theory
- fraud triangle theory.

■ Sociological theory of crime or fraud (or both)

This theory states that society creates conditions under which a person commits a crime. That is, people are influenced by society to commit crimes. The words 'sociological' and 'society' are linked, so it can also be said that sociological theory looks at crime as a social problem, not an individual one (Natalie n.d.). Based on this theory, fraud is considered a crime, and it is essential to reflect that the idea of what constitutes a crime is continuously being tailored to the needs of any society. The theory believes that crime and criminal motivations are integral to a 'normal' social order and can express the same incentives that give rise to accepted behaviour.

■ Psychological or physiological theory

This theory states that criminal behaviour results from individual differences in thinking processes. There are many different psychological theories, but they all believe that the person's thoughts and feelings dictate their actions. As such, problems in thinking can lead to criminal behaviour (Natalie n.d.).

Oluwadare (1993) and Uket and Uduoayang (2012) argue that there are some justifications by scholars that crime is a personal issue rather than a social problem. In other words, the attitude differs from people who believe that some are naturally wicked to others who indicate that a genetic reason for committing a crime is linked to the endocrine glands. Lombroso (1876) states that the act of committing a crime is inherent (natural or inborn) following the outcome of the experiment conducted on the skull of a notorious criminal and found some features perceived to be the result of a

'throwback' to a previous evolutionary type. Lombroso (1876), therefore, establishes a type of criminal, defined as 'insensitivity to the pains of others with excessive acute sight, love of orgies and irresistible love for evil'.

■ Culture transmission theory

This theory perceives crime as the end product of a process of social living. Tarde (1886) argues that criminal intentions and behaviour are acquired in the family and the community where a typical behaviour is shared by a group and accepted as a norm.

■ Fraud triangle theory

The FTT was developed to probe the root causes of fraud. Cressey (1953) 1950 first invented and published the FTT in 1953, in the journal *Other People's Money*. Cressey, in 1950, was disturbed by the question of the rationale behind people committing financial crimes and was propelled to examine 250 criminals within five months. Cressey established that 'trust violators' (threat actors) commit financial crimes when they think of a financial problem others cannot discuss. Their knowledge or awareness that the problem can be secretly solved through the violation of position or trust reposed in them often leads to fraud. Sometimes, they rationalise their opinion as trusted persons, allowing them to take advantage of the entrusted funds or property. Johnson, Ryan and Tian (2003) state that compensation pressures and incentives are considerably associated with firms with a fraud history.

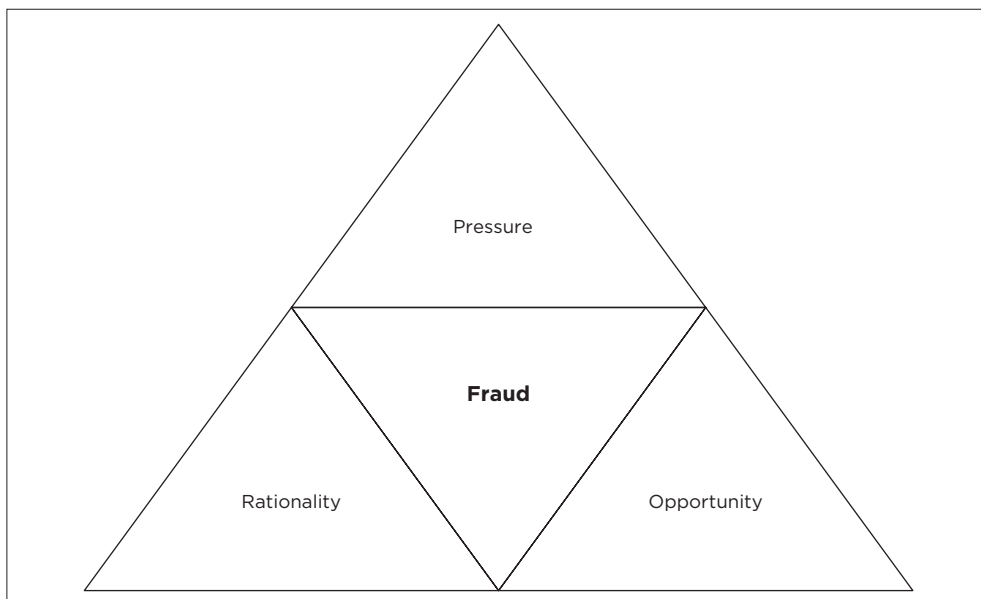
Figure 7.6 is the fraud triangle, which indicates why people engage in fraudulent practices.

□ Perceived pressure, incentives and motivation

This is the primary reason for committing fraud (Johnson, Ryan & Tian 2009). Pressure can include almost anything (financial and nonfinancial) that can encourage an individual to commit fraud. SAS No. 99 indicates that four common types of conditions of pressure can lead to fraud. These include financial instability, external pressure, personal financial needs or targets.

□ Perceived opportunity

This is the ability of a threat actor to recognise and exploit certain loopholes in the organisation to violate trust. Opportunities to commit fraud can be created because of the vulnerability of the internal control system, poor corporate governance, lack of job rotation, poor job monitoring or inadequate employee supervision, among others.



Source: Adapted from Manurung and Hadian (2013).

FIGURE 7.6: Fraud triangle theory.

□ Rationalisation

This is the attitude or ethical opinion that enables people to commit fraud. Rationalisation can also be a factor that allows the threat actors to justify their course of evil action. Rationalisation and attitude are described by Kenyon and Tilton (2006, n.p.) as ‘potential red flags and fraud detection techniques’, indicating that some people are more susceptible to committing crime than others. This implies that the tendency to perpetrate fraud is a function of people’s ethical values and their individual situations. The authors affirmed that ethical behaviour is inspired by an individual’s character and external factors. External factors may include job insecurity, usually experienced when there is downsizing or redundancy in an organisation or a work environment that motivates hatred. Similarly, the external environment could include the management’s attitude towards fraud risk and response to fraud incidences.

In this chapter, there are two significant variables, namely, IT and FA. Information technology consists of several factors on which FA depends for effectiveness and efficiency, including the speed of processing informative investigation and accuracy of financial reporting to serve as evidence in case of litigation.

■ The independent variables

The following are the independent variables considered in this study and their discussion. Information technology, which includes computer software and hardware components that could be employed to perpetrate fraud; however, the fraud committed via the software component could prove more apparent. Operation system software comprises computer programs which keep the computer operational automatically. In contrast, application software includes computer programs that apply the programs to the users' needs by performing tasks the user wants to complete. Both the operation system software and software applications present potential challenges for forensic accountants to identify. Computer hardware and software could be used to perpetrate fraud (Akabom-Ita 2012). However, the use of IT facilities may promote information processing in the following ways:

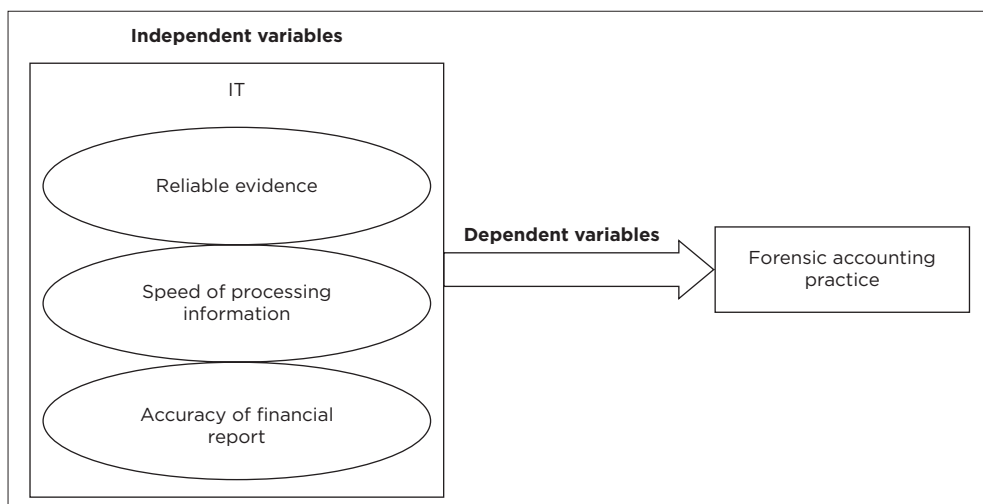
1. **Accuracy:** The accuracy of a computer is very high, with every calculation performed at the same accuracy. Errors occur because of human error rather than technology weaknesses; the primary sources of error are incorrect program usage by the users or inaccurate data.
2. **Speed:** Computers can assess and process data millions of times faster than humans. It can store data and information in its memory, process them and produce the desired result. Most modern computers can perform 100 million calculations per second.
3. **Reliability and storage capacity:** Computers have an enormous storage capacity. They have the capability of storing vast amounts of data or information. Computers have a considerable ability to store data in a minimal physical space. Apart from storing information, today's computers can also store pictures and sounds in digital forms.

■ The dependent variable

The dependent variable in this research is explained as 'forensic accounting practice'.

In the views of Razee et al. (2009), FA is a specialised field that involves detecting, investigating and reporting financial fraud so that the evidence gathered will be admissible in court. Forensic accounting experts provide services in the areas of accounting, auditing, investigation, damage claims, analysis valuation and general consultation and have critical roles in divorce, insurance claims, personal damage claims, fraud claims, construction, auditing of publication rights and in detecting terrorism by using financial precedence (Hassan & Morteza 2012). The effectiveness of FA relies on IT facilities as this is now the modern way of perpetrating fraud by criminals.

Figure 7.7 presents the independent and dependent variables investigated in this chapter.



Source: Authors' own work.
Key: IT, information technology.

FIGURE 7.7: Framework for the investigation of the effect of IT on forensic accounting practice.

■ Variables

The findings from the literature indicate that there is a consensus among the authors that ICT has a positive impact on FA as it relates to fraud mitigation, provided there is a capacity for it (Bhasin 2013; David 2005; Omar et al. 2013; Pearson & Singleton 2008; Shim & Eom 2008). In addition, the authors indicate the need for effective deployment of IT tools that match the FA techniques and the human capacity-building on implementing both the IT and FA tools. This leads to an answer to this chapter's first research question: 'How reliable is the evidence forensic accountants get from IT facilities?'

Existing literature indicates that IT-enabled forensic investigation is less prone to error, thus improving the quality and outcome of forensic investigations (Bigler 2001; Golden et al. 2006; Howard & Sheetz 2006; Singleton et al. 2006). Hinders (2009) indicates that the information and outcome of investigation provided by forensic accountants must be precise and accurate, hence the integration of IT into the FA investigative framework. This is because information nowadays is mainly stored in computers and data management (acquisition, storage, analysis and sharing) can easily be achieved with high reliability through IT-enabled platforms.

Forensic accountants can use dedicated software and computer hardware to manage information and evidence. This encompasses the process by which evidence is acquired, preserved, analysed and documented to promote the integrity and reliability of the investigative process (Hinders 2009).

The second research question is: 'To what extent can IT enhance the work of forensic accounting in fraud detection?'

Existing literature indicates that IT makes the work of a forensic accountant time-effective in sifting and searching for evidence. Furthermore, IT has also enabled the analysis of large amounts of diverse data gathered from different sources (big data) in a fraction of time. Information technology-enabled investigation often reduces the investigation procedural steps through automation. Technologies such as optical character recognition (OCR) enable forensic accountants to facilitate documentation, comprehensively search documents for keywords and sort documents by date range (Akabom-lta 2012). In addition, cloud storage and the IoT have simplified the processes of gathering, sharing and storing big data and information. This makes the work of a forensic accountant faster and easier in grouping and processing evidence that is admissible in the court of law (Howard & Sheetz 2006; Nunn et al. 2006; Singleton et al. 2006; Vacca 2005; VeraMunoz, Hov & Chow 2006; Wang, Gopal & Zionts 1997). Winter (2004) further indicates that IT-enabled forensics investigation permits identifying incidents, gathering and analysing evidence, potential recovery of records and proper records management.

Hinders (2009) indicated that IT supports these congruent views and is integral to FA. This is because forensic accountants often use computer software or programs to manage data to obtain legally valid evidence. One of the significant areas in which IT can support FA is the knowledge of databases coupled with understanding how the database system works (KPMG 2018). Forensic accountants may understand information management but realise all the basics of systems and database operations. An understanding of the operation of the system and its database may foster evidence gathering and fraud detection. Looking at a fraud scenario from a fraud-awareness viewpoint, forensic accountants may need the assistance of IT and, at times, IT experts in scrutinising an organisation's data to find patterns or fraud profiles. Thus, from the findings from the literature, it could be concluded that FA has a relationship with providing more reliable evidence through standardised IT facilities. Furthermore, FA software is related to the speed of fraud detection.

■ Conclusion

With regard to IT and FA, this chapter involves a lot of researchers' views on FA concerning several factors, and all are directed towards minimising fraudulent practices. This chapter's findings stressed the need for sound knowledge of IT for effective FA investigation. Furthermore, the review's outcome buttresses criminals using the latest technologies to provide themselves with links with criminals worldwide without a concrete need for

physical contact. Thus, the more complex the context in which criminals operate, the more professional experience is required to reduce risks associated with these crimes. There is significant consensus in the literature that FA effectively controls fraud and improves financial reporting and internal control. Thus, from the findings from the literature, it could be concluded that FA has a relationship with the provision of more reliable evidence using standardised IT facilities. Furthermore, the use of FA software has a relationship with the speed of fraud detection. However, based on some other literature reviewed in this study, it was found that fraudulent practices and the provision of forensic services have implications for accounting education and practices. In addition, this chapter explained the different perspectives of FA with respect to fraud, which is the independent variable of this study. These findings revealed in this study may assist corporate organisations in effectively mitigating internal and external fraud schemes.

The effect of forensic accounting software on the accuracy of financial investigation

■ Introduction

The complex nature of fraud necessitates accurate investigation for its detection and mitigation. Hence, in this chapter we examine the effect of FA software on the accuracy of financial investigation using the Auditor-General's office of a state in Nigeria.

Using a case study approach, a structured questionnaire was used to obtain qualitative data. One hypothesis was developed to statistically validate the research questions raised. The inferential statistical analysis was conducted using the Statistical Package for Social Science (SPSS version unconfirmed, IBM) software package to test the formulated hypothesis. The chi-square and Fisher's exact tests were employed to validate the hypothesis statistically. At the same time, Cronbach's alpha was calculated to examine the reliability and internal consistency of the instrument used. A pie chart was also employed to visualise the percentage of responses obtained from the questionnaire.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'The effect of forensic accounting software on the accuracy of financial investigation', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 155-172. <https://doi.org/10.4102/aosis.2024.BK485.08>

The results indicate that the instrument employed is internally consistent and that there is no significant agreement between the use of FA software and the accuracy of the financial reporting investigation for the survey conducted.

This work provides insight into the correlation between FA software and the accuracy of financial reports in the quest to tackle economic crime. The novelty of this work lies in the fact that the investigation of the effect of FA software, namely the Forensic Tool Kit (FTK), EnCase, Tableau, ACL and IDEA, on the accuracy of financial investigation and reporting has not been sufficiently highlighted by the existing literature.

■ Forensic accounting software

The complex nature of fraud necessitates accurate investigation for its detection and mitigation. Akinbowale, Klingelhöfer and Zerihun (2021) reported that fraud is increasingly becoming complex to detect and investigate, with significant consequences on the organisation's reputation and profitability. Financial information and investigation accuracy are critical to identifying financial misrepresentation falsification and reducing economic crimes. Forensic Accounting is a scientific method aimed at financial investigation, uncovering, analysing and presenting fraud-related matters in an acceptable way to the court of law. It integrates accounting, auditing and investigative skills (Akabom-Ita 2012; Yadav & Yadav 2013). Forensic accounting depends on different pillars. These pillars include the accountant's character, expertise, tools employed and knowledge of law (Hamdan 2018). Forensic accountants are extensively knowledgeable individuals who possess comprehensive skills in numerous areas. These include general accounting principles, the law, criminal behaviour, fraud and computerised systems (Hitchcock 2018). Fraud and fraudulent cases in some countries have increased the demand for FA (Okoye & Alamobi 2009). An organisation's lack of well-developed accounting policies further weakens the corporate reporting system; hence, it is the auditor's duty to detect fraud and the transparency of financial reports provided by top management (Olaoye & Olanipekun 2018). Bhasin (2016b) posits that the need for FA is due to the increasing rate of financial fraud and the limitation of the auditing process to mitigate it. Thus, a well-structured system of accounting and investigation is necessary for minimising fraud. The tasks of accounting, investigation and provision of litigation support have been identified as a forensic accountant's core functions in handling fraud-related cases (Akinbowale, Klingelhöfer & Zerihun 2020). Forensic accounting employs a combination of qualitative and quantitative techniques to address underlying problems related to financial data manipulation. The methods employed in FA adapt and develop in response

to the specific requirements of the organisation. Forensic accounting employs a combination of qualitative and quantitative techniques to address underlying problems related to financial data manipulation. The methods employed in FA adapt and develop in response to the specific requirements of the organisation. The increase in the number of fraudulent activities is one of the significant reasons for FA (Özkul & Pamukçu 2012). Forensic accounting shares a closer connection with the legal field than other business disciplines. It is often perceived as the convergence of law and accounting, and the legal system significantly influences the practices of FA (Özcan 2019).

Okoye and Gbegi (2013) consent that FA can also be called investigative accounting or fraud audit. This combines forensic science and accounting. Forensic science deals with the application of laws of nature to human laws. Forensic scientists are examiners and interpreters of facts and evidence in legal cases requiring expert court opinions. Hao (2010) indicates that FA integrates the accounting framework and legal framework, while Chattopadhyay (2014) argues that forensic accountant titbits of evidence were inadequately framed as this leaves a gap in relation to the various accounting standards which the counsel may not be prepared to accommodate in the brief to be tendered in the court. Grubor, Ristić and Simeunović (2013) explain that FA differs from regular financial auditing processes. While the auditing process determines the accuracy and reliability of the financial statement from a sample of transactions and reports about the accuracy, deviation or falsification detected, the process of FA deals with the investigation of suspicious financial reports or transactions using dedicated digital forensic processes and techniques (Nigrini 2011). Forensic accounting comprises several phases such as identification, investigation, sorting, evidence extraction and recording, analysis, settling and reporting, and verification of digital financial data and other accounting activities to present substantial evidence against the culprits for a legal process (Carvey 2009; Kwok 2008). Bhasin (2013) indicates that the role of forensic accountants in corporate governance is critical in fraud investigation and prevention, while Özcan (2019) explains that FA, which has brought an up-to-date approach to the investigation of financial information inconsistencies, includes a wide variety of activities such as fraud investigation, litigation support and expert witness.

The exponential increase in global economic crimes has necessitated the deployment of FA software to aid the accuracy of financial investigation. The accuracy of financial information and investigation is critical in identifying financial misrepresentation and falsification and reducing economic crimes (Kubi, Saleem & Popov 2011). The integrity of the financial investigation process and reports, as well as its admissibility in a

court of law, anchors to the accuracy of the investigation and data analysis, which the software can enhance if rightly deployed. Forensic accounting software is the interface between the investigator and the data under investigation; hence, the accuracy of the financial investigation is primarily a function of the performance of the software employed (Albano et al. 2011). Seda, Bonita and Larry (2019) explain that computer and FA software aids in fraud investigation, detection, prevention, deterrence, data extraction and analysis. A reliable digital forensic technique, which integrates FA software, is necessary to investigate, detect and prevent electronic crime (Nissan 2012).

Using big data technology can also promote sustainability in the fight against economic fraud by identifying irregularities in financial information (Akinbowale et al. 2020). Many works have been reported on implementing FA principles in financial investigation and tackling economic crime. For instance, Ehioghiren and Atu (2016) investigate the relationship between FA and fraud management, drawing evidence from Nigeria. The study employs primary data from a structured questionnaire and the ordinary least square regression technique for analysis. The result indicated that FA can significantly aid the process of fraud detection and control. The study also establishes a significant correlation between professional forensic accountants' duties and conventional auditors' duties. Onyekwelu, Ugwu and Nnamani (2016) investigate the effectiveness of FA on the quality of financial reporting and use the Nigerian banking sector as a case study. The study employs both the primary and secondary data sourced directly from the accountants and from the annual reports of the selected, respectively. The correlation analysis shows that the significant qualitative features of financial reporting can be considerably improved by implementing FA to tackle economic crime sustainably. Akinbowale et al. (2020) developed an innovative method for fighting economic crime using FA techniques. The work featured the development of two simplified conceptual models, which integrate FA principles into an organisation structure and capture fraud investigation and data analysis processes in the lifecycle of fraud mitigation.

Akinbowale et al. (2021) also integrate FA and MCSs to combat cyberfraud. The work employed the linear programming (LP) approach validated via the genetic algorithm (GA) to validate the LP model. The results indicated the LP-GA model's feasibility to minimise the cost of the employed capacities for fraud mitigation. It also shows the developed approach's suitability to improve the organisation's reputation. Forensic accounting is still an evolving field, and many emerging economies are still developing capacities to implement it to curtail corporate fraud.

This chapter is motivated by the fact that FA software can aid the accuracy of financial investigation if adequately deployed; hence, this chapter aims to investigate the effect of FA on the accuracy of financial reports at the Auditor-General's office of a state in Nigeria. The findings of this work can create awareness about the relevance of FA software in financial investigations. They will aid managerial decision-making geared towards fraud mitigation. There is still a shortage of information regarding the principles of FA and the implementation of accounting software for financial investigation; hence, this study will add to the knowledge of the principles of FA and the FA software geared towards financial investigation. The novelty of this work lies in the fact that the investigation of the effect of FA software (i.e. FTK, EnCase, Tableau, ACL and IDEA) on the accuracy of financial investigation and reporting has not been sufficiently highlighted by the existing literature. The succeeding section presents the methodology employed for this study involving the FA software considered and the instruments used. In contrast, the following section presents the data analysis and discussion of the results obtained. The last section offers the conclusion and the recommendation from the study's findings.

■ Method

This study considered using five FA software packages: FTK, EnCase, Tableau, ACL and IDEA. The specific objectives are to determine the effect of FA software on financial investigation and reporting accuracy. This study seeks to answer the question: 'Does using forensic accounting software improve the accuracy of financial investigative evidence(s)?' This led to the development of one hypothesis to validate the research question statistically. Existing studies have reported on the significance of FA software to financial investigation and reporting (Albano et al. 2011; Bhasin 2016b). Some reports argue that each software tool has its peculiarities. It may be counterproductive if the software tool's capabilities are identified and appropriately deployed to solve the right problem (Cusack & Ahokov 2016; NIST 2013). Based on this premise, a null hypothesis was formulated to investigate the correlation between the effective usage of FA software and the accuracy of financial reporting investigation. The null hypothesis is expressed as follows:

H₀: 'There is no significant agreement on the effective usage of forensic accounting software and accurate financial reporting investigation.'

This study's sample size comprises 131 participants from the Auditor-General's office of a state in Nigeria. A random sampling approach was employed to select the participants as a matter of voluntary participation. The total target population was 196. Therefore, at a 95% confidence level

with a 5% margin for error, an ideal minimum of 130 sample size was obtained using Equation 8.1:

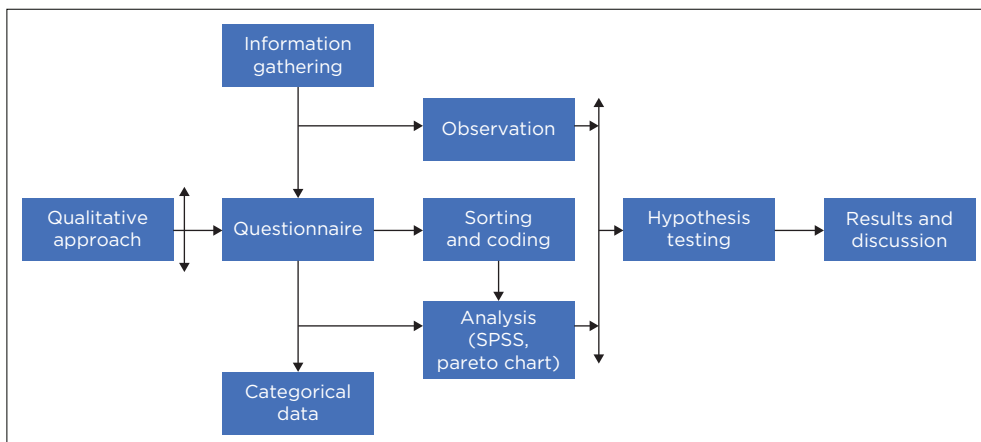
$$\text{Ideal sample size} = \frac{(Z - \text{score})^2 \times \sigma \times (1 - \sigma)}{e^2} \quad [\text{Eqn 8.1}]$$

where the Z score at 95% confidence level is 1.96, σ is the standard deviation and e is the margin of error (confidence interval) of $\pm 5\%$.

The questionnaire was employed as the survey instrument to collect data. It was administered to the Auditor-General's office of a state in Nigeria. The questionnaire comprises four parts. The first part seeks to probe deep into the relevance of IT as it assists forensic accountants in accurately presenting data and supporting evidence in courts. The second part of the questionnaire investigates how forensic accountants can use specialised computer software and hardware to collect, preserve, analyse and document evidence. In contrast, the third part seeks to know whether computerised information can enable forensic accountants to investigate disputes or fraud, whether an organisation's disputes, fraud, business economic losses or professional negligence, among others. The last part of the questionnaire examines how FA poses a challenge for regular accountants and accounting auditors in Nigeria due to inadequate expertise and knowledge in digital forensic investigation.

The questionnaire was used to collect data, and the inferential statistical analyses were carried out using the SPSS. The inferential analysis uses the chi-square and Fischer's exact tests to validate the hypothesis statistically. The tests are suitable for ordinally scaled data for investigating whether the null hypotheses should be accepted or rejected (Kim 2017; Rana & Songhai 2015). In order to examine the reliability of the scales summed up to measure the accuracy of financial reporting investigation with the aid of FA software, Cronbach's alpha was calculated. The pie chart was also employed for visualising the percentage of the responses obtained from the questionnaire administered. The framework used for the methodology is presented in Figure 8.1, while Figure 8.2 shows the framework for implementing FA software for fraud detection.

The process involves significant steps: data integrity check, data filtering, comprehensive data study, data-mining, fraud identification, detailed investigation, evidence gathering, reporting and establishment of litigation against the suspects. Following the acquisition of data from different sources linked to the fraud, the data can be subjected to an integrity check to ensure its credibility and to ascertain that quality information and evidence are captured. The collected data are then filtered to streamline

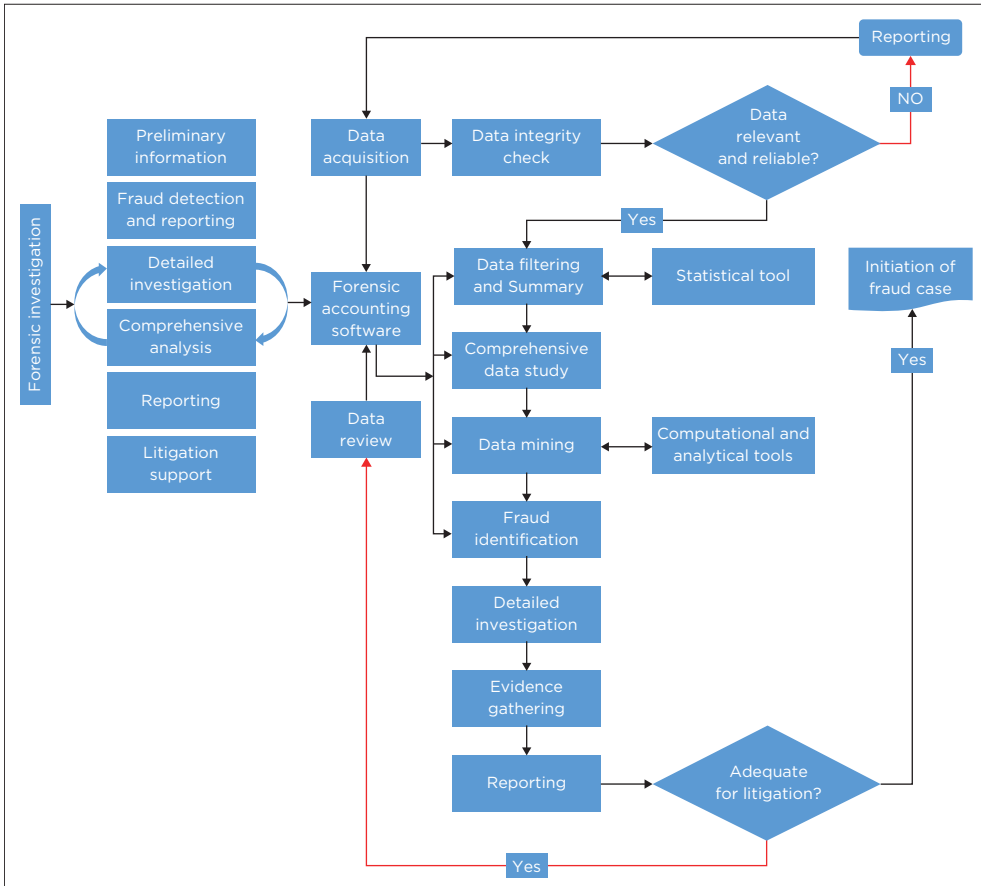


Source: Authors' own work.

FIGURE 8.1: Framework for the methodology employed.

and reorganised to sort out the relevant ones before storing them to prevent loss. This stage is usually followed by a comprehensive data study, transformation and evaluation to understand the data's peculiarities and extract useful information. It is possible to code the data obtained at this stage for security reasons and to enhance the data analysis process. During the evaluation phase, the data are analysed. The forensic expert searches for anomalies, patterns and trends using advanced algorithms inherent in the software used to uncover fraud. Statistical tools can also provide descriptive analytics of the data set in terms of its mean and standard deviation variation to estimate some deviations from the mean values. Several data-mining techniques can also be used at the data-mining stage for anomaly detection (detection of patterns or records outside the norm). The association rules of the data-mining technique can search and identify relationships, interdependencies and sequences within the data set. Clusters can be created for data with the same features, and classifications can be made by correlating new data sets obtained with the most appropriate sets. Regression analysis can also determine the degree of change when a variable within the data set changes. Data visualisation is usually helpful in overviewing the patterns identified, which is critical in uncovering fraud. The identification of fraud perpetration is generally followed by a detailed investigation to consolidate the evidence gathered and validate them, and then the investigation findings are reported for onward transmission to the litigation phase.

From Figure 8.2, the process of electronic information gathering is rapidly changing with the evolution of technology. The forensic accountant is expected to possess relevant IT skills to aid the information identification



Source: Adapted from Akinbowale et al. (2020).

FIGURE 8.2: Framework for the implementation of forensic accounting software for fraud detection.

and gathering process while ensuring the data's integrity (Miller & Martson 2011). Some of the identified information to be gathered include the details of transactions, communications, the model, make and type of computer system used, internal and external disk drive capacity, the operating system employed, applications used, network design and the literacy of the users. The information relating to those mentioned above can be obtained on electronic devices and accessories such as personal computers, network servers, smart cards, magnetic strips, caller identity (ID) devices, photocopiers, printers, storage media, wireless and cordless telephones, answering machines, scanners, ID card printers, global positioning systems, compact disc, security systems and digital cameras, among others (Miller & Martson 2011). Next is the handling and storage of

the captured data to ensure the integrity of the data and the investigative process. This can be achieved via proper documentation of the applications and procedures performed on the electronic devices, duplication and storage of the data and information acquired in a safe location, creation of an image copy of the evidence, as well as analysis of a copy of the original document rather than the original itself (Miller & Martson 2011). Forensic accounting software plays a significant role in ensuring the integrity of the contents of the documents and the identification of suspicious transactions. The software can also assist in data filtering, analysis, evaluation, duplication, matching, sorting, correlation, classification and mining. The software ranges from spreadsheet software such as Microsoft Excel for analysing small data sets to sophisticated ones with enhanced fuzzy matching capabilities, critical control and security features, access restriction and querying capabilities to link numerous data together and establish a relationship between them (Decker et al. 2011).

The use of relational database packages such as Microsoft Access, Microsoft SQL servers and ORACLE has also been reported to aid the storage, security, maintainability, scalability and reliability of large and complex data sets. In contrast, more specialised software for advanced statistical analysis, such as the Statistical Analysis System and SPSS, can aid the data analysis process (Decker et al. 2011).

Equation 8.2 presents the chi-square expression for the computation of chi-square statistics (Kim 2017):

$$\chi^2 = \frac{(O - E)^2}{E} \quad [\text{Eqn 8.2}]$$

where O is the observed value of the cells and E the expected value.

The p -value was employed for hypothesis testing. When $p < 0.05$, the null hypothesis is rejected. On the contrary, for $p > 0.05$, the null hypothesis is accepted.

For the expression of Fisher's exact test, Equation 8.3 holds thus (Amigo-Dobaño, Garza-Gil & Varela-Lafuente 2020):

$$p = \frac{((a + b)!(c + d)!(a + c)!(b + d)!)}{a!b!c!d!N!} \quad [\text{Eqn 8.3}]$$

where a , b , c and d represents the frequencies of the categorical variable of the 2×2 contingency table and n is the total frequency.

■ Results and discussion

There were 131 respondents, and the responses obtained for the following questions (Q1–Q4) are presented in Table 8.1–Table 8.4, respectively:

- **Q1:** Information technology makes it easy for forensic accountants to present information or data accurately in courts with supporting evidence.
- **Q2:** Forensic accountants can employ specialised computer software and hardware to preserve, collect, analyse and document evidence.
- **Q3:** Computerised information can enable forensic accountants to examine disputes or fraud cases such as corporate disputes, fraud, business economic losses and professional negligence.
- **Q4:** Implementing FA principles is challenging for regular accountants and accounting auditors in Nigeria due to the required expertise and knowledge about digital forensic investigation.

Table 8.1 presents the percentage analysis of respondents’ perception of the convenience of using IT-based FA by forensic accountants in showing data and supportive evidence in court: 5.3% (7) strongly disagreed with the statement, 3.1% (4) disagreed, 13.7% (18) were undecided, 39.7% (52) strongly agreed and 37.4% (49) agreed. Figure 8.3 is the pie chart that visualises the percentages of the responses obtained regarding Q1. A significant portion of the chart shows that the respondents concur that IT makes it easy for forensic accountants to present information or data in courts with supporting evidence accurately.

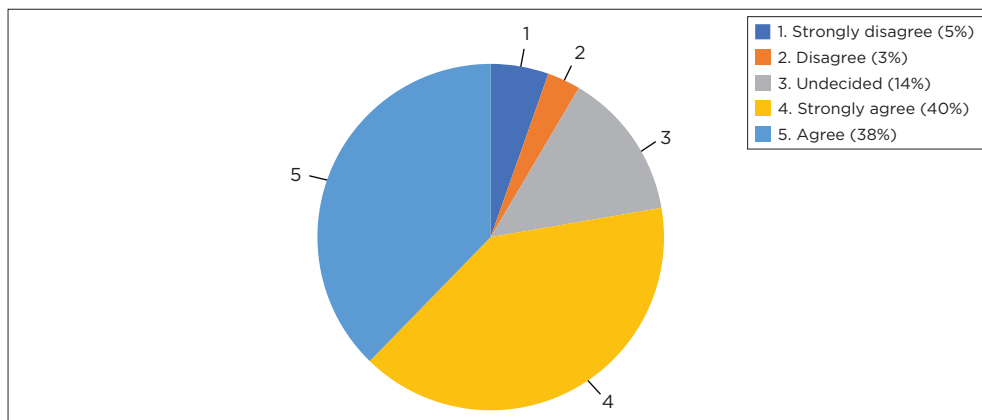
Hence, from the results obtained from the survey, it can be inferred that IT enables easy presentation of data and supporting evidence by forensic accountants.

Table 8.2 indicates the percentage analysis of respondents’ responses on using specialised computer software and hardware by forensic accountants to preserve, collect, analyse and document evidence: 5.3%

TABLE 8.1: Survey results for Q1 (information technology enables easy presentation of data and supporting evidence by forensic accountants).

Validity	Respondents’ opinions	Scale	Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	0	7.0	5.3	5.4	5.4
	Disagree	1	4.0	3.1	3.1	8.5
	Undecided	2	18.0	13.7	13.8	22.3
	Strongly agree	3	52.0	39.7	40.0	62.3
	Agree	4	49.0	37.4	37.7	100.0
	Total	-	130.0	99.2	100.0	-
Missing	System	-	1.0	0.8	-	-
Total		-	131.0	100.0	-	-

Source: Authors’ own work.



Source: Authors' own work.

FIGURE 8.3: Pie chart for the responses for Q1.

TABLE 8.2: Survey results for Q2 (forensic accountants can use specialised computer software and hardware by forensic accountants to preserve, collect, analyse and document evidence).

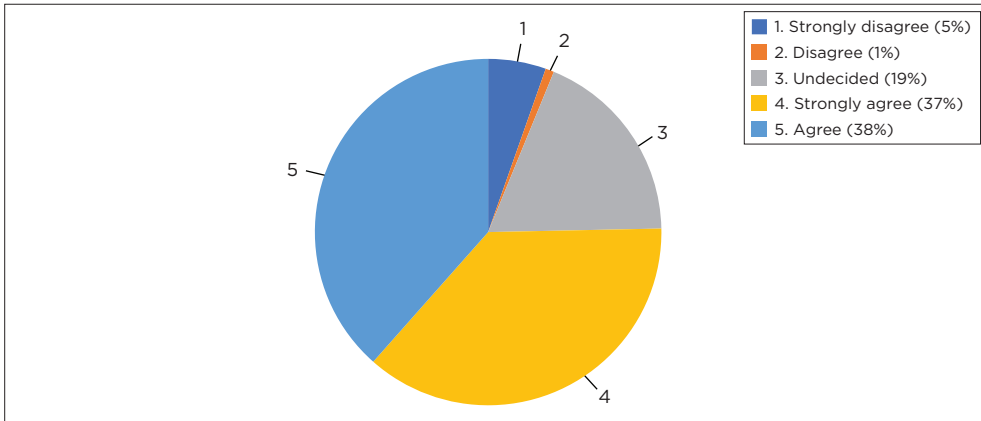
Validity	Respondents' opinions	Scale	Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	0	7.0	5.3	5.4	5.4
	Disagree	1	1.0	0.8	0.8	6.2
	Undecided	2	24.0	18.3	18.5	24.6
	Strongly agree	3	48.0	36.6	36.9	61.5
	Agree	4	50.0	38.2	38.5	100.0
	Total	-	130.0	99.2	100.0	-
Missing	System	-	1.0	0.8	-	-
Total		-	131.0	100.0	-	-

Source: Authors' own work.

(7) strongly disagreed with the statement, 0.8% (1) disagreed, 18.3% (24) were undecided, 36.6% (48) strongly agreed and 38.2% (50) agreed. Figure 8.4 is the pie chart that visualises the percentages of the responses obtained regarding Q2.

Figure 8.4 shows that most respondents concur that forensic accountants can use specialised computer software and hardware to preserve, collect, analyse and document evidence. Hence, from the results obtained from the survey, it can be inferred that forensic accountants often employ specialised forensic computer software and hardware to preserve, collect, analyse and document evidence.

Table 8.3 presents respondents' responses on the ability of computerised information to assist forensic accountants in examining disputes or fraud cases such as corporate disputes, fraud, business economic losses and



Source: Authors' own work.

FIGURE 8.4: Pie chart for the responses for Q2.

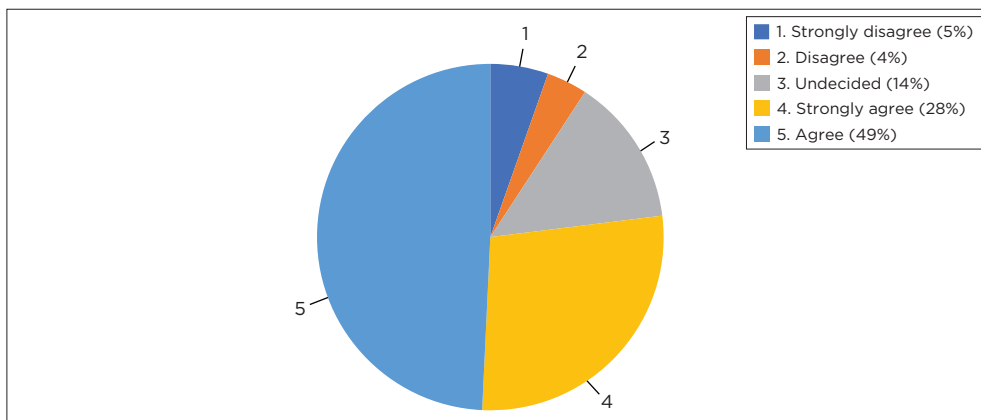
TABLE 8.3: Survey results for Q3 (computerised information enables forensic accountants to investigate disputes or fraud).

Validity	Respondents' opinions	Scale	Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	0	7.0	5.3	5.4	5.4
	Disagree	1	5.0	3.8	3.8	9.2
	Undecided	2	18.0	13.7	13.8	23.1
	Strongly agree	3	36.0	27.5	27.7	50.8
	Agree	4	64.0	48.9	49.2	100.0
	Total	-	130.0	99.2	100.0	-
Missing	System	-	1.0	0.8	-	-
Total		-	131.0	100.0	-	-

Source: Authors' own work.

professional negligence, among others: 5.3% (7) strongly disagreed with the statement, 3.8% (5) disagreed, 13.7% (18) were undecided, 27.5% (36) strongly agreed and 48.9% (64) agreed. Figure 8.5 is the pie chart employed to visualise the percentages of the responses obtained with respect to Q3. A significant portion of the chart shows that respondents concur that computerised information enables forensic accountants to examine disputes or fraud cases such as corporate disputes, fraud, business economic losses and professional negligence. Hence, based on the level of evidence obtained from the survey, it can be inferred that computerised information can assist forensic accountants in fraud investigation processes.

From Table 8.4, 4.6% (6) of the respondents strongly disagreed with the statement 'The implementation of FA principles is a challenge for regular accountants and accounting auditors in Nigeria due to the required



Source: Authors' own work.

FIGURE 8.5: Pie chart for the responses for Q3.

TABLE 8.4: Survey results for Q4 (the implementation of forensic accounting principles is a challenge for regular accountants and accounting auditors in Nigeria).

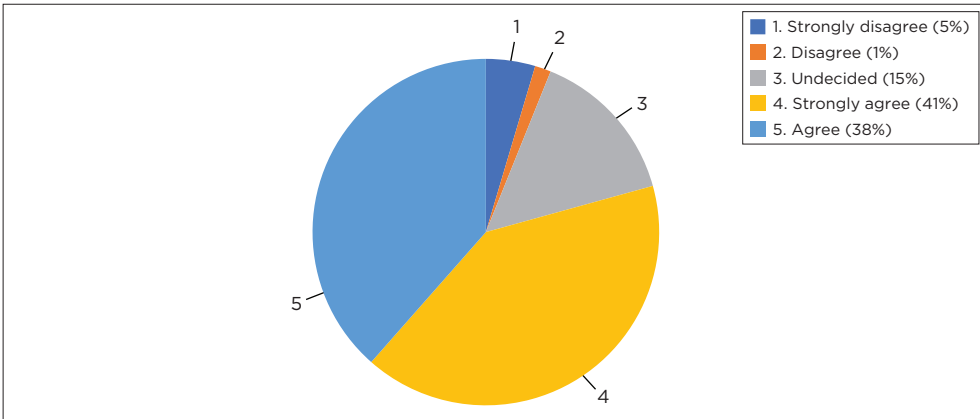
Validity	Respondents' opinions	Scale	Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	0	6.0	4.6	4.6	4.6
	Disagree	1	2.0	1.5	1.5	6.2
	Undecided	2	19.0	14.5	14.6	20.8
	Strongly agree	3	53.0	40.5	40.8	61.5
	Agree	4	50.0	38.2	38.5	100.0
	Total	-	130.0	99.2	100.0	-
Missing	System	-	1.0	0.8	-	-
	Total	-	131.0	100.0	-	-

Source: Authors' own work.

expertise and knowledge about digital forensic investigation': 1.5% (1) disagreed, 14.5% (19) were undecided, 40.5% (53) strongly agreed and 38.2% (50) agreed. Figure 8.6 is the pie chart employed to visualise the percentages of the responses obtained with respect to Q4. A significant portion of the chart shows that the respondents concur that implementing FA principles is a challenge for regular accountants and accounting auditors in Nigeria due to the required expertise and knowledge about digital forensic investigation.

Hence, based on the level of evidence obtained from the survey, it can be inferred that FA is still evolving in Nigeria. Due to a lack of the required expertise, many accountants and accounting auditors in Nigeria find implementing some of its principles challenging during fraud investigations.

Concerning Q1 and the responses from the survey, it can be inferred that IT makes the accurate presentation of data or facts obtained during



Source: Authors' own work.

FIGURE 8.6: Pie chart for the responses for Q4.

forensic investigations by forensic accountants easier. This may be because IT devices enable an unambiguous representation of facts and evidence. Darshan (2020) also supported the view that using computers (part of IT devices) can facilitate quick arrangement, preservation, analysis, documentation and presentation of digital facts and evidence during forensic investigation.

Concerning Q2 and the responses from the survey, it can also be inferred that forensic accountants use specialised computer software and hardware to preserve, collect, analyse and document evidence. This may be because specialised software and hardware can aid the information and data handling processes during forensic investigation. Proper data and information handling is necessary for any forensic investigation's success. This finding agrees significantly with the report of the US National Institute of Justice (2007). According to the US National Institute of Justice (2007), specialised computer software and hardware enable easy acquisition of information, storage and transfer of digital evidence. It also facilitates the duplication and imaging of evidence and enables the monitoring, surveillance and tracking of assets or transactions during investigation. The report, however, indicated that the computer software and hardware should not alter the evidence and that proper documentation of the activities involving the storage, examination and transfer of digital evidence must be properly carried out. Hence, training is usually required to develop human capacities to ensure proper computer software and hardware device handling.

Furthermore, concerning Q3 and the responses from the survey, it can be inferred that computerised information enables forensic accountants to examine disputes or fraud cases such as corporate disputes, fraud, business

economic losses and professional negligence, among others. Rowlingson (2004, p. 1) highlights the potential sources of digital evidence as computers, backup disks, hard drives, telephone recordings, closed-circuit television (CCTV), log files, emails, network traffic records and telephone records, among others. Hence, an organisation can leverage computerised information to enhance the effectiveness of a forensic investigation.

In addition, concerning Q4 and the responses obtained from the survey, it can be inferred that implementing FA principles is a challenge for regular accountants and accounting auditors in Nigeria. In line with this finding, Akhidime and Uagbale-Ekatak (2014), while investigating the increasing applicability of FA as a tool for tackling fraud in Nigeria, found that FA was a sustainable technique with a prospect for fraud mitigation but with certain limitations. The authors report that FA in Nigeria is still evolving and has insufficient implementation frameworks, statutory support and professional recognition.

For hypothesis Ho, 'There is no significant agreement on the effective usage of FA software and accurate financial reporting investigation', the outcome of this hypothesis testing focuses on the agreement between the effective usage of FA software and the accuracy of financial reporting investigations. The result of the analysis conducted to justify this hypothesis revealed that there is no significant agreement between the effective usage of FA software and the accuracy of financial reporting investigation, and this further implies the acceptance of the null hypothesis while rejecting the alternative.

To prove the reliability of the scales summed up to measure the accuracy of financial reporting investigation with the aid of FA software, Cronbach's alpha was calculated (Table 8.5). The alpha value computed was 0.749, implying that the construct under test is internally consistent and significant. The general rule of thumb is that a Cronbach's alpha score of 0.70 and above is good, 0.80 and above is better, while 0.90 is best (StatisticsSolution 2020). This implies that the instrument employed for the study is consistent. Hence, a Cronbach's alpha score of 0.749 obtained in this study indicates that the instrument used for the survey is internally consistent and reliable and that the combination of the questions can determine the effect of FA software on financial investigation.

Table 8.6 shows the outcome of data analysis using the chi-square and Fisher's exact test at a 0.05 significance level. The null hypothesis tested was therefore accepted, while the alternative was rejected. This is justified because the *p*-values (0.201; 0.332; 0.141; 0.120; 0.202; and 0.115) are more significant than the 0.05 significance level. This further implies that there is no significant agreement on the usage of FA software and accurate financial reporting investigation; FA may not significantly bring about proper

TABLE 8.5: Accuracy of financial reporting investigation.

Cronbach's alpha	Cronbach's alpha based on standardised items	Number of items
0.749	0.756	6.000

Source: Field Survey (2016).

TABLE 8.6: Results from chi-square and Fischer's exact tests.

Hypothetical statements	<i>n</i>	Chi-square statistics	Asymptotic significance (2-tailed)	Fischer's exact significance
IT makes it easy for forensic accountants to present information or data in courts accurately with supporting evidence	130.000	8.254	0.201	0.223
Forensic accountants can employ specialised computer software and hardware to preserve, collect, analyse and document evidence	130.000	2.334	0.332	0.386
Computerised information can enable forensic accountants to examine disputes or fraud cases such as corporate disputes, fraud, business economic losses and professional negligence, among others	130.000	8.456	0.141	0.137
The implementation of forensic accounting principles is a challenge for regular accountants and accounting auditors in Nigeria	130.000	4.678	0.122	0.120

Source: Survey data.

Key: IT, information technology.

supporting evidence but rather the source of the evidence. Lack of direct correlation between the use of FA software and the accuracy of the financial investigation may reduce the effectiveness of the fraud investigation, pattern recognition, and data analysis and jeopardise the fight against economic crimes. Also, this hypothesis supports the fact that FA is a great challenge for regular accountants and accounting auditors in Nigeria due to a lack of knowledge and experience in digital forensic investigation. This supports the findings revealed by Okwoli (2004) that the level of awareness on the use of FA techniques in Nigeria is low, especially in the Abakaliki urban area, which calls for the need to create awareness on the relevance of FA as an effective tool for fraud detection and investigations in the public sector.

The possible reasons for the low performance of FA software have been identified. Some of the reasons are the complex interface between the investigator and software, emerging technologies, low technical know-how or lack of the required skills or expertise to enhance the effective performance of the software, lack of standard procedures and practices, different and overlapping capability of the various software, among others (Ayers et al. 2007; Cusack & Ahokov 2016; Jansen & Ayers 2007; Nissan 2012; NIST 2013). Given the identified reasons, there is a need to promote

human capacity development through periodic training to acquire skills for effective software utilisation. This will also encourage accurate identification of data patterns, compliance and irregularities, which may occur during financial investigation and data analysis. Also, investigators need to keep up with the progress of FA software technologies (Jansen & Ayers 2007). Therefore, before the financial investigation process, there is a need to follow standard procedures and practices to avoid inconsistencies in the data analysis process. Ayers et al. (2007) also emphasise bridging the structures, protocols and designs in which the data resides. Notably, each FA software has its peculiarities and core features, distinguishing it from others and making it suitable for delivering a specific outcome (NIST 2013). Hence, selecting the right software for the proper application is necessary to enhance the accuracy of financial investigation. Mohtasebi and Dehghantanha (2013) suggest that investigators should be conversant with the scope of each software program before the selection for use, while Kubi et al. (2011) stress the need for investigators to know the reliability and accuracy of the software to be used to promote effectiveness and efficiency during use.

To mitigate fraud and avert financial losses, developing a real-time alert system capable of informing financial institutions or customers about fraud cases has been proposed (Akinbowale et al. 2020). Akinbowale et al. (2020) also developed two streamlined conceptual models for implementing FA. The first model integrates FA principles into an organisation's control structure, while the second details the investigation and comprehensive data analysis processes for fraud mitigation.

■ Conclusion

This chapter investigated the effect of FA software on the accuracy of financial investigation. This was achieved via a structured questionnaire and statistical analysis of the qualitative data collected in the SPSS environment. The null hypothesis tested, which states that there is no significant agreement on the effective usage of FA software and accurate financial reporting investigation, was accepted. At the same time, the alternative was rejected, as justified by the fact that the p -values (0.201, 0.332, 0.141, 0.120, 0.202 and 0.115) are greater than a 0.05 level of significance. In addition, the alpha value computed was 0.749, implying that the construct under test is internally consistent and significant. This work provides insight into the correlation between FA software and the accuracy of financial reports in the quest to tackle economic crime. The implementation of FA framework and principles, which encompasses the FA software, is therefore recommended for organisations to combat

economic crime. In addition, there is a need to enhance the performance of FA software through the development of human capacity and the establishment and strict adherence to standard products and practices. Future works can consider investigating the level of effectiveness of the different accounting software and their applicability.

The implementation of forensic accounting for fraud mitigation in financial institutions: A strength-weakness-opportunity-threat approach

■ Introduction

This chapter investigates the implementation of FA for fraud mitigation in financial institutions. Existing literature was reviewed to identify the progress of FA implementation concerning fraud mitigation in financial institutions. Considering the outcome of existing literature on applying FA techniques to mitigate fraud, this study employs the strength-weakness-opportunity-threat (SWOT) approach to identify the gaps and potential of FA implementation in the financial sector. This study is limited to implementing FA within the context of fraud mitigation in financial institutions. The findings from the review indicate that FA is a suitable technique for fraud mitigation in financial institutions. However, there is a need to introduce some regulatory and policy frameworks for its effective implementation. The SWOT analysis developed three conceptual frameworks for addressing some of the

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'The implementation of forensic accounting for fraud mitigation in financial institutions: A strength-weakness-opportunity-threat approach', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 173-192. <https://doi.org/10.4102/aosis.2024.BK485.09>

identified gaps and harnessing the potential of FA. Implementing these conceptual frameworks may assist financial organisations in making decisions and suggesting the implementation of FA (future direction). The novelty of this work lies in developing three unique conceptual models for addressing the threats and weaknesses of FA implementation.

■ The implementation of forensic accounting for fraud mitigation

Fraud is a purposeful act driven by deceit with the sole aim of misleading another party. It also involves illegally taking possession of another person's or company's property. Over the years, fraud has been reported as a menace threatening the existence of several banks and other profitable establishments globally. Forensic accounting has been seen as a technique capable of mitigating fraud when taken through proper procedures and investigative processes. The implementation of FA for fraud mitigation has recorded numerous successes, with some identified shortcomings during implementation. Hayles (2020) defines FA as combining accounting, auditing and investigative skills to investigate personal or corporate finances. Forensic accountants are responsible for recognising red flags and ending fraudulent activities before they become big enough to significantly impact large numbers of people (Hitchcock 2017). When FA investigation is conducted within the confines of the law, the outcome of the investigation may be suitable for litigation. Forensic accounting is broad and multidisciplinary; thus, it applies to many organisations, government agencies, financial and nonfinancial institutions and public institutions (Hegazy, Sangster & Kotb 2017; Tiwari & Debnath 2017). It has continued to gain widespread attention in resolving financial and nonfinancial crimes because of the increasing trends of crimes globally. Hassan and Morteza (2012) stated that forensic accountants can also perform essential roles relating to fraud or insurance claims, divorce and damage claims using financial inclinations. Some authors have classified some of the services provided by forensic accountants - for instance, litigation support such as expert witness, dispute advisory and resolution (Alshurafat, Al Shbail & Mansour 2021; Hegazy et al. 2017; Tiwari & Debnath 2017).

Another service is the investigation of fraud-related activities such as money laundering, theft, financial misstatement, cybercrime (Akinbowale, Klingelhöfer & Zerihun 2020, 2021; Louwers 2015), forensic analysis (Pearson & Singleton 2008), business valuation such as injury compensation, stock compensation risk analysis and bankruptcy advisory risk analysis (DiGabriele & Lohrey 2016), among others. Similarly, Shaheen et al. (2014) identify forensic accountants' roles in legal support, administrative support, expert witness, settlement of divorce cases or marital disputes, investigation of professional negligence, mediation and arbitration, criminal investigation

and fraud investigation, among others. However, the scope of this study is limited to implementing FA within the context of fraud mitigation in financial institutions. Hayles (2020) states that a FA expert is saddled with the responsibilities of evidence compilation, analysis, interpretation and summarising complex financial or business matters to uncover fraud. Furthermore, a forensic expert may also develop computer applications to manage (storage and analysis) the information obtained. The reliability of the outcome of a forensic investigation is partly a function of the nature of the computer application employed for the analysis. After that, the analysis outcome is usually communicated as an expert report, which can be used for litigation support. Financial crimes in financial and corporate organisations are now becoming a dangerous trend. Hence, FA can be a useful mitigating tool if its potential is sufficiently harnessed. PwC (2018) reports a growing concern for fraud risk emanating from various sources, such as internal, external, regulatory and reputational sources. On a regional landscape, Africa tops the list of the continent with the highest reported rate of economic crime, followed by Asia-Pacific and Eastern Europe, while the lowest rate was experienced in Western Europe (PwC 2020).

PwC (2020) identifies the prevalence of the various forms of economic crimes in 2020 globally (Figure 9.1).

■ Fraud types and some associated concepts

This section covers the synthesis of some selected literature on fraud and types of fraud, as well as the concept of FA.



Source: PwC (2020).

FIGURE 9.1: Prevalence of various forms of economic crimes in 2018.

■ Fraud and types of fraud

Fraud is a deliberate act to manipulate, deceive or mislead individuals, groups of people or corporate parties (Arens & Loebbecke 1997; Popoola, Ahmad & Samsudin 2015a, 2015b). There are various types or categories of fraud; thus, fraud can be characterised differently. However, the major types of fraud that are relevant to accountants and auditors are as follows:

- **Employee fraud or misappropriation of assets:** This type of fraud encompasses cash theft, inventory theft, skimming revenues, payroll fraud and embezzlement, among others. Asset misappropriation is the most common type of fraud. Examples of asset misappropriation are fraudulent disbursements such as billing and payroll schemes, expense reimbursement fraud, cheque alteration and cash register disbursement fraud. This fraud category may also include employees' aiding and abetting third parties (people outside the organisation) to defraud the organisation or other third parties (Thomas, Galar & Kumar 2006).
- **Financial statement fraud:** This type of fraud is described as deliberate misinformation, misstatements or omission in financial reports to purposely deceive the users of such financial information. Specifically, financial statement fraud comprises manipulation, falsification or alteration of accounting records or other supporting documents used to prepare financial statements. It is a deliberate misapplication of accounting principles to manipulate information or financial statements (Thomas et al. 2006).

■ The concepts of forensic accounting

The accounting field has constantly experienced certain drawbacks, such as the inconclusive nature of some auditing processes and the inability to look beyond the figures to identify underlying issues leading to fraud perpetration. Sometimes, the auditors may lack the capability to provide detailed background information about fraud-related cases. The core function of an auditor is to examine financial statements and give their opinion regarding the accurate and fair view of those financial statements. Hence, auditors might be unable to perform risk assessments and detect fraud in detail. To address these limitations, there is a need for a more detailed and critical investigation from experts with multidisciplinary knowledge. This quest led to the emergence of FA for fraud investigation, detection and litigation support. Abdullah et al. (2013) state that the emergence of FA is because of the growing rate of misrepresentation and falsification of accounting information. The field of FA was introduced to address the limitation of the conventional accounting system to promote fraud investigation and detection. In support of this view, Shimoli (2015)

indicates that FA is a tool that can be deployed for fraud detection, investigation and litigation support. This is because specific fraud schemes perpetrated in corporate organisations are complex to conceal the scam. Hence, a thorough investigation will be required to unveil such schemes and bring perpetrators to book.

Forensic accounting is versatile and can offer services relating to fraud or negligence investigation and risk assessment (Shimoli 2015). The investigative process consists of evidence gathering, interview, data analysis, conclusion, reporting and provision of litigation support. The FA process deals with the provision of accounting analysis of suspected fraud cases to obtain evidence admissible in court. This will form the basis of fraud resolution as the parties concerned may opt for litigation or out-of-court settlement (Effiong et al. 2017; Hecht & Redmond 2012; Stanbury & Parley-Menzies 2010). The core function of a forensic accountant as a subdivision of the accounting profession involves the identification of fraudulent activities both inside and outside an organisation. It has its own unique framework, investigative methodologies and procedures to produce a comprehensive report for legal support (Modugu & Anyaduba 2013). Houck et al. (2006) state that a forensic accountant applies accounting principles, know-how and skills to detect suspected fraud cases.

This study provides a SWOT analysis of FA for fraud mitigation in financial institutions. It discusses practical insights on formulating strategic decisions based on the three conceptual frameworks developed to address the perceived threats and limitations of FA and promote its performance for fraud mitigation. The novelty of this work lies in developing three unique conceptual models for addressing the threats and weaknesses of FA implementation.

■ Methodology

The methodology employed in this chapter involves a detailed review of some of the literature on applying FA techniques to mitigate fraud. This was followed by the SWOT approach to identify the strengths, gaps, trends, opportunities, threats and progress of FA implementation in the financial sector.

The SWOT analysis is a strategic planning and management approach that can assist individuals or organisations in identifying the core strengths, weaknesses, opportunities and threats of a business or technique (Gurel & Tat 2017).

In this chapter, the SWOT analysis assesses the strengths and weaknesses, opportunities and threats of FA implementation for fraud mitigation in the financial institution. The analysis unveils the potentials, resources,

limitations, capabilities, core competencies, and competitive advantages and disadvantages inherent in using FA for fraud mitigation. The analysis takes a holistic assessment of the opportunities and threats considering the business environment (financial institutions) and the general environment. The objective of the SWOT analysis is to obtain a fact-based analysis that leads to the evolution of ideas and strategic formulations to aid effective decisions regarding implementing FA for fraud mitigation. The strength (S) considers the features of FA, which gives its implementation for fraud mitigation in financial institutions an advantage over other fraud mitigation approaches. The weakness (W) is the features of FA, making its application for fraud mitigation disadvantageous. The opportunity (O) is the potential and capabilities of FA implementation for fraud mitigation, which financial institutions can leverage for their benefit. Threats (T) are the elements in the external environment that could hinder the effective implementation of FA for fraud mitigation in financial institutions.

Based on an extensive literature review, Table 9.1 presents the SWOT analysis of FA as a tool for fraud mitigation in financial institutions.

The detailed outcome of these strengths, gaps, trends, opportunities, threats and progress was employed to develop a framework that can assist in making decisions to harness the potentials of FA fully. The framework involves the combination of the components of the SWOT approach, which is presented in Table 9.2:

- **Strength-Opportunity (SO):** Leveraging the strength of FA to explore its opportunities.
- **Weakness-Opportunity (WO):** Minimising the weaknesses of FA to explore its opportunities.
- **Strength-Threat (ST):** Leveraging the strength of FA to minimise its threats.
- **Weakness-Threat (WT):** Minimising the weaknesses of FA to reduce the threats.

From Table 9.1, FA presents many strengths and opportunities that can be harnessed for combatting fraud. Figure 9.2 presents a framework which highlights these strengths and opportunities. Firstly, FA can serve as a deterrence approach to fraud perpetration through continuous monitoring of financial transactions and the use of advanced software and technology for fraud detection. Once the perpetrators, especially the internal perpetrators, know that the FA technique deployed by the organisation can track financial activities and detect fraud, it may discourage any attempt to perpetrate fraud. Incorporating FA techniques into the management control structure can identify and mitigate potential fraud cases before they escalate to fraud occurrence. Once fraud is committed, FA can be deployed for fraud investigation, including preliminary and

TABLE 9.1: The strength-weakness-opportunity-threat analysis of forensic accounting.

Strength		Weakness	
Author	Findings	Author	Findings
Crumbley et al. (2004); Kresse (2008)	Forensic accounting is multidisciplinary. It combines varied knowledge from different fields such as auditing, accounting, statistics, information communication, law, sociology, criminology, psychology, administration, management, etc.	Kresse (2008)	Variation in the forensic accounting curricula
Brickner et al. (2010); Tiwari and Debnath (2017)	Forensic accountants are exposed to a variety of knowledge, skills and abilities, for example, analytical, communication, investigative, IT and management skills	Alshurafat et al. (2021)	The consultation and implementation of forensic accounting may be expensive, especially for small- to medium-scale organisations
Lee et al. (2015)	It boasts creativity, innovation and high problem-solving capability	Rowlingson (2004); Albano et al. (2011)	Because of the detailed analysis and processes required, the various activities that characterise the implementation of forensic accounting could be tedious, multifaceted and time-consuming
Mehta and Bhavani (2017); Santos Filho et al. (2017); Akhidime (2017); Sule et al. (2019); Serhii et al. (2019, p. 7)	Fraud mitigation (investigation and detection) and information security	Akhidime and Uagbale (2014)	Slow rate of usage or emergence in some countries
Honigsberg (2020)	Enhance management decisions and promote effective management controls	Alshurafat et al. (2021)	Can affect the morale of innocent employees
Lalit and Virender (2012)	It can offer proactive and reactive fraud risk reduction roles	Chakrabarti (2014)	Poor publicity, awareness and sensitisation of potential of forensic accounting
Bhasin (2014)	It looks beyond the figures and deals with the business realities or situations at hand in the course of investigation to uncover fraud	Rowlingson (2004); Williams (2006)	Because of the detailed analysis and processes required, the various activities that characterise the implementation of forensic accounting could be tedious, multifaceted and time-consuming
		Oseni (2017)	Poor publicity, awareness and sensitisation of the potential of forensic accounting. Insufficient technical know-how. Shortage of skilled, expertise, professionals and educators
		Ocansey (2017) Al-Sharairi (2017) Alshurafat et al. (2020)	

Table 9.1 continues on the next page →

TABLE 9.1 (cont.): The strength-weakness-opportunity-threat analysis of forensic accounting.

Strength		Weakness	
Author	Findings	Author	Findings
Shaheen et al. (2014)	It can offer other supports such as litigation, administrative, expert and support	Cusack and Ahokov (2016); Hibshi, Vidas and Cranor (2011)	Complexity of the forensic accounting tool
Shimoli (2015)	Enhance management decisions and promote effective management controls		
Hegazy et al. (2017)			
Nonye and Okoli (2015)	Useful for business valuation	Ocansey (2017)	Variation in the implementation or operational guideline and reporting structure
Leedom et al. (2011); Markman et al. (2011)	Useful for determining the amount and possibility of financial loss	(Huber 2012)	Lacks altruism compared to public accounting
Leedom et al. (2011)	It is detailed in scrutiny and examination of the necessary information and documents		
Leedom et al. (2011)	Performance of cross-examination of suspects, investigation of other parties' report and determination of shortcomings to provide expert support		
Abdullah et al. (2013)	It can offer other supports such as litigation, administrative, expert and support		
Enofe et al. (2015)	<ul style="list-style-type: none"> • Enhance management decisions and promote effective management controls • It is more effective than the conventional accounting system 		
Lakshmi et al. (2016)	Can form strong synergy between other fraud anti-fraud agencies		

Table 9.1 continues on the next page →

TABLE 9.1 (cont.): The strength-weakness-opportunity-threat analysis of forensic accounting.

Opportunity		Threat	
Author	Findings	Author	Findings
Carpenter, Durtschi and Gaynor (2011)	Finds application in many organisations (financial and nonfinancial) because of the versatility and multidisciplinary nature	Dubey (2014); Teufel, Subramanian and Pedro (2011)	Strict and dynamic legal as well as low-level regulatory frameworks depending on the environment
Rezaee et al. (2016); Wang, Lee and Crumbley (2016); Kramer, Seda and Bobashev (2017); Alshurafat et al. (2020)	Increasing need and demand because of the increasing and complex nature of crime and fraud	Boyd et al. (2009); Huber (2014)	Certification and different professional requirements. For instance, the certified fraud examiner as a major certification requirement for forensic accountants
Huber (2014)	New career path	Krstic (2009); Huber (2014); Hegazy (2017); Tarr et al. (2016); Louwers (2015)	Lack of standard procedures or guidelines, ethical or disciplinary procedures
Lakshmi and Ganesh (2016)	Loss minimisation and increase in profitability when properly harnessed by corporate organisations	Hegazy (2017); Howieson (2018)	Lack of control over professional entry
Enofe, Utomwen and Danjuma (2015)	Can promote improvement in the customers' satisfaction level	Alshurafat et al. (2020)	Lack of government and public recognition as a professional discipline
Enofe et al. (2015)	Can promote improvement in the reputation and goodwill of corporate organisations	Chakrabarti (2014) Cusack and Ahokov (2016)	Dynamic nature of evolving technology and crime trend or nature
Golden and Murphy (2011)	Can aid organisation's management in making effective decision-making	Okoye and Akenbor (2009) Chakrabarti (2014)	Globalisation and intra- or inter-jurisdiction challenges. Lack of accountability for the juveniles in some countries.
Alshurafat et al. (2021)	Useful in adjudication and conciliation	Njanike, Dube and Mashayanye (2009); Olukowade and Balogun (2015); Ocansey (2017)	Lack of cooperation from anti-fraud agencies or concerned parties
Tawfeeq et al. (2014)	Improvement in the efficiency of corporate organisations	Chakrabarti (2014)	Gathering of admissible evidence in the court of law against 'big-shots' (politicians or bureaucrats)

Table 9.1 continues on the next page→

TABLE 9.1 (cont.): The strength-weakness-opportunity-threat analysis of forensic accounting.

Opportunity		Threat	
Author	Findings	Author	Findings
Sidharta and Fitriyah (2015); Ehioghiren (2016); Ocansey (2017)	It can facilitate the combat of financial and economic fraud or crimes	Chakrabarti (2014)	Financial defalcation
Khersiat (2017)	It can minimise professional negligence in financial institutions	Chakrabarti (2014)	Organisation's reputational risk
Dubey (2014)	It can aid the processes of fraud risk management	Chakrabarti (2014)	Fraud involving individual or corporate organisations from other countries
Nonye and Okoli (2015); Lakshmi and Ganesh (2016)	Determination of economic damage	Njanike et al. (2009); Ocansey (2017)	Inadequate material resources and training for forensic accounting personnel
Nonye and Okoli (2015)	Useful in the level of bankruptcy or insolvency for an organisation	Njanike et al. (2009)	Management override or interference
Nonye and Okoli (2015)	It can act as a guide in the re-organisation of financial activities	Alshurafat et al. (2021)	Admissibility of evidence. For instance, any infringement on the investigative laws may void the outcome of the investigation.
Nonye and Okoli (2015)	used to check on the integrity of the organisation's security fraud	Rowlingson (2004); Miller and Martson (2011); Ehioghiren (2016)	Sometimes, poor information gathering, handling and reporting could jeopardise investigative processes as well as the final outcome

Source: Literature synthesis.

Key: IT, information technology.

TABLE 9.2: Combination of the components of the strength-weakness-opportunity-threat approach.

Strength-Opportunity (SO)		Weakness-Opportunity (WO)	
Author	Findings	Author	Findings
Kwok (2008)	Fraud identification, investigation, analysis, scene or evidence recording, extraction and sorting of evidence, reporting and verification of financial information and other accounting activities to present strong evidence against the culprits for the legal processes	McIntyre et al. (2014)	Development of human capacity through periodic training and education for the effective delivery of forensic accounting services can improve the technical knowledge, skills and expertise of forensic accountants
Rowlingson (2004, p. 9)	Definition of the business situations which require forensic investigation	Okoye and Akenbor (2009)	Introduction of courses and training programmes relating to forensic accounting in the professional and academic curricula of higher institutions
	Determination of the requirements for the collection of evidence	Ocansey (2017)	
Rowlingson (2004, p. 9)	Establishment of the capability for gathering digital evidence legally, such that it will be admissible as evidence during the litigation process	Seda et al. (2019)	Synergy between academia and organisations that provide forensic services
(Hamdan 2018, p. 1)	Investigation using the right tool. Specification of the circumstances in which the digital evidence may be launched for full investigation.	Huber (2012)	Although it may not be publicly recognised as a profession at present, the field is rapidly growing and perceived to fully evolve and mature with time
Hamdan (2018)	Harness the expertise, experience and legal understanding of forensic accounting	Seda et al. (2019)	Periodic training will also cater for the understanding and effective usage of complex forensic accounting tools. This may also make the process of implementation time-effective as forensic accountants will gain familiarity with the process and tools over time.
Olaoye and Olanipekun (2018)	The presence of well-established forensic accounting frameworks or policies in an organisation to reinforce the management controls system	Akinbowale et al. (2020)	The initial cost will be offset over time through loss minimisation once it is properly integrated as a subset of the management control system
Singleton and Singleton (2010)	Expert witness in the court and provision of comprehensive information regarding financial fraud cases	Akinbowale et al. (2020)	Investigation should be carried out without the violation of human rights
Eliezer and Emmanuel (2015)			
Efosa and Kingsley (2016)			

Table 9.2 continues on the next page →

TABLE 9.2 (cont.): Combination of the components of the strength-weakness-opportunity-threat approach.

Strength-Opportunity (SO)		Weakness-Opportunity (WO)	
Author	Findings	Author	Findings
Strength-Threat (ST)		Weakness-Threat (WT)	
Author	Findings	Author	Findings
Seda et al. (2019)	Beyond consultation services, the incorporation of forensic accounting as a fraud control structure in corporate organisations will minimise organisation's reputation risk and management override	McIntyre et al. (2014)	There is a need for forensic accountants to be aware of the various laws (constitution, common and customary laws, etc.) applicable to the field
Okoye and Akenbor (2009)	In terms of admissibility of evidence, knowledge of the investigative laws and legal requirements can guide against infringements. Furthermore, the presentation of relevant accounting information gathered to an attorney for examination before it is used will increase the chances of admissibility.	Okoye and Akenbor (2009)	International cooperation is necessary for prosecuting criminals across different countries
Okoye and Akenbor (2009)	The cost incurred for the deployment of resources for forensic accounting implementation may promote organisation's profitability, and reduction in fraud, operational and reputational risk	US Department of Justice (2007)	Need for the establishment of regulatory authorities with a clear regulatory framework that will cater for operational standard procedures, guidelines, qualification and certification, ethical, professional entry requirements and disciplinary procedures
Okoye and Akenbor (2009)		Okoye and Akenbor (2009)	
Ocansey (2017)	The publicity of the milestones of forensic accounting can be published to increase the awareness and public interest to facilitate the growth of forensic accounting for fraud mitigation by the stakeholders	Seda et al. (2019)	Need for the recognition of forensic accounting as an independent field
Ocansey (2017)	Existing synergy between anti-fraud agencies and government institutions can be explored to secure the needed backing for the effective operation of forensic accounting by the government at all levels	Rowlingson (2009)	Establishment of a procedure for safe handling and storage of potential or captured evidence
Rowlingson (2004)	Staff training on incidence awareness and sensitivities of evidence from the legal perspectives	Akinbowale et al. (2020)	Clear identification of forensic accounting roles with minimal management interference or overrides
Rowlingson (2004)	Provision of legal framework to facilitate effective prosecution of the culprits	Okoye and Akenbor (2009)	Review of existing laws to accommodate accountability of juveniles. Enactment of specific laws for fraudsters will aid the process of prosecution.

Source: Authors' own work



FIGURE 9.2: Potential of forensic accounting implementation for fraud mitigation based on the three major threats or weaknesses affecting the implementation of forensic accounting.

detailed investigation to uncover such fraud. When properly deployed, the outcome of such investigation may provide insight into the method employed by the fraud perpetrators, the nature of fraud and the extent of the loss incurred. Forensic accounting can also facilitate the remediation and reconciliation processes after the investigation to ensure the recovery of losses and out-of-court settlement. Where the remediation and reconciliation processes fail, an alternative is to initiate a lawsuit by acting as a litigation support expert witness and providing a detailed conclusion of the investigation to prosecute the culprit. Based on the nature of fraud perpetrated and the potential for other forms of fraud, a forensic accountant can liaise with the organisation's management to develop fraud mitigation approaches for fraud control and risk management. This ensures robust

internal control and risk management strategies to curtail fraud. The implementation of FA will require the review of legal, policy, regulatory and procedural frameworks as well as the standards and ethical requirements to promote the credibility of the outcome of the investigation and admissibility of evidence for the prosecution of the culprits.

Figure 9.3 and Figure 9.4 present a framework for addressing the lack of accounting capacity development, curriculum review, and the gathering



FIGURE 9.3: Framework for addressing capacity development and curriculum review for effective forensic accounting implementation.

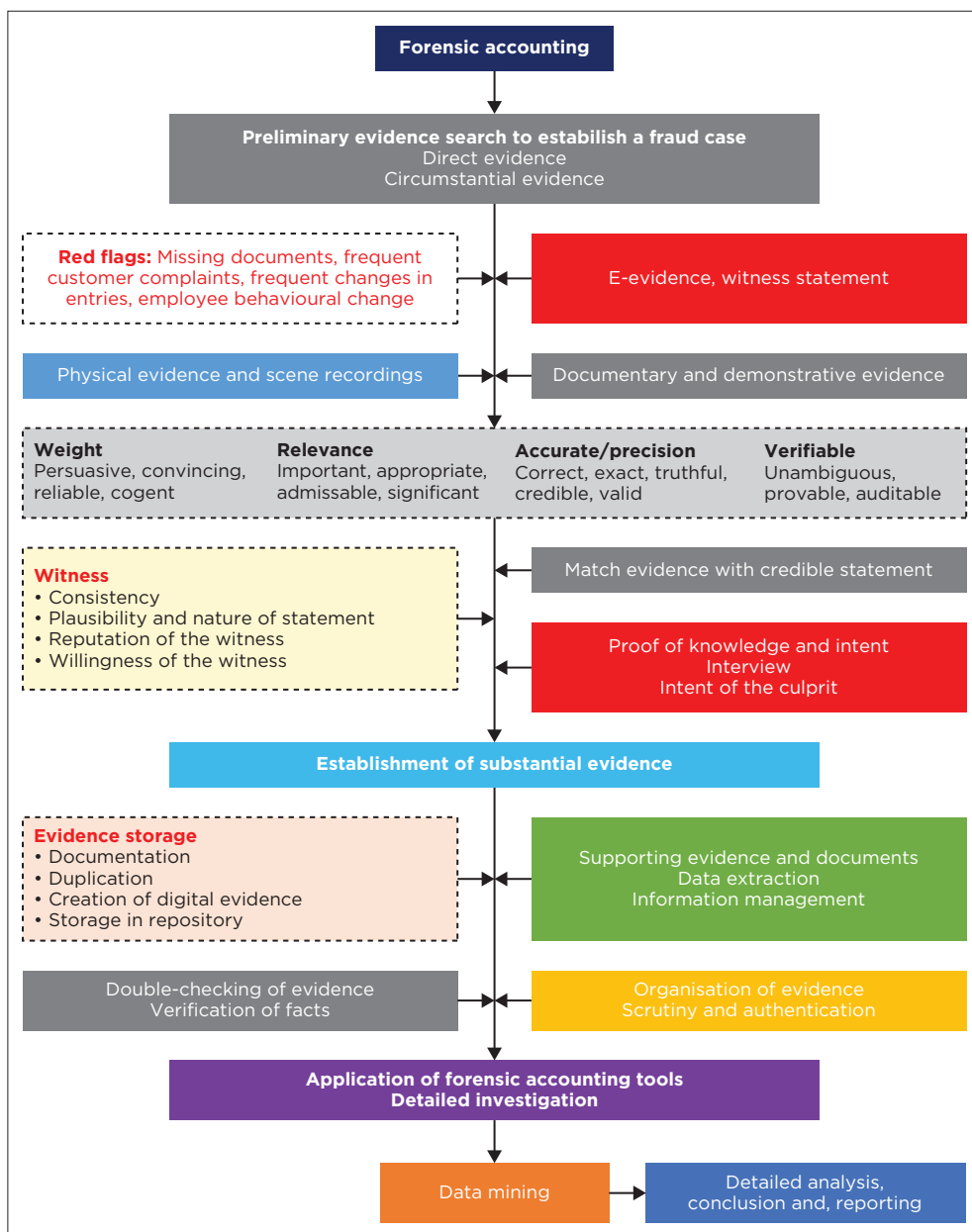


FIGURE 9.4: Framework for evidence management.

and handling of admissible evidence (Table 9.1). To address curriculum review, there is a need to harmonise the curricula of professional and academic institutions to focus on some key aspects such as forensic investigation (fraud investigation techniques, valuation of losses and damages, arbitration and mediation, advisory services, litigation and expert

witness, reporting), fraud management (fraud prevention, detection, investigation, risk analysis, remediation, deterrence), criminology (nature and scope of fraud, dynamics and trends of fraud, legal environment and ethical considerations) and introductory courses (auditing, accounting, statistics, Information Communication Technology, law, sociology, psychology, administration and management) as depicted in Figure 9.3. The curriculum on forensic investigation will also detail fraud identification – preliminary and detailed investigation, evidence gathering, detailed data analysis, reporting structure and litigation (Carpenter et al. 2011). Fraud management can also describe the two major categories of fraud, namely asset misappropriation (cash theft, credit fraud, inventory theft, payroll fraud, fraudulent reimbursement, cheque misrepresentation and fund embezzlement) and financial statement fraud (account misappropriation, intentional omission, forgery and alteration). To address the shortage of skills and technical expertise of forensic accountants, there is a need for FA to be skilled in specific fields relating to accounting, auditing, communication, administration, computer forensics, investigation, transaction analysis, analytics, interview and legal. Furthermore, periodic training will be necessary so that forensic accountants can be more versatile in using FA techniques. There is also the need for FA to periodically upgrade the knowledge of regulatory requirements, law, technology, legal services, corporate organisations, fraud and corporate finances. In addition, for continuous development, short learning programmes in critical areas such as skills review, fraud examination, fraud risk management, financial crime investigation, FA laws, statutory laws, electronic crime schemes and investigation will be helpful (Figure 9.3).

Figure 9.4 presents the framework for addressing the evidence gathering and handling challenge. Forensic accountants may fail in their operations unless evidence is gathered and handled within the confines of the law and ethical requirements. Evidence not handled correctly may jeopardise the outcome of the investigation and lawsuit. Hence, deploying the right FA tool can aid the safe movement of evidence to a secure repository. It can also ensure evidence storage and analysis for a credible investigative process.

Rowlingson (2004) described ten key activities for handling evidence-related issues while implementing a FA technique. These are:

1. defining the business situations which require evidence
2. identifying the sources and various types of prospective evidence
3. determining the requirements for the collection of evidence
4. establishing the capability for gathering evidence legally such that they will be admissible as evidence during the litigation process
5. establishing a procedure for the safe handling and storage of potential or captured evidence

6. effective monitoring to ensure the detection and deterrence of significant incidents
7. specifying circumstances in which the digital evidence may be launched for full investigation
8. training staff on incidence awareness and sensitivities of evidence from the legal perspectives
9. documenting an evidence-based case which describes the occurrence and its impact
10. ensuring that financial information and investigation accuracy are paramount in identifying financial misrepresentation falsification and reducing economic crimes.

From Figure 9.4, once a forensic accountant is deployed to handle a suspected fraud case, the first step is to conduct a preliminary evidence search to establish or dismiss the case. The red flags that can lead to a suspected fraud case include missing documents, perceived omissions, frequent customer complaints, frequent adjustments or changes in entries and changes in the employees' behavioural patterns. Other potential red flags may include a high volume of reimbursement, unusually high volume of credit and debit entries, improper recording of transactions in line with the standard procedure, unusual transactions (time, volume, nature or complexity), unrecorded differences between subsidiary records and control accounts, unauthorised access of employees to organisation's system and record, as well as poor documentation of transactions in terms of period, amount, classification (Tapp & Henderson 2011). Clayton (2011) identifies some common indicators that can be used to discover asset misappropriation, such as identification of duplicate payments, nonserial invoice numbers, transactions to the same recipient, arrangement of payment in either ascending or descending order of values, analysis of payment frequency to merchants, summarising payments by the payee to detect the account credited, detection of common payment methods, amounts or duplicate amounts, searching for cancelled cheques, voids or gaps, identification of serial vendor invoice numbers, identification of vendors with the same name, but different information or identification of vendors with the same information but different names, identification of all new suppliers, nonstandard journal entries, as well as controversial accounts, classification of employees by overtime pay or customer accounts by balance size. Evidence can be direct or circumstantial. Direct evidence supports or refutes the suspected fraud case directly. From such evidence, the occurrence or nonoccurrence of fraud may be substantiated. Conversely, circumstantial evidence often relies on the deduction of inferences to connect to the assertion. Hence, direct evidence is stronger, more reliable and has more weight than circumstantial evidence. However, circumstantial evidence can corroborate direct evidence and vice versa (IACRC 2022). For circumstantial evidence to be admissible, it should be based on the

principle of evidence for investigation and litigation support. This includes weight, relevance, accuracy and verification of facts. Circumstantial evidence should not be limited to pieces of information but form cumulative information well connected to the assertion. Evidence should be properly organised, documented, clearly presented and thoroughly investigated. Weak and disorganised evidence may yield poor investigative and litigation outcomes. Evidence could be in the following forms: electronic or digital evidence, witness statement, physical evidence, scene recordings, documentary or demonstrative evidence, depending on the nature of the case under investigation. The weight of evidence is a function of how persuasive, convincing, cogent and reliable the evidence is. This includes the source of the evidence, the type of evidence (direct or circumstantial), and the credibility of the witness or evidence provider. The relevance of evidence is based on its admissibility and appropriateness in proving or disproving a suspected case. Accuracy is a function of its correctness, exactness and validity. Evidence should also be verifiable; in other words, it should be unambiguous, traceable and provable. The witness statement is the testimony of the parties concerned with the assertion or related facts based on personal or direct knowledge about the case under investigation. It is nonspeculative and usually not based on personal opinion. The credibility of a witness depends on the coherence of the witness statement prior and subsequent statements, the plausibility of the statement *vis-à-vis* the assertion, the reputation and integrity of the witness, the nature of the statement obtained from the witness, and the willingness to be quoted, identified, testify or attest during the investigation (IACRC 2022). After gathering the evidence, it should be matched with a credible statement concerning the assertion. To substantiate the evidence gathered, there is also a need to obtain the knowledge of intent where possible. The knowledge of intent states the mind or intention of the suspect for committing the fraud and can be proven by direct or circumstantial evidence or a combination of both. For a suspected fraud case, a knowledge of intent may include alteration, forgery, an attempt to destroy or conceal potential evidence, deception of investigators or obstruction of the investigation (IACRC 2022). After substantiating the evidence gathered and authenticated, it can be preserved through documentation, duplication, creation of digital evidence, organisation and storage. Information management entails the management of the evidence acquired through effective control so that it can be used to prove the suspected fraud case. For effective management of evidence and other related information, it is necessary to ensure that the collection does not jeopardise the nature of the evidence collected and is stored in such a way that the evidence is preserved and that the evidence presented is the same as the one collected. These can be achieved via proper filing, labelling, indexing, description, duplication, digitalisation and chronological organisation. Care must be

taken to ensure that electronic data and evidence are not altered. The analysis process may commence at this stage by extracting data from the evidence acquired. Forensic accounting software such as FTK, EnCase, Tableau, ACL, IDEA and other data-mining techniques can be deployed to investigate the accuracy of the data extracted and to identify certain trends that can lead to fraud detection.

Cusack and Ahokov (2016, p. 17) explain that there must be substantial evidence to establish the occurrence of a fraud case before proper investigation can commence. Hence, at the evidence gathering phase, all the indicators that may signal the possibility of fraud are searched for (Kovalerchuk, Vityaev & Holtfreter 2007). Relevant evidence should be identified and gathered, including other supporting documents. Fraud detection is challenging because fraud is often characterised by concealment and collusion (Kenyon & Tilton 2011). Hence, the relevant evidence and supporting documents may be deliberately destroyed, altered, omitted, falsified or misplaced to conceal it. However, proper FA techniques can promote the chances of detecting fraud promptly once the evidence is properly gathered, kept and analysed (Kenyon & Tilton 2011).

■ Conclusion

This chapter aimed to identify the gaps and potentials of FA implementation in the financial sector. This was achieved using the SWOT analysis, identifying the strengths, weaknesses, opportunities and threats of forensic implementation for fraud mitigation in the financial institution. The findings from the review indicate that FA is a suitable technique for fraud mitigation in financial institutions. However, there is a need to introduce some regulatory and policy frameworks for its effective implementation. This led to the development of three conceptual frameworks to address some of the identified weaknesses and threats. The first framework highlights the potential of FA implementation for fraud mitigation, while the second addresses human capacity development and curriculum review for effective FA implementation – the third features evidence gathering and management processes to aid the investigative process. Implementing these conceptual frameworks may assist financial organisations in making decisions and suggesting the implementation of FA (future direction). Future works can consider the development of frameworks for addressing other threats and weaknesses of FA that have been identified.

Because of the increasing technological advancement and the complexity of fraud in financial organisations, there will always be potential red flags that must be investigated before they escalate to fraud perpetration. Given this, forensic accountants can be employed for consistent review of an organisation's management control in line with

financial operations. This will strengthen the internal control measures for early detection of potential fraud cases and effective risk management. As part of the organisation's policy, there should be a clear policy on the employees who must be involved in evidence gathering with the forensic accountant whenever there is a suspicion of fraud. Furthermore, a robust organisation's policy on ethics and disclosure of conflicts of interest can prevent impropriety so that the reliability of evidence and the confidence of investigators will not be undermined. This will further enable the forensic investigators to perform their duties objectively. In addition, the organisation's security policy regarding access to sensitive information can threaten evidence gathering. Although such security policies may not eventually hinder a FA accountant from accessing critical information, a periodic review might be necessary, particularly when considering time is a significant factor.

The roles of digital forensics in fraud investigation: A systematic literature review

■ Introduction

The admissibility of evidence in a fraud case partly depends on the reliability of the evidence. Fraud investigators sometimes face the challenges of retrieving information concealed in digital devices. Thus, this chapter aims to identify the role of digital forensics (DF) in fraud investigation. The study employs a systematic literature review in which 40 articles were reviewed. There is a consensus among the authors in the articles reviewed that DF is necessary to successfully investigate and prosecute fraud-related cases in this digital era. Thus, the study presents different DF frameworks that an organisation can adopt and adjust to suit the uniqueness of their organisation. This chapter adds to understanding DF and provides a blueprint for implementing DF during a fraud investigation. Integrating DF into the FA framework can aid the investigation process through incidence capturing and evidence preservation.

■ The roles of digital forensics in fraud investigation

A forensic accountant may investigate suspected cyberfraud incidences involving electronic systems devices through DF investigation (Mushtaque,

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'The roles of digital forensics in fraud investigation: A systematic literature review', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 193-216. <https://doi.org/10.4102/aosis.2024.BK485.10>

Ahsan & Umer 2015, p. 233). Digital forensics is a branch of forensic science comprising the recovery and investigation of materials (evidence) found in electronic systems or devices related to digital crime. Brown (2015, p. 72) indicated that DF is the process by which an investigator can discover, acquire, and investigate information in an electronic system or device capable of processing or storing information digitally. Dezfouli et al. (2012, p. 186) link their definition of DF to litigation as DF involves integrating computer science and legal fields geared towards fraud investigation.

Through DF investigation, the materials found in systems and devices can be extracted, documented and analysed as evidence that the court can use to prosecute (Prayudi, Ashari & Priyambodo 2015). Williams (2023) defines DF as the science of searching for evidence in digital media such as computers, mobile phones, servers, or networks. Electronic systems and devices usually have good storage capabilities and features that can hide information. Hence, a forensic accountant can inspect, identify, analyse and preserve digital evidence on various electronic devices with DFs.

Thus, through DFs, an enquiry can be launched into suspected fraud cases that occurred through the Internet, electronic devices or via an intrusion into the organisation's computer system (Brown 2015, p. 72). The extraction of the information stored in the files during an investigation requires effective management to ensure the adequacy and credibility of the outcome of the investigation. This means that the right software must be used to acquire and analyse information stored in digital devices to obtain credible information.

For any evidence to be credible, five major rules must be observed (Guan 2013):

- **Admissible:** It must be able to be used in court or elsewhere.
- **Authentic:** Evidence must be relevant to the incident under investigation.
- **Sufficient and complete:** The evidence presented must be adequate and presented wholly, not partially or fragmented.
- **Valid and reliable:** The evidence must be exact, genuine and accurate.
- **Clear:** Easy to understand.

The credibility of evidence for litigation purposes depends on strict adherence to the set of guidelines and rule of law during the data acquisition and investigation processes (Ayers et al. 2007, p. 6). Hence, FA software programs are often used to ensure that the data analysis process is completed with a higher confidence level in line with the specified standards (Albano et al. 2011, p. 381). Using the proper DF techniques is central to fraud detection, prevention, investigation and reporting (Nissan 2012, p. 843). Investigators must ensure the selection of appropriate forensic software tool that matches the proposed application. Each software tool has unique characteristics to deliver specific outcomes (NIST 2013, p. 4).

According to Adhyansh (2021) and Williams (2023), the following are the objectives of DF:

- To assist in recovering, sorting, analysing and preserving computers, potential evidence and other related materials for cross-examination and litigation.
- To assist in the postulation of the possible motive behind the crime and to identify the culprits.
- To assist in the acquisition of uncorrupted and untampered digital evidence.
- To acquire and duplicate data.
- To recover deleted files and partitions from digital media and to extract the evidence from them.
- To assist in quickly identifying the evidence and estimating the potential impact of fraudulent activity where possible.
- To enable easy access to stored information or evidence during investigation or litigation.

Digital Forensic investigation can either be proactive or reactive (Grobler & Louwrens 2009, p. 1). Proactive digital forensics (ProDF) is described as the process of restructuring procedures, description and technologies for the creation, collection, preservation, and management of comprehensive digital evidence (CDE) (Grobler & Louwrens 2009, p. 4). The ProDF may serve two purposes. The first is preventing fraud through systems that capture activities or information in real time. For instance, in organisations where security cameras are installed, it may discourage potential perpetrators from committing fraud. The second purpose is to ensure a successful, timely and cost-effective investigation with marginal disruption in the business processes (Grobler & Louwrens 2009, p. 4). On the contrary, reactive digital forensics (ReDF) is defined as an investigation that occurs after the detection of fraud or other related incidences (Grobler & Louwrens 2009, p. 7). The goal of the ReDF is to establish the root cause of the fraud-related incidences, identify the perpetrators and link them to the incident. It might also minimise the impact of fraud and provide a means for a successful investigation (Grobler & Louwrens 2009, p. 7).

Rowlingson (2004, p. 1) highlighted the potential sources of digital evidence as computers, backup disks, hard drives, telephone recordings, CCTV footage, log files, emails, network traffic records and telephone records, among others.

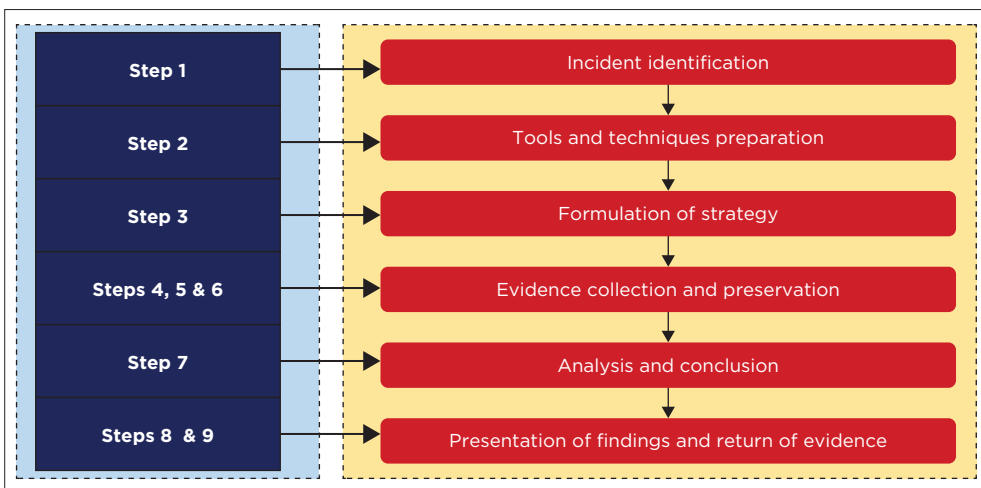
■ Systematic literature review on digital forensics

Reith, Carr and Gunsch (2002, p. 10) proposed using a DF model comprising a merger of standard techniques recognising the typical forensic analysis

implementation stages. The proposal combines the conventional forensic approach into a digital framework for fraud mitigation. The operation of the framework was captured in nine procedural steps. The first step is identifying an incident. The second step is preparing tools, techniques and authorisation to investigate the suspected fraud incident. The third step involves formulating a strategy to maximise the collection of untampered evidence with minimum impact on the victim. The fourth step is the isolation and preservation of digital evidence, excluding people or devices from accessing the digital evidence.

The fifth step involves the footage of the physical crime scene and the duplication of evidence using standard and acceptable techniques. The sixth step is a detailed and systematic search of evidence and the documentation of the evidence gathered for analysis. The seventh step is the analysis stage, which features the thorough investigation and scrutiny of the evidence gathered to conclude. The eighth step is the presentation of the outcome of the study. At the same time, the last step (ninth step) involves returning the physical and digital evidence to the owner. The nine procedural steps of the DF model proposed by Reith et al. (2002) are presented in Figure 10.1.

Adams, Hobbs and Mann (2013) suggested deploying the advanced data acquisition model for digital FA operation. This concerns the data management and digital nature of the social space, often employed for committing fraud. The model operates through three major stages. The first stage is the initial planning stage, where high-level consideration is given to the documentation relating to the investigation.



Source: Adapted from Reith et al. (2002, pp. 6-7).

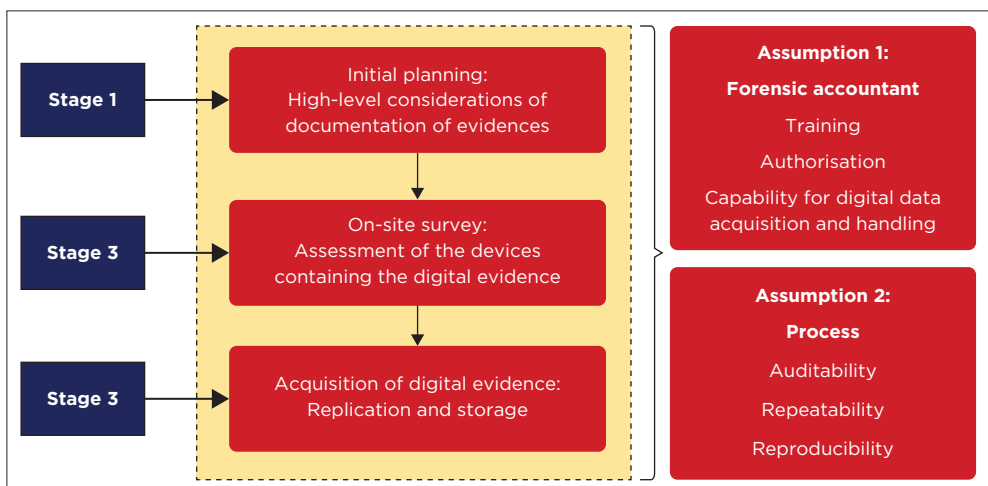
FIGURE 10.1: Digital forensic model proposed by Reith et al.

The second stage is the onsite survey for the on-the-spot assessment of the devices containing digital evidence. The last stage involves acquiring digital data for evidence replication and storage (Adams et al. 2013, p. 38). The use of this model is based on two major assumptions. Firstly, the model assumes that the forensic accountant is trained, qualified, authorised and equipped with specialised knowledge and expertise for performing digital evidence acquisition and handling. Secondly, the actions of the forensic accountant are auditable, repeatable, reproducible and justified.

Figure 10.2 captures the components of the proposed advanced data acquisition model for DF accounting.

Carrier and Spafford (2003, p. 1) incorporate the investigative process of the FA technique into a digital framework. The model suggested by the authors integrates the crime's physical and digital scenes for a thorough investigation to identify the perpetrator. It combines the application of both law enforcement and corporate investigations. According to Carrier and Spafford (2003, pp. 14-16), in the case of a server intrusion, the first phase is operational readiness, which allows an organisation to prepare for the incident. The phase comprises the incident response processes, kits and forensic accountant for the investigation. Next is the infrastructure readiness phase, where appropriate information and activities on the server are synchronised. At the detection and notification phase, the suspected intrusion is reported with the details of the affected system.

The incident is confirmed at the verification and authorisation phase, leading to the physical crime scene investigation. The physical search and information collection phase signals the beginning of digital crime, involving



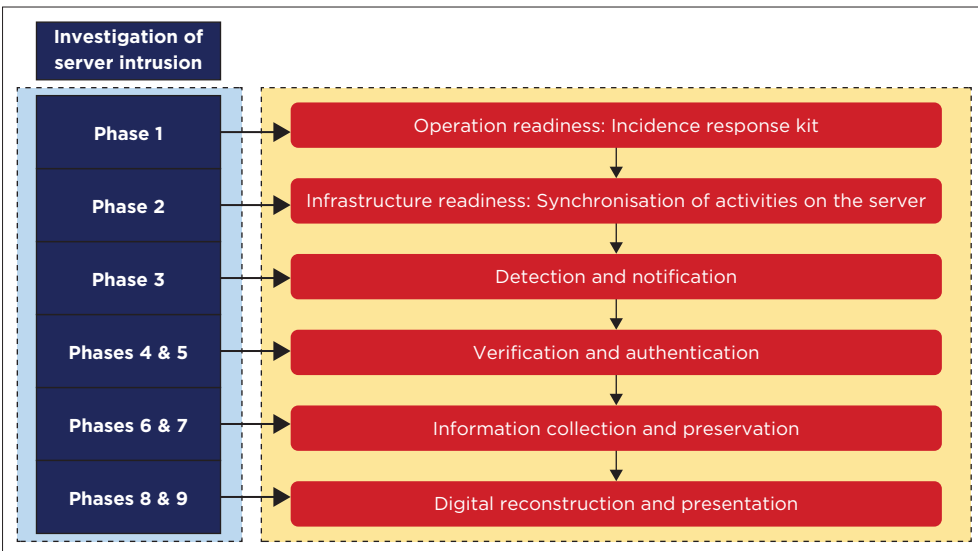
Source: Adapted from Adams et al. (2013, p. 38).

FIGURE 10.2: Components of the advanced data acquisition model for digital forensic accounting proposed by Adams.

the search for more details about the incidence. Next is the preservation phase, involving the duplication and storage of the digital data. At the digital reconstruction phase, the analysis of the evidence found will be carried out for a conclusion to be made. For the digital preservation phase, the final report of the analysis is presented and kept for reference. Figure 10.3 highlights the digital model components that Carrier and Spafford (2003) proposed.

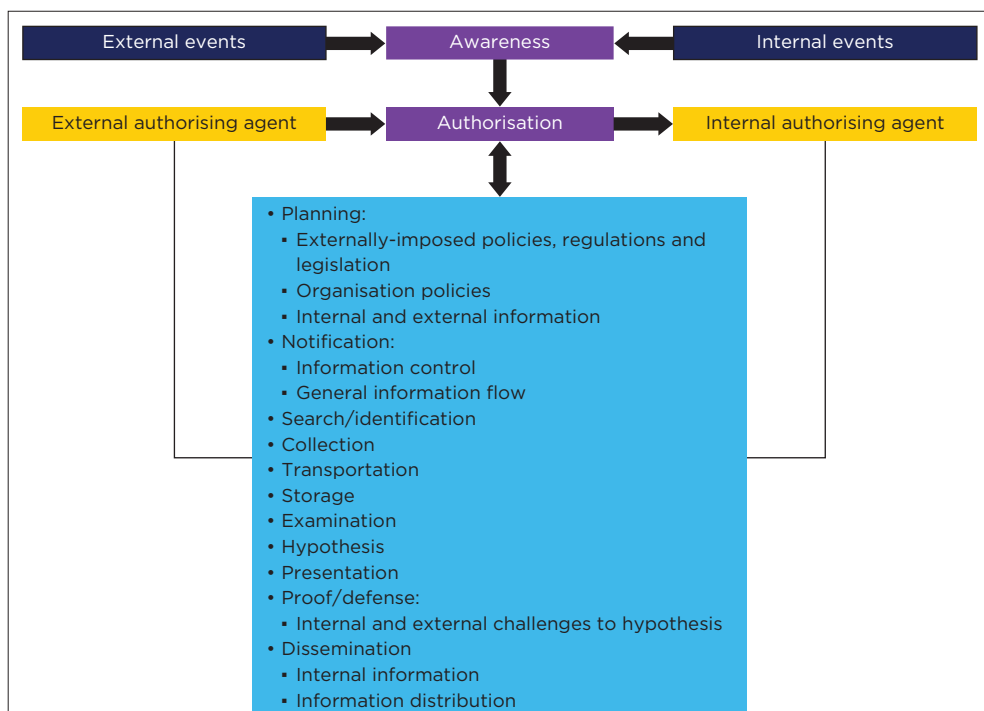
Ciardhuain (2004, p. 1) proposes a comprehensive model to identify the critical operations necessary to model the information flow during forensic investigation in a single digital setup. This is geared towards cybercrime investigation.

The extended model integrates the existing models, generalising them, and explicitly addresses certain activities not part of the current models. The model presents the flow of information during an investigation with an adequate capture of its full scope (Figure 10.4). According to Ciardhuain (2004, pp. 15-17), the first phase is the awareness phase, which involves the exchange of information between the bank and the investigator about the occurrence of fraud. At the authorisation phase, approvals are secured by the external investigator to search for evidence and investigation. Next is the planning stage, where the investigator decides on the best strategy to identify the suspect and collect the necessary evidence. Next is the notification phase, which involves informing stakeholders about the investigation processes. The phase consists of the search for evidence and information, collection of information, preservation and movement of



Source: Adapted from Carrier and Spafford (2003, pp. 14-16).

FIGURE 10.3: Components of the digital model proposed by Carrier and Spafford.

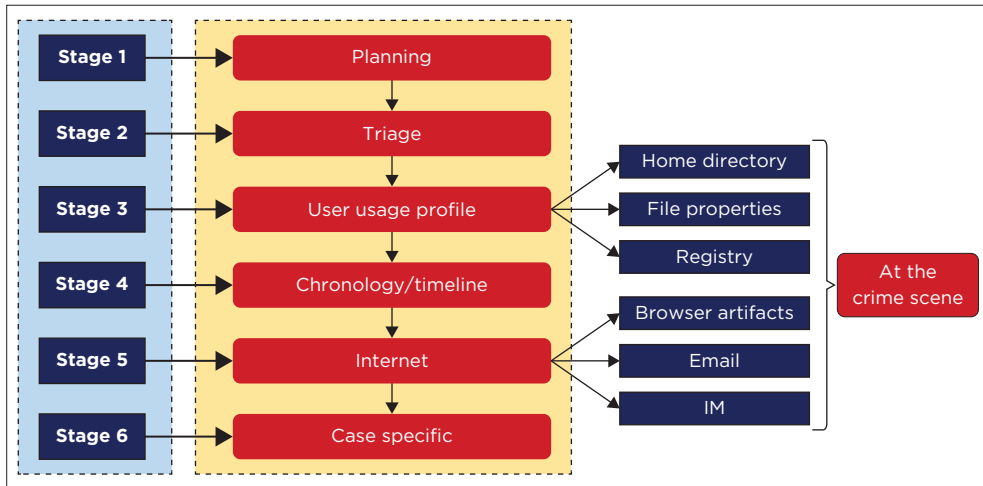


Source: Adapted from Ciardhuain (2004, p. 22).

FIGURE 10.4: Proposed model for cybercrime investigation.

digital information from the bank's file or server to the investigator and subsequently, the storage phase, where the transferred information is retained. The next is the examination phase, involving a detailed analysis of the information collected and the hypothesis phase, which validates or refutes the allegation of cybercrime. This phase is followed by the presentation phase throughout the investigation lifecycle. It involves the exhibition of the evidence gathered by the bank to the investigator or the investigator's findings to the court. This phase is followed by the proof and defence, which occurs once litigation is initiated. The last phase is the reporting phase, which involves disseminating the activities and the outcome of the investigation or litigation.

Rogers et al. (2006, p. 19) proposed using the computer forensics field triage process model (CFFTPM) to close the gap between physical and digital examinations. The model comprises six significant phases, as shown in Figure 10.5. The essence of the model is to provide the information to be used during the detailed investigation or litigation stage. The first stage is the planning stage, a pre-investigative process in which the investigator quantifies the various possibilities relating to cybercrime and the digital evidence acquired.



Source: Adapted from Rogers et al. (2006, p. 21).
 Key: IM, instant messaging.

FIGURE 10.5: Proposed computer forensics field triage process model by Rogers et al.

The second stage is the triage stage, where the investigation process commences, and the investigator relates directly with the suspect and the crime scene. Next to this stage is the usage stage, where the analysis and examination of the storage system are carried out with the possibility of obtaining more evidence. At the chronology stage, the sequence of events of the investigation, including the timeline, is defined.

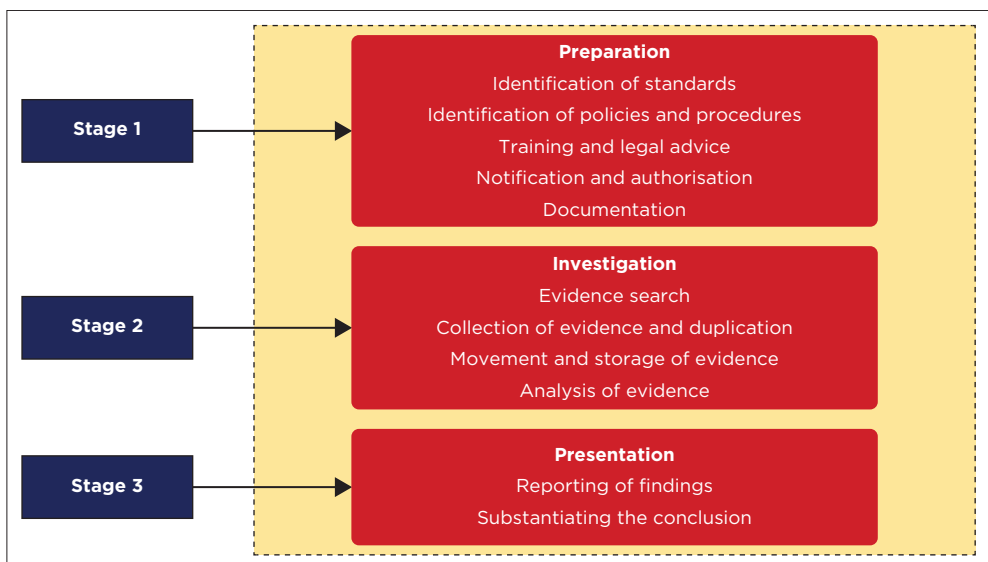
The next is an examination of the artefacts which relate to the Internet activities of the suspects, for example, emails, web browsing and instant messaging. At this stage, the forensic investigator examines the Internet-related activities involving the suspects and establishes a relationship with the case, if any. The last stage (case-specific evidence) aims to adjust the focus of the investigation to the specific case. The investigator looks in-depth into the case and reconciles the conflicting requirements.

Köhn, Olivier and Eloff (2006, p. 3) highlighted the three essential parts of a digital FA model for comprehensive investigation and reporting. They are the preparation, investigation, and presentation stages (Köhn et al. 2006, pp. 6-7). According to the DF investigation framework proposed by Köhn et al. (2006), the preparation stage includes the identification of standards used by the organisation, identifying policies and procedures that can aid forensic investigation, training and legal advice, the notification of concerned authorities, and documentation of previous incidences and planning. The investigation phase includes evidence search, collection of evidence and duplication, evidence movement to a safe location or repository, evidence storage, and evidence analysis using the right FA tools. Two vital steps were identified at the presentation stage: presenting findings and substantiating the conclusion reached during the investigation.

Figure 10.6 shows the framework for the proposed DF investigation proposed by Köhn et al. (2006).

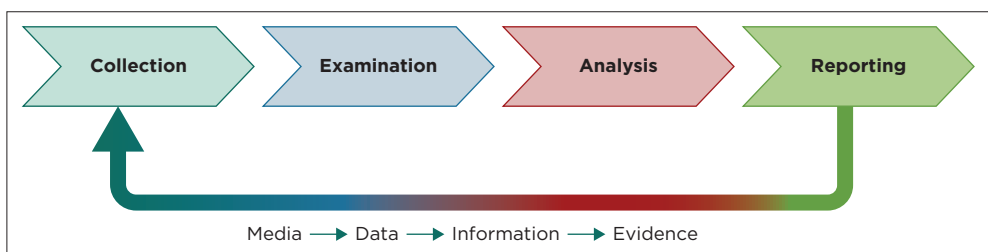
Furthermore, to enable organisations to develop customised forensic capability based on their requirements, Kent et al. (2006, p. 2) developed a forensic process framework to provide the required information to promote DF accounting use in organisations (Figure 10.7). In the framework, importance was laid on the processes of information acquisition investigation, analysis and reporting as the necessary steps for fraud mitigation. The forensic process framework comprises four primary phases: collection, examination, research and reporting.

During the first phase (collection), data linked to the incidence is sorted, collected, labelled and documented. The second phase (examination) involves applying the proper forensic techniques to the data gathered and



Source: Adapted from Köhn et al. (2006).

FIGURE 10.6: Framework for digital forensic investigation proposed by Köhn et al.



Source: Adapted from Kent et al. (2006, pp. 3-1).

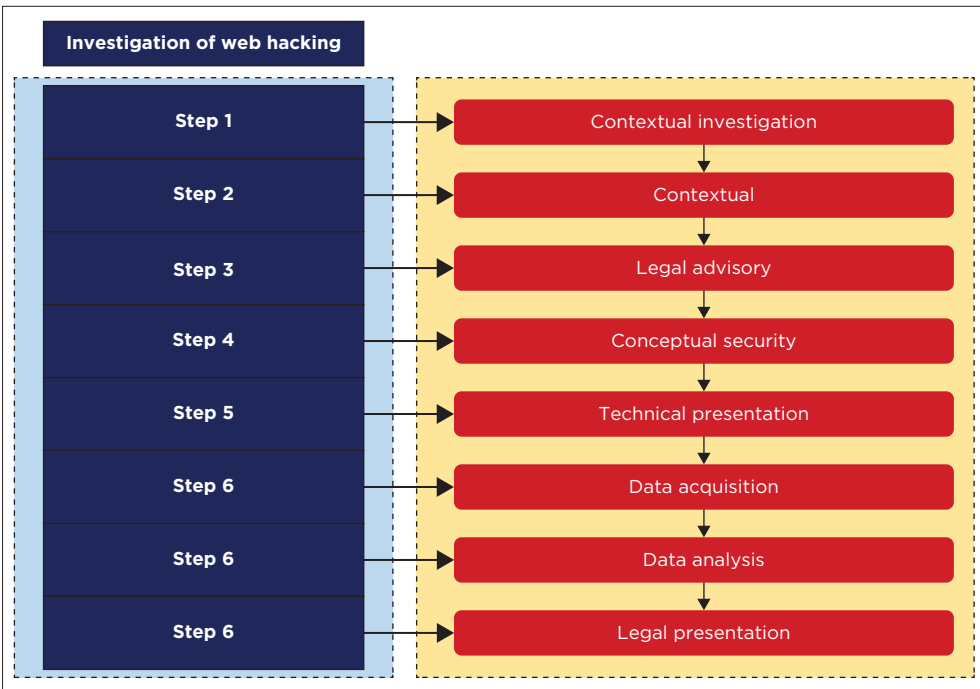
FIGURE 10.7: Forensic process proposed by Kent et al.

extracting relevant information. At this stage, the extracted data are converted into a processible format using the appropriate FA technique and subsequent transformation of the data into relevant information.

In the next phase (analysis phase), the investigation outcomes are analysed to obtain valuable facts which address the questions relating to the incidence. The final phase involves reporting the findings from the analysis, describing the actions performed, determining the course of activities to be taken and recommending procedures, processes or policy improvements (Kent et al. 2006, pp. 3-1).

Leong (2006, p. 29) developed an FA digital framework incorporating legal issues (Figure 10.8). The proposed framework seeks to integrate the roles of a prosecutor into the forensic investigation process for ease of work and information flow. This is aimed at enabling the acquisition of essential information necessary for prosecuting culprits during a forensic investigation. The proposed model incorporates a technical-independent framework to connect the activities of the information technologists, legal practitioners and investigators. The framework comprises eight layers. The first layer is the contextual investigation layer.

In the case of a hacked corporate web system, the investigation team leader would determine the possible rationale and motivation for the



Source: Adapted from Leong (2006).

FIGURE 10.8: Digital framework for forensic accounting, which incorporates legal issues proposed by Leong.

incident at the contextual investigation layer. This will answer the question of 'why'. The investigation team leader will also confirm the type of incidence and ascertain the need for investigation. Next is the identification of the parties involved. This will answer the question of 'who'. The time of the incident will be confirmed ('when'), as well as the reporting time, start time and end time of the cybercrime incident.

Next is the verification of the location of the incidence (where) and the determination of the nature of the incidence (what). Next to this is the planning phase to unveil the strategies for the investigation (how). This event leads to the next layer in the model. In the second layer, the investigator will seek input from the organisation by conducting a preliminary interview with some of the organisation's employees. This will add to understanding the business's nature and objectives, the nature of the data affected and the organisational structure and systems support. Next to this layer is the legal advisory layer. At this layer, the investigator seeks legal advice on the necessary information to be acquired, legal implications, time frames and case eligibility for litigation. The outcome of this layer will determine whether the investigation will focus on the root cause of the web hacking or initiate a legal procedure. The fourth layer is the conceptual security layer, which explores the organisation's information structure and security controls. This is necessary to determine the occurrence pattern of the incident and the nature of security controls put in place by the organisation before the incident. Next is the technical presentation layer, which involves planning the required forensic investigation objectives, data and entity model. As web hacking cannot occur without human involvement, the hypothetical data model will outline the relationship between the entities involved and the parties to be interviewed at this stage.

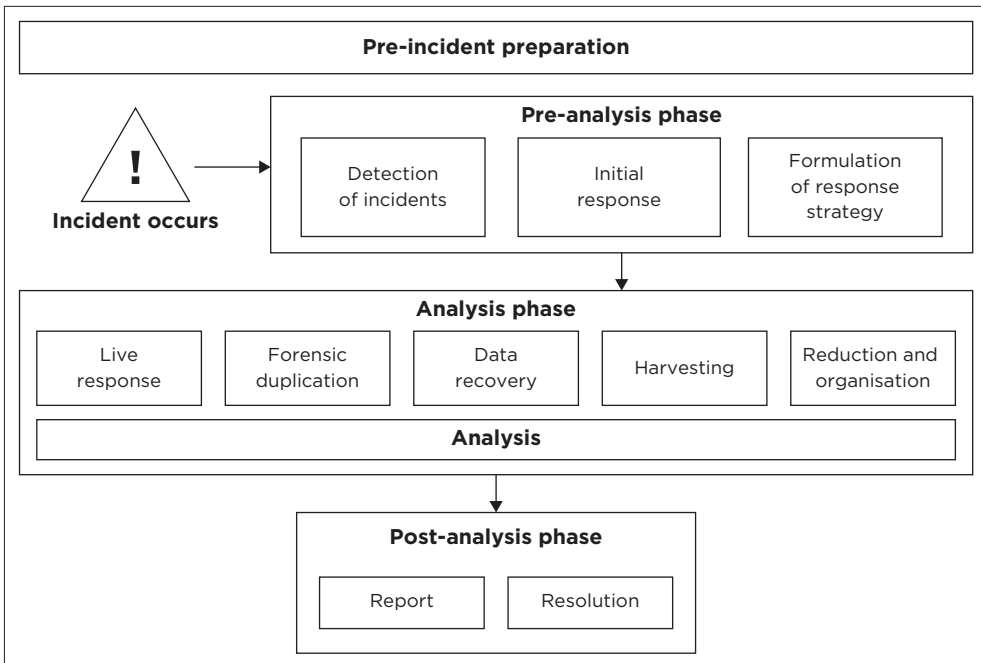
The next stage is the data acquisition layer, which involves checking the log files from the servers and the hacked servers, onsite forensic investigation, interview of the suspects and witnesses, and forensic data acquisition. This is aimed at gathering the relevant data for FA. At the next stage, the data analysis layer, the acquired data is moved to the forensic laboratory for analysis. The extraction of relevant information is carried out according to the hypothetical model, followed by the reconstruction of the event data.

Also, the network information, user account, phone numbers, electronic mail, organisational chart and IP address information from the network service provided are further analysed. The last layer is the legal acquisition layer, which presents the legal objectives, attributes and procedures. At this stage, the suitability of the case for litigation and the relevance and admissibility of the data will be determined.

Valjarevic and Venter (2012, p. 1) highlighted the process flow framework to reduce flaws and promote adequate documentation during

a fraud investigation. The process flow model comprises thirteen phases that incorporate the phases underscored by the previous model. These phases are the incidence detection phase, first response phase, planning and preparation phases, incidence scene recording, prospective evidence detection phase, prospective evidence acquisition phase, forthcoming evidence transportation phase, prospective evidence storage phase, prospective evidence analysis phase, presentation phase, conclusion phase and the parallel action phase. The authors proposed that some phases, such as incident scene documentation and potential evidence identification, should be performed consistently and simultaneously. This is to ensure efficiency during the investigation and admissibility of digital evidence.

Freiling and Schwittay (2007, p. 1) proposed a model that integrates incident response and computer forensics processes into a single flexible model. The incident response component of the model detects and contains the computer security incidents while the DF obtains valid evidence of cybercrime perpetration for investigation. The model allows for efficient management during digital investigations. The authors emphasised that there are three significant stages of analysis, namely, pre-analysis, analysis and post-analysis. The activities which characterise each of the phases are captured in Figure 10.9.



Source: Adapted from Freiling and Schwittay (2007, p. 10).

FIGURE 10.9: Process model for incidence response and digital forensics proposed by Freiling and Schwittay.

Khatir and Hejazi (2007, p. 10) developed a process model to ensure the evidence's reliability. The authors concluded that the reliability of evidence presented in the court plays a vital role in the success of a forensic investigation. The model integrates parts such as confirmation, authentication, authorisation, documentation, preservation and physical and digital evidence collection to improve the quality of evidence gathered during fraud investigation. Hence, the work contributes knowledge by providing a process model responsive to the management and team responsibilities and exculpatory and inculpatory evidence. Selamat, Yusof and Sahib (2008, p. 166) integrate the common parts in the previous models to obtain a more concise DF investigation framework. The study proposes a digital forensic investigation framework (DFIF) map that groups similar procedures that produce the same outcome into a single phase. This is done to balance the process and obtain substantial evidence for litigation purposes. The identified parts include the data collection preparation, examination and analysis, preservation, presentation, or fact reporting. Agarwal et al. (2011, p. 118) developed a systematic DFIF that can promote the development of an organisation's policies and procedures. The framework integrates all the phases and activities a forensic accountant requires for fraud detection. The study presents a consistent, standardised model for DF investigation comprising a model that works systematically and flexibly enough for compatible applications in other countries' DF investigation technologies with a general approach that can be used to relay the technology to a nontechnical observer.

This review presents various DF models, the components of the forensic models, and the procedural steps for cyberfraud mitigation. From the discussion, the different models will assist financial organisations in capturing, preserving, analysing, and presenting information or evidence necessary for litigation to mitigate cyberfraud. The models also provide a generalised framework for DF tool development and a standardised method for cyberfraud investigation. The models present the approaches needed for integrating the present and future technologies into the DF framework with the potential for incorporating both digital and nondigital information. As there is no globally acceptable model because of the uniqueness of the forms of cyberfraud and the organisational mitigating approaches, organisations can adopt any models that fit into the organisation's structure.

Alternatively, an organisation can adjust any of the described models to fit into the organisation's control structure. The flexibility of the models will allow the incorporation of the various components of forensic models to meet an organisation's need for cyberfraud mitigation. Akinbowale, Klingelhöfer and Zerihun (2021) developed two conceptual and simplified FA models incorporating DFs for cybercrime mitigation. The first model

integrates FA principles into an organisation's control structure, while the second details the investigation and comprehensive data analysis processes for fraud mitigation.

■ Types of digital forensics

Among others, the types of DF may include the following listed and discussed in the following sections.

■ Disk and storage forensics

This involves extracting information or data from media or storage devices by searching active, modified, or deleted files.

Decker et al. (2011, p. 355) indicate that computer forensic tools can be used to search systems and digital devices to acquire evidence thoroughly. Some of the information which is potential evidence may reside in the trash files, having been deleted, while some may be kept in hidden locations. Thus, computer forensic tools can scan through the space between or at the end of files or clusters where vital information or data may reside. Also, the slack space not used by an active file may harbour some data. Miller and Martson (2011, p. 181) state that some information needed for a forensic investigation can be retrieved electronically in this digital era. Hence, the information stored on systems, electronic devices and accessories such as photocopying or printing machines, personal computers, servers, digital cameras, and storage devices can be acquired for investigation using DF tools (Miller & Martson 2011, p. 181).

■ Network forensics

This involves monitoring and analysing computer network traffic to collect important information and legal evidence (Pilli, Joshi & Niyogi 2010). With network forensics, the entire contents of electronic mail, Internet surfing activities and file transfers can be recovered from the network equipment to reveal the original transaction. The network protocol data surrounding each communication is vital to investigators to understand the scenario being investigated (Conrad, Misener & Feldman 2012). Some of the challenges of network forensics may include data storage, integrity and privacy, access to the IP address, data extraction location and high data transmission speed.

■ Database forensics

This deals with studying and examining databases and their related metadata to acquire information for investigation. Fowler (2016) defines database forensics as part of forensic science that analyses and preserves

relational and non-relational database platforms. The goal of database forensics is to trace past activities within database systems, recover previously deleted information or data and determine the pre- and post-state of information. Thus, database forensics can enable an investigator to investigate breaches relating to information stored on the database. It can also assist in tracking suspected intrusion and determining the scope of a violation to limit its impact precisely (Fowler 2016).

■ Malware forensics

This deals with identifying malicious code, viruses, worms or other unauthorised programs that interfere with the personal or organisational system. It is the science of investigating and analysing the properties of malware viruses and probing the rationale behind the attack by the culprits. Malware forensics may include certain activities such as investigating the malicious code, determining the method of entry and propagation of the malicious code, and its impact on the system. Brand, Valli and Woodward (2010) indicated that malware forensics aims to extract signatures from the malware for threat detection and to develop eradication strategies.

■ Email forensics

This deals with recovering and analysing emails, including deleted emails, calendars, and contacts. The communications of fraud perpetrators can be tracked through active or deleted electronic mail. During a fraud investigation, the FA of emails can be used to determine the date, source, legitimacy, time, the sender's identity, recipients, IP address, and hostname. Panhalkar (2023) indicates that email forensics is a systematic and in-depth scrutiny of emails, such as the transmission routes, attached files and documents, servers, computers, and sender IP addresses. Through email forensics, the source of emails can be tracked. When emails are deleted from the personal computer, the server can be scanned because it typically keeps a copy of any email sent after delivery. From the logs of email retained on the server, the personal computer's address can be traced to the original sender. When the server is unavailable, the network devices such as the switches, routers and firewalls can be used to trace the source of the mail (Panhalkar 2023).

■ Memory forensics

This deals with collecting data from system memory or other external memories in the unprocessed form. It is an essential form of cyber investigation that allows an investigator to identify unauthorised or anomalous activity on a target computer or server. Memory forensics is

usually achieved by running unique software that captures the current state of the system's memory as a snapshot file, otherwise known as a memory dump (Messina 2019). A forensic investigator can then analyse the captured file. Memory forensics is useful during fraud investigation in corporate organisations because it gives access to the processes, files and programs that run in the system's memory. Therefore, once these processes, files, and programs are captured, other important information such as the IP addresses, network information, system users, and files are opened, and the investigators can track the identity of those who opened them. Hence, suspicious programs, malware and viruses can be tracked down and traced to their sources. Sometimes, the activities of the viruses and malware on the computer system may be hidden; the use of memory forensics can assist in identifying their presence, activities and sources (Messina 2019).

Furthermore, some of the information in the system's memory may be volatile; memory forensics can enable the capturing of this volatile information and subsequent storage.

Memory forensics differs from disk or storage forensics. Memory forensics captures the current snapshot of a system while in use. This provides the forensic investigator with the actual time image of the system, while disk or storage forensics is usually employed for data recovery and decryption from a particular disk or storage device. Thus, memory forensics can provide a real-time response to a threat, while disk or storage forensics can acquire information or data after an incident occurrence. Memory forensics is time-sensitive and used for acquiring volatile data or information. Disk or storage forensics is not time-sensitive and can be used for acquiring less critical data or information than memory forensics. In memory forensics, image capturing depends on the nature of the investigation. Usually, memory forensic investigation relates to the user's activities on the system and other evidence that establishes the fact that a system has been compromised.

According to Messina (2019), some examples of acquisition formats that can be used in memory forensics include:

- **RAW format:** Information extracted from a live environment.
- **Crash dump:** Information gathered by the operating system.
- **Hibernation file:** A saved snapshot of your operating system that can return after hibernating.
- **Page file:** A file that stores similar information to that stored in your system's RAM.
- **VMWare snapshot:** This is a snapshot of a virtual machine that captures and saves the system's state when the capturing was carried out.

Some specific examples of memory forensic tools include data carving, volatility suite, Helix ISO, Belkasoft RAM Capturer and Process Hacker.

According to Messina (2019), some common approaches that can be used by a forensic investigator when acquiring information through memory forensics include:

- **Open files associated with process:** This approach shows the files opened by a suspicious process on the system. Malware attacks can be tracked by locating the opened files linked to them. This may mean some breach of security or controls, which an investigator may use as evidence.
- **Decoded applications in memory:** Perpetrators of malware attacks may code or encrypt the system to confide the accessibility and usage of the information collected to themselves. The decoded or decrypted version of the application can be captured in the memory snapshot, which may assist the forensic investigator in precisely accessing previously encrypted information and investigating the activities of the attacker and the application.
- **Timestamp comparison:** Sometimes, malware interference with the target host's timestamps on the system files can prevent the investigator from discovering when the infection occurred. However, capturing the memory dump can assist the forensic investigator in comparing the process time stamps to the system file timestamps to establish the first time and date the system got compromised.
- **Network information:** Once the infected files and processes have been identified, the specific network communications related to the infection can be identified. This can aid other information such as the source IP address linked to the malware, the compromised ports on the target system, the frequency of communication of the malware over the network and other information on the spread of the infection on the network.
- **User Activity:** This deals with the examination of the previous information and activities of the user to establish the circumstances that led to the incident. This can be ascertained through the system log files earlier captured to show the user's involvement in the attack. In addition, the level of compromise of the network protocol and intrusions can be detected.

■ Mobile phone forensics

This deals with the inspection and analysis of mobile devices. Fraud perpetrators can be tracked by tracking the communications on the phone, SIM contacts, call logs, incoming and outgoing text or multimedia messages, audio and videos. The mobile device can store much information that can aid criminal investigation, thus the need for mobile phone forensics. Mobile forensics can provide insights into the scope of attack, methods and

networks of the perpetrators. Mobile forensics retrieves digital evidence from mobile devices such as smartphones, androids, and tablets. Mobile devices contain text messages, history of websites searched and visited, information downloaded, communications and data location history, which may be helpful during fraud investigation (Security Scorecard 2022).

The phone calls, text messages, images, audio, videos and visited websites acquired from the phone of a suspected fraudster can be linked to various forms of cybercrime such as online money laundering schemes, cyberstalking, data breach litigation, digital extortion, ransomware hacking incidents, DoS attacks and phishing.

According to the Security Scorecard (2022) report, there are guidelines for mobile phone forensics before the evidence presented can be admissible. These include:

- **Step 1: Seizure.** This must be done in line with the law guiding the arrest and seizure of the properties of the perpetrator in the domiciled country. For instance, the law enforcement agency may seize the suspect's mobile device and hand it over to the forensic investigator. The forensic investigator must handle the devices cautiously to track and preserve the evidence.
- **Step 2: Acquisition.** Important information linked to the incident under investigation can be extracted as potential evidence. This can be done by duplicating the files with a software imaging tool. The duplicate must maintain the integrity of the original files to be used as evidence for the original copy. In other words, no alteration or modification can be made to the duplicate files not to nullify the proof.
- **Step 3: Analysis.** Once the critical information has been extracted, the forensic investigator must conduct data analytics to detect fraud, establish trends, or scientifically link the information acquired to the fraud incidence.
- **Step 4: Examination.** The outcome of the analysis must be examined in line with the rules of evidence before it is tendered as evidence for litigation.

■ Challenges faced by digital forensics

The significant challenges faced by DF:

- Many organisations have systems that may be linked to fraud perpetration. The scrutiny of each of these systems may be time-consuming.
- The dynamics and anonymity of cyberspace may make it difficult to track down some information.
- Lack of physical evidence makes prosecution difficult. However, it often produces a credible result when matched with physical evidence.

- Usually, big data (large amounts of data collected from different sources) requiring large amounts of storage space are collected and processed during DF. This often makes the work of an investigator challenging.
- Digital forensics is dynamic and subject to changes with technological advancement. Hence, an upgrade is usually required with time.
- The admissibility of DF evidence necessitates absolute compliance with the rule of law and guiding relations.

■ Merits and demerits of digital forensics

The merits of DF include:

- It ensures confidentiality and the integrity of the computer system.
- It helps to gather credible and admissible court evidence for litigation against the culprit.
- It helps organisations to capture or recover important information anytime their network or system is compromised.
- It can aid the tracking down of cybercriminals from anywhere in the world.
- It fosters information security.

It permits acquiring, analysing, interpreting and preserving information or data as potential evidence.

■ Demerits

- The process of capturing and storing electronic records is time-consuming and relatively costly.
- The investigator and the attorney must have extensive computer knowledge.
- The evidence from the DFs must be authentic and convincing.
- Digital forensic evidence that does not comply with the specified guidelines and standards stands the risk of court disapproval.
- Insufficient investigator expertise and technical knowledge may affect the outcome of the forensic investigation.

Williams (2023) and Miller and Martson (2011, p. 175) indicate that DF comprises identification, information gathering, analysis storage and documentation. Nigrini (2011) states that the DF process for investigation could aid in uncovering corporate fraud, such as suspicious financial reports or transactions. Nissan (2012, p. 841) also supports this notion that a reliable DF technique can be employed to investigate, detect and prevent electronic crime. The evidence gathered from the DF investigation is known as CDE (Grobler & Louwrens 2009, p. 4). This refers to the digital evidence containing the information for prosecuting a culprit in court.

With increasing technological changes, there is a need to support FA frameworks with DF to meet the demand of conducting successful investigations (Mushtaque et al. 2015, p. 233). Integrating digital components into the FA framework can aid the research through incidence capturing and evidence preservation. Acquiring reliable and valid evidence will improve the investigation's efficiency and outcome. The result of a FA investigation is partly a function of the evidence gathered and its handling processes. Digital forensics can enhance the recovery and information of potential evidence found in digital devices related to cybercrime.

The proper identification, protection, sorting, and reporting of digital information as evidence can promote evidence admissibility in the court, thereby enhancing the litigation process (Adhyansh 2021). Adhyansh (2021) further indicates that the digital accounting forensic phases can be categorised into four: information identification, preservation, examination, documentation and presentation. Mushtaque et al. (2015, p. 237) suggest the implementation of a DF model as a component of FA to aid:

- evidence collection, examination, preparation, preservation and presentation
- retrieval of information that has been lost or tampered with
- rapid and proficient searching, sorting and analysis of information or evidence
- reporting and drawing of outcomes from all the preceding phases.

Rowlingson (2004, p. 1) explains that DF evidence is usually valuable for combatting security threats in an organisation. The author further elucidated that information security programs are often employed as preventive and detective measures. Hence, as a preventive measure, DF evidence might be less beneficial but highly beneficial from a business perspective, where certain situations require collecting suitable digital evidence. However, developing a system capable of acquiring digital evidence should be implemented before an incident occurs (Rowlingson 2004, p. 2).

An organisation can leverage digital evidence to enhance the costs and cost-effectiveness of an investigation depending on the size of the organisation and the nature of the investigation. Forensic digital evidence could assist in the effective management of the impact of specific business risks, and it could also assist in the litigation process and in verifying the terms of a transaction.

It can also be used to substantiate a legal process. Hence, an organisation usually desires to support its position during litigation (Rowlingson 2004, p. 2). It is generally feasible within organisations' fraud, theft, or dispute concerns, which require valid evidence and not just information security defence against fraud (Rowlingson 2004, p. 4).

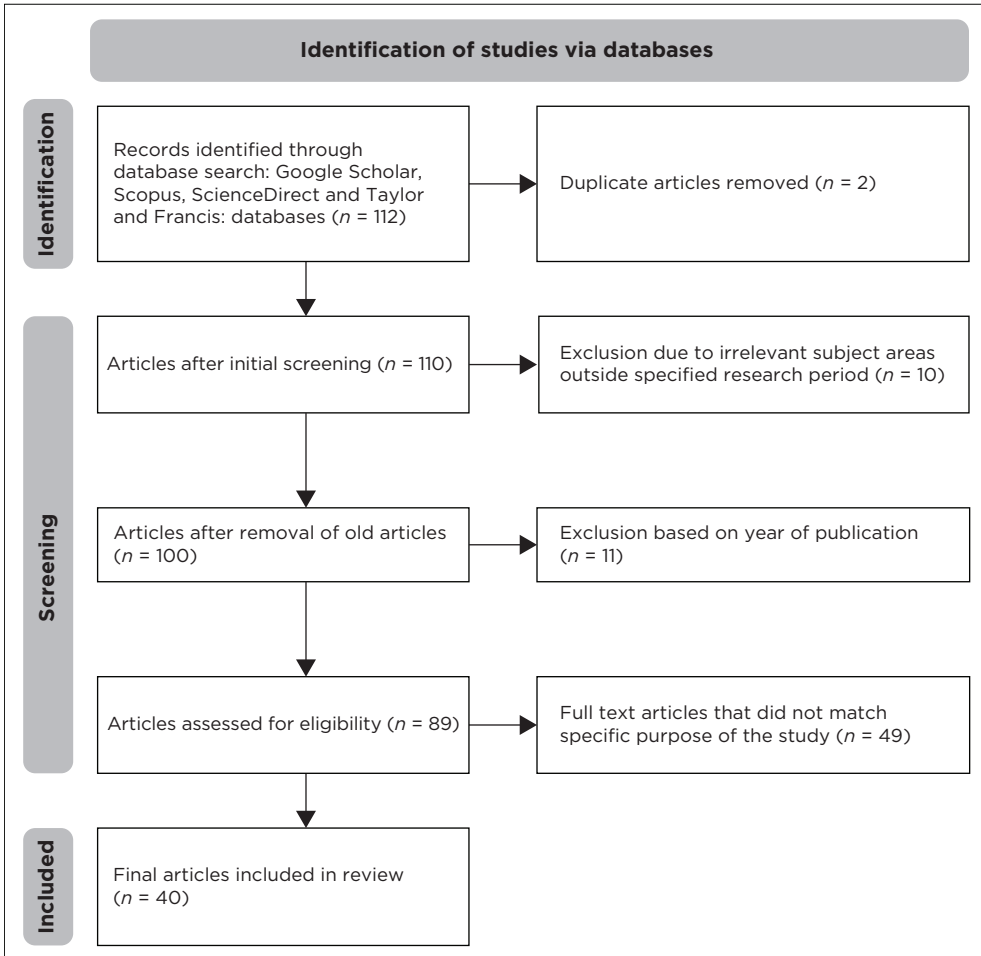
In addition, Rowlingson (2004, p. 9) describes ten key activities necessary for implementing a forensic programme as:

1. defining the business situations which require digital evidence
2. identifying the sources and various types of prospective evidence
3. determining the requirements for the collection of evidence
4. establishing the capability for gathering digital evidence legally such that it will be admissible as evidence during the litigation process
5. establishing a procedure for the safe handling and storage of potential or captured evidence
6. effective monitoring to ensure the detection and deterrence of significant incidents
7. specifying the circumstances in which the digital evidence may be launched for full investigation
8. staff training on incidence awareness and sensitivities of evidence from the legal perspectives
9. documenting an evidence-based case which describes the occurrence and its impact
10. providing a legal framework to facilitate effective prosecution of the culprits.

■ Methodology, results and discussions

■ Methodology

This study conducts a systematic literature review to investigate the role of DF in fraud investigation. Firstly, relevant articles were obtained using the search engines and the most relevant ones were systematically reviewed. The systematic review comprises data source identification, search procedure, the use of keywords, and the implementation of the exclusion and inclusion criteria (Akinbowale et al. 2021; Daniyan et al. 2021). The keyword search was to ensure that only related literature was reviewed. Some keywords employed include 'digital forensic', 'types of digital forensic', 'digital forensic model/framework', 'digital evidence' and 'computerised forensic investigation'. A total of 112 articles were initially obtained using different search engines, but only 40 were reviewed because of their relevance to the topic discussed. The 60 articles selected were based on their relevance to the issue of discussion, the year of publication, and the results obtained. The systematic review employed in this study followed the procedure outlined in the review of the guidelines provided in the existing works (Abdulrahman et al. 2020; Kitchenham et al. 2009). To streamline the study, the relevant inclusion and exclusion criteria, such as the year of publication and the relevance of the keywords to the subject matter, were considered (Daniyan et al. 2022). Figure 10.10 presents the framework for the systematic literature review employed in this study.



Source: Authors' own work.

FIGURE 10.10: Framework for the systematic literature review.

Results and discussions

Table 10.1 summarises the recent advances in developing a sustainable digital framework for fraud investigation.

The literature reviewed gathered that ‘digital forensics’ encompasses various fields such as computer forensics, network forensics, mobile device forensics, memory forensics, database forensics, malware forensics and incidence forensics. There was a consensus among the authors that the DF process encompasses using unique techniques to investigate electronic storage and smart devices to gather data for analysis and evidence in court. The method comprises critical phases such as evidence identification, acquisition, analysis, reporting and documentation. In cyberfraud mitigation,

TABLE 10.1: Recent advances in the development of a sustainable digital forensic framework for fraud investigation.

Author	Contribution	Process
Pilli et al. (2010)	A generic framework for network forensics	Preparation, authentication, detection, incidence response, data collection, preservation, protection, examination, analysis, investigation, fact presentation and review
Agarwal et al. (2011)	Systematic digital forensic investigation model	Preparation, scene capturing, survey, documentation, communication, evidence collection, preservation, examination, analysis, result presentation and review
Amshire and Meshram (2012)	Development of a digital forensic model	Planning, scene capturing, examination, analysis, result presentation, review and reporting
Prayudi et al. (2015)	Digital forensic business model	Digital investigation, evidence handling, object identification and environment recognition
Jain et al. (2015)	Digital forensic framework	Planning, authentication, evidence gathering, cybercrime classification, reporting and future updates
Talib and Alomary (2015)	Comprehensive ontology-based examination for digital forensics of cybercrime	Preparation, investigation, scene capturing and presentation
Jadhaio and Agarwal (2016)	Digital forensics investigation framework for social networking	Checking, analysis, scanning, communication and reporting

Source: Yang and Wu (2017, pp. 25-37).

DF can be used for incidence response. In this case, security incidents are analysed to identify the root cause and determine the occurrence's scope. It could be used to analyse malware attacks whereby the activity and features of the attack, including the code, network activity, and system logs, are identified. Sometimes, data breaches could stem from within an organisation, whereby the employees abuse their confidential information to perpetrate fraud. This can also be investigated with the aid of DF. Existing studies also reported on the use of DF for the investigation of data breach incidences. The evidence gathered via DF in email communications, call or chat logs, or other electronic evidence can serve as evidence in criminal prosecution. However, the successful implementation of DF for cyberfraud mitigation requires some level of expertise in terms of technical and analytical proficiencies. For instance, deploying DF to combat cyberfraud requires knowledge of computer systems, software and networks beyond the basics. This may also include the knowledge of computer languages, operating systems and network protocols. The successful implementation of DF also requires understanding forensic techniques and tools used for investigation. The knowledge of data recovery, imaging and memory analysis are essential. Furthermore, DF personnel must be proficient in analytical skills such as pattern recognition, data-mining and ML to trace data patterns over periods to uncover fraud. Digital forensics also requires strong problem-solving skills because of the volume and complexity of data stored in electronic devices. In addition to these, DF personnel must

also acquire regulatory and legal knowledge relevant to the nature of the investigation. Understanding the regulatory framework and the legal implications of the investigation process will promote the admissibility of the evidence gathered in court. Finally, DF personnel must also acquire communication and reporting skills to pass complex and technical information to nontechnical stakeholders without ambiguity.

To promote cybersecurity, DF can be employed to identify the remote, primary or secondary source of the attack, including the location and the tool or techniques used by the threat actors. This information can assist organisations in making informed decisions on developing and implementing mitigating measures. Understanding the source and characteristics of cyber threats or attacks can also help organisations identify the vulnerabilities or loopholes in the security architecture the threat actors exploit. Thus, organisations can reinforce their security architecture via DF. This will enable them to investigate historical and real-time incidences and data and respond swiftly to cyberfraud incidences. Some examples of DF tools include Encase Forensic, FTK, EnCase, Tableau, ACL, IDEA, FTK imager, X-Ways Forensics, ProDiscover Forensics and Magnet Forensics.

■ Conclusion

Digital forensics involves recovering and investigating materials (evidence) found in electronic systems or devices related to digital crime. Many fraud-related cases are perpetrated or concealed digitally, hence the need to develop a DF framework for fraud investigation. Forty articles on DF were reviewed using systematic literature. The findings from the article reviewed that DF is needed to aid the process of evidence gathering and investigation in fraud-related cases. Many authors opined that the DF model could benefit the following: evidence collection, examination, preparation, preservation and presentation, retrieval of information that has been lost or tampered with, rapid and proficient search, sorting and analysis of information or evidence as well as reporting and drawing of outcomes from all the preceding phases. Thus, the study presents different DF frameworks which an organisation can adopt and adjust to suit the uniqueness of their organisation. This chapter adds to understanding DF and provides a blueprint for implementing DFs during a fraud investigation. Integrating DFs into the FA framework can aid the investigation process through incidence capturing and evidence preservation.

A systems-thinking approach

■ Introduction

This chapter uses a systems-thinking approach to develop information and cybersecurity frameworks for financial institutions' internal and cyberfraud mitigation. It was used as a diagnostic tool to examine the challenges of internal and cyberfraud and provide sustainable measures to mitigate them. To tackle it, the causal loop diagram was employed to gain insight into the causes and effects of internal and cyberfraud. By representing the internal and cyberfraud from a causal perspective, the causes and consequences of internal and cyberfraud were established. This led to the development of information security and cybersecurity frameworks to mitigate them. The causal loop diagram can assist organisations in understanding the relationship and interdependencies among the internal and cyberfraud variables identified. Furthermore, the information security and cybersecurity frameworks developed can aid decision-making relating to fraud mitigation and be adjusted to suit an organisation's need to mitigate internal and cyberfraud. This chapter adds to the existing information about using the system's thinking approach to visualise the challenges of internal and cyberfraud. It also highlights the multiple and interdependent effects of managerial efforts at mitigating internal and cyberfraud.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'A systems-thinking approach', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 217-234. <https://doi.org/10.4102/aosis.2024.BK485.11>

■ Information and security frameworks for internal and cyberfraud mitigation in financial institutions

Cybersecurity involves the protection of cyberspace and connecting devices such as computer systems and networks and services from intrusion, disruption, theft of or damage to their hardware, software or electronic data (Agarwal et al. 2011). On the contrary, information security refers to protecting an organisation's sensitive information from misuse, theft or intrusion. This ensures that the organisational information is strictly within the domain of authorised users (Agarwal et al. 2011). Cybersecurity and information security are intertwined because an organisation's information cannot be secure if the cyberspace, network and computer systems where the organisation's data and other information are stored are not safe. Feruza and Kim (2007) and Tiwari, Bhalla and Rawat (2016) argue that information security combines technologies and procedures to safeguard an organisation's networks and data from unauthorised users. Hinde (2003) estimates that a significant percentage of cybersecurity breaches can be traced to internal employees (either directly or indirectly). This implies that cybersecurity breaches may be minimised if a robust internal control mechanism is implemented to mitigate the potential red flags of internal fraud.

One of the challenges of financial institutions is information security (Akinbowale, Klingelhöfer & Zerihun 2020). Kopp, Kaffenberger and Wilson (2017) state that many financial institutions deployed emerging technologies to secure cyberspace from cyberattackers. Financial institutions are at risk of data and cyber breaches because of the exposure of their computer systems to cyberspace and the use of interconnected networks and other digital infrastructures for business operations (Dzomira 2014; UK Finance 2018).

Malik and Islam (2019) emphasise that public sensitisation is crucial to the information security approach. For any organisation to achieve holistic cybersecurity success, information security must be ensured at the personal and organisational levels. There is a need for regular sensitisation of the customers and the public about cybersecurity trends and the avenues employed by the perpetrators to commit crimes. Furthermore, customers must be aware of the necessary proactive or reactive steps to be undertaken personally to promote information security. These include using a strong password, levels of authentication, preventive measures to be taken while connecting to a public network, information protection or disclosure tips, and the organisational support mechanism in any cyber or information breaches (Dzomira 2015a, 2015b). Holappa et al. (2005) state that information security involves the deployment of administrative and technical capacities to ensure that an organisation's data and information are protected from unauthorised persons.

Cyber and information insecurity can negatively impact an organisation's financial performance, goodwill, reputation and shareholders' satisfaction (Dzomira 2017; Lagazio, Sherif & Cushman 2014; Mohd et al. 2010). It could also cause damage to the organisation's cyber infrastructure, poor operational efficiency and loss of confidence by the customers (Lagazio et al. 2014, p. 60).

In achieving information security, Choobineh et al. (2007) suggest the effective management of information security operations as part of the organisation's goals. Usher (2006) advocates the consideration of five factors relating to information security – confidentiality, integrity, network security, application security and host security. Hence, information security is necessary for minimising internal and cyber-related fraudulent activities.

■ Challenges of organisation's information security

Pooley (2013) identifies some of the challenges organisations face regarding information security:

- **High expectations of stakeholders:** Stakeholders usually place high expectations on the organisation's information security apparatus. Any information security breach by internal or external fraud perpetrators may be perceived as a betrayal of trust by the stakeholders.
- **Global and dynamic nature of threats:** Threat actors are increasingly becoming automated and sophisticated in their fraudulent schemes. Nowadays, cyberfraud is being coordinated so that many cyberattacks can be carried out simultaneously. For instance, the past decades have witnessed computer viruses constrained to individual users' systems, causing a slight decline in staff efficiency and organisational performance for a given period. However, now malicious threats may come in the form of blended threats, presenting multiple security threats and causing major disruptions and significant losses in an organisation's profitability. The blended threat combines various malicious codes to exploit the organisation's security vulnerabilities.
- **Lack of security expertise:** Some financial institutions primarily targeted for cyberfraud may not have enough security expertise. Although security experts are employed in some of these organisations, the number still falls short of those required to combat cyberfraud effectively. Using qualified information security personnel is a challenging task for many organisations. This may affect the maturity level and implementation of innovative and digital solutions from information security vendors that require information security skills. Thus, management must invest more in training and developing human capacity to overcome these challenges.

- **They are emerging digital technologies:** Information security challenges keep multiplying, necessitating the implementation of various technologies. Some emerging technologies exploit the lapses in an organisation's security architecture to commit fraud (Ali et al. 2017). Sometimes, organisational staff may find it challenging to cope with the dynamics of technology. Using smart and storage devices, including universal serial bus (USB) drives, creates a way for losing important information from the network and an avenue for malware attacks. Sometimes, employees may use personal accounts such as email addresses for corporate activities. Threat actors can hijack personal accounts to obtain sensitive information for fraud perpetration.
- **Information-sharing:** One of the main targets of the threat actors is information. The threat actors explore every means of searching for personal or sensitive information for fraud perpetration. Sometimes, employees may use personal accounts such as email addresses for corporate activities. Threat actors can hijack personal accounts to obtain sensitive information for fraud perpetration. Nowadays, businesses have assumed open innovation in this era of networking and globalisation, thereby necessitating collaboration and information-sharing among other organisations and stakeholders. This may affect information confidentiality and compromise the organisation's control of access to sensitive information. Threat actors can also hijack sensitive information from collaborators for fraud perpetration.
- **Customers' negligence and behaviour:** Another cause of information security lapses is customers' negligible behaviour. Customers sometimes overlook security tips such as confidentiality of sensitive information, strong passwords, caution in public network connectivity, clicking unverified links or downloading unknown email attachments. All these contribute to information security compromise, which threat actors leverage to commit fraud.
- **Data and ethical breaches by employees:** Tiwari et al. (2016, p. 46) state that data breach is another threat to information security where sensitive data are stolen. Sometimes, an organisation's employee may collude with external fraud perpetrators to divulge customers' and the organisation's confidential information for fraud perpetration (PwC 2020). The Verizon Data Breach Investigation Report (2012) posits that 75% of the 621 established cases of data breaches were financially induced.

Murphy and Free (2016, p. 41) survey fraud criminals in prison, employees of organisations and auditors who are fraud investigators. The study investigated the presence of instrumental climate (described as a condition whereby an employee violates ethical issues to make fraudulent decisions for personal or organisational reasons).

Omar, Johari and Hasnan (2015, p. 371) further suggest that organisations should implement ethical training programmes to strengthen ethical culture.

■ Information security risk management

Information security protects an organisation's data or information from intrusion, theft or misuse (Agarwal et al. 2011, p. 118; Jhawar & Piuri 2017, p. 165). Pandya and Frazin (2013) stress that information security aims to define and design an organisation's information architectural infrastructure to secure and protect information resources from theft, compromise and intrusion. The three main objectives of information security are confidentiality, integrity and availability. Confidentiality prevents unauthorised access to the data, while data integrity ensures that the data are correct in order and that all unauthorised modifications that can cause data compromise are blocked. On the contrary, data availability concerns the ease of accessibility of the acquired or stored data by authorised persons. Thus, information security is concerned with protecting information in the correct format from unauthorised users so that it is only accessible to authorised users (Agarwal et al. 2011, p. 118; Jhawar & Piuri 2017, p. 165). Tiwari et al. (2016, p. 46) and Feruza and Kim (2007, p. 17) define information security as the integration of procedures and technologies intended to protect information from intrusions by cybercriminals. Information security means effectively protecting data or information systems from unauthorised intrusion. Information security is often used interchangeably with network security or cybersecurity, but there are differences between them, though they are interconnected. Having defined information security, cybersecurity can be seen as a subset of information security that protects an organisation's cyberspace, including Internet-connected systems, from potential cyberattacks. On the contrary, network security is a subset of cybersecurity concerned with preserving an organisation's IT and Internet infrastructure from online threats.

Information security is a significant challenge in financial institutions. However, organisations must implement control policies such as access control policies, systems or network intrusion detection architecture and regulatory compliance to promote information security. Despite generally strong controls developed by financial institutions to guide against intrusion, fraudsters continuously create methods to perpetrate personal data theft and commit fraud. Therefore, financial institutions need to implement an information security risk management system in addition to solid control.

The International Standardisation Organisation (ISO) defined risk as the result of an uncertainty on a target, in other words, the combination of likelihood and consequences (ISO 2011). Risk levels are often categorised

based on the potential events, the consequences or a combination of these factors (ISO 2018). Financial institutions are subject to cyber risk due to a combination of factors, such as the digital nature of the technology used for business operations, the Internet-enabled systems and devices and the dynamics of cyberspace, among others. Thus, it is incumbent on the institutions to plan, control, monitor and organise fraud prevention plans and risk management strategies to mitigate cyber risks. Kopp et al. (2017, p. 6) indicate that the challenge of anonymous perpetrators who exploit cyberspace for fraud perpetration also increases the threat levels of cyberfraud perpetration in many financial institutions. UK Finance (2018) emphasises that the financial institutions and customers' exposure to cyberspace and dependence on interconnected networks and critical infrastructures for business operations are major risk factors. Furthermore, the sophistication of cybercriminals and the reduction in counterattacks may make some financial institutions more vulnerable to cyberattacks. The consequences of cyberattacks on financial institutions may be in the form of a reduction in the organisation's financial or operational performance, loss of the organisation's goodwill and reputation, as well as stakeholders' dissatisfaction and destruction of critical banking infrastructure (Lagazio et al. 2014, p. 60). Altamimi (2011) indicates that the banks in Saudi Arabia devote more efforts to external risk management than internal risk. Hence, the banking institutions in Saudi Arabia are more protected from external risks than internal attacks from employees.

To promote information security, an organisation must include it as part of the cybersecurity objectives and implement performance measurement techniques such as balanced scorecards to measure performance and correct deviations. Choobineh et al. (2007, p. 959) indicate the need for adequate information security and risk management in achieving organisational goals of fraud mitigation. Information security is prone to three challenges: the management of information security, conceptualisation, and development and management of information security (Choobineh et al. 2007, p. 959). Usher (2006) state that a well-conceptualised and developed information security approach should address five major areas - confidentiality, integrity, network security, application security and host security.

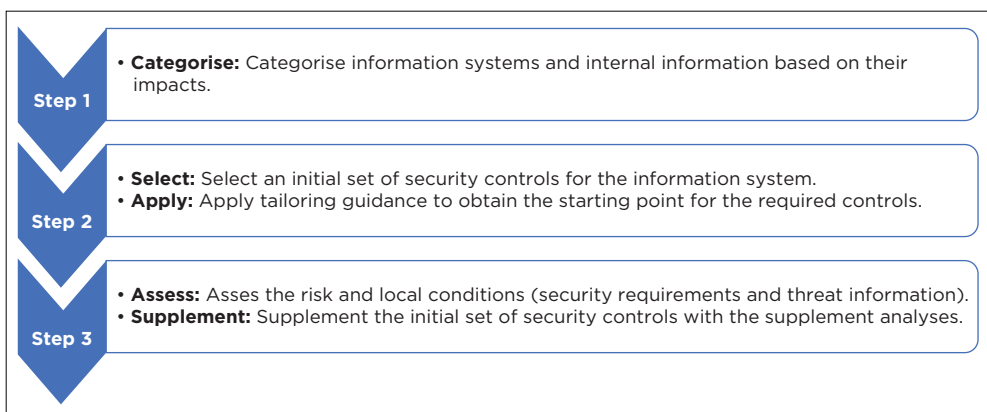
Holappa et al. (2005, p. 18) stress the need for confidentiality to ensure that the organisational information is only accessible to authorised persons, without any intrusion (Holappa et al. 2005, p. 18). The loss of confidentiality may lead to data or information breaches or violation of personal or organisational information. This may lead to a loss of trust and integrity in the organisation by the stakeholders and the public. It can also lead to loss of customers and costly legal implications. On the other hand, loss of data integrity can jeopardise customer relationships (Mohd et al. 2010, p. 270).

Besides, it can affect the outcome of fraud investigation and, ultimately, the decision-making processes.

Information security management is a necessary factor in reducing cyberfraud occurrences. To effectively combat cyberfraud, an organisation needs a holistic appraisal of its IT-based services, the level of information security risk, the effectiveness of information security on customer service and the effectiveness of information security in combatting cyberfraud. This may inform the need for a redesign and management of the information security architecture of the organisation.

For instance, the proposals of Dzomira (2017, p. 150) and Van Niekerk (2017, p. 127) emphasise the need to strengthen information security and increase the sensitisation of users of digital platforms regarding the nature of cyberfraud perpetrated by cybercriminals in South Africa. Obeng-Adjei (2017, p. 76) indicates that South African banks must implement stringent security controls across their networks and other supporting infrastructure, such as databases and servers, to protect customers' information. The study also recommends implementing and enforcing access controls to tighten information security. Similarly, Ko and Dorantes (2006, p. 22) indicate that security breaches harm organisational profitability. Hence, information security could minimise the negative effect of cyberfraud on organisational performance as banks with a high level of information security will be able to checkmate the occurrences of cyberfraud (Finau, Samuwai & Prasad 2013, pp. 15–16; Malik & Islam 2019, p. 50).

The 'Federal Information Security Management Framework Recommended by the National Institute of Standards and Technology' provided an information management framework (Bhaskar & Kapoor 2013). It comprises some activities that any corporate organisation can use as a guideline to achieve effective security management, as depicted in Figure 11.1.



Source: Adapted from Bhaskar and Kapoor (2013).

FIGURE 11.1: Information security management framework recommended by NIST.

According to Bhaskar and Kapoor (2013), there are various IT security factors that an organisation must take into consideration. These include security policies and procedures, security organisational structure, IT security processes, business continuity strategy processes, IT security governance planning processes and rules and regulations. The security policies and procedures are central to any organisation's security strategy. To implement an organisation's IT security management, the following steps need to be considered (Bhaskar & Kapoor 2013):

1. Allocate and authorise security roles and responsibilities to the security personnel.
2. Set rules for the users and security stakeholders.
3. Set rules for business continuity.

It is vital that the security policy be taken up by the organisational personnel with the support of the top management. The following should be reviewed to ensure alignment with the organisation's culture, strategic objectives and resources to mitigate cyberfraud:

- Management should protect customers and the organisation's confidential information.
- Real-time alert system to inform customers and the organisation's security personnel about intrusion or cyberattacks.
- Computerising of human responsibilities that are prone to errors or deviations from protocols that may subsequently promote cyberattack or increase cyber risk.
- Human capacity development (i.e. training of employees on cyberfraud risk awareness).
- Assessing information inventory and implementation of strategies to protect it.
- Implementing strategies and policies to curb data breaches.
- Implementing the organisation's cybersecurity programs that are consistent with the regulatory standards.
- Reviewing internal control measures to promote effectiveness.
- Developing and implementing risk management plans, including incidence response and recovery plans.

The internal control objectives may include the following:

- Improvement of the organisation's work and ethical values.
- Protection of customers' and organisational information.
- Implementation of risk management plans.
- Activities control - these include the control of all operational processes and policies, such as access control and staff rotation, to foster safe and effective operations.

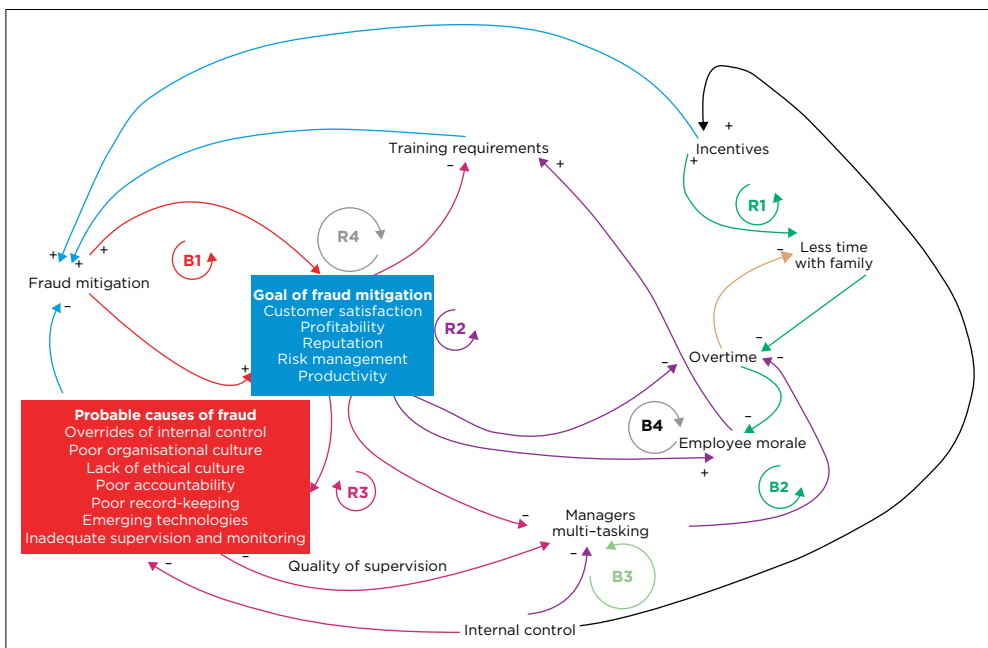
- Information and communication control ensure a logical flow of information across all departments and provide balanced reporting following cyberfraud occurrences.

Methodology: Systems thinking

This research employed a systems-thinking approach as a diagnostic tool to examine the challenges of internal and cyberfraud and provide sustainable measures to mitigate them. To tackle it, the causal loop diagram was employed to gain insight into the causes and effects of internal and cyberfraud.

Figure 11.2 presents the causal loop diagram for fraud mitigation to visualise internal and cyberfraud causes and effects.

A causal loop diagram consists of four essential elements: the variables, the arrows that connect the variables, the signs on the arrows and the direction of the loop (which indicates the nature of behaviour the system will exhibit). Either of the arrows on the causal loop diagram is labelled using a 'plus' or 'minus' sign. The 'plus' symbol denotes that the first variable causes a positive change over the second variable. In other words, a change in one variable causes the other variable to change in the same direction).



Source: Authors' own work.

FIGURE 11.2: Causal loop diagram for internal and cyberfraud.

On the other hand, the 'minus' sign indicates that the identified variable causes a negative change over the other variable.

The probable causes of internal and cyberfraud are identified from the literature as overriding internal controls, poor organisational culture, lack of ethical culture, poor accountability, poor record keeping and inadequate monitoring and supervision. The probable causes of internal and cyberfraud are linked to the organisation's goals of fraud mitigation. These are customer satisfaction, organisational profitability, reputation, risk management and productivity.

The need for training increases in the quest to achieve the goals of internal and cyberfraud mitigation. This is due to the perception that lack of employee training and human capital development may be responsible for some of the probable causes of internal and cyberfraud perpetration, such as lack of ethical culture, poor accountability, poor record keeping and emerging technologies. Employees may be made to work overtime to meet the organisation's productivity goals. This might imply that the employees might spend less time with their families or less time for other activities outside the workplace. Thus, incentives are needed to boost the psychology of the employees if the goals of fraud mitigation are to be achieved. Where incentives are lacking, employees and managers may be forced to multitask to tidy up other work not done or properly done by the employees. This may cause a dip in productivity and provide a loophole for fraud perpetration. The intervention provided by the managers can also put pressure on them. Once the training requirement is not regulated, employees may spend less time on training and work. When the manager multitasks with frequent intervention, the quality of supervision may also decrease, thus creating room for fraud perpetration. As shown in Figure 11.2, the arrows are linked together to form a loop. Each loop has a reinforcement denoted as (R1, R2, R3 and R4) or a balancing denoted as (B1, B2, B3 and B4).

In this case, the reinforcement and balancing denoted the following:

- **R1:** Employees must be motivated by incentives as part of the internal control strategies to mitigate fraud.
- **R2:** The organisation's goal of fraud mitigation should be reinforced to minimise incidences of fraud perpetration.
- **R3:** The quality of supervision, auditing, evaluation and monitoring should also be reinforced. Other experts, such as forensic accountants, can be engaged to detect loopholes that could lead to fraud perpetration.
- **R4:** Training requirements and human capacity developments should also be reinforced. This will enable employees to be kept abreast of emerging technologies and to deploy them effectively to combat fraud.
- **B1:** There is a need to achieve a balance among the organisation's goal of fraud mitigation so that an organisation will not pursue one at the detriment of others.

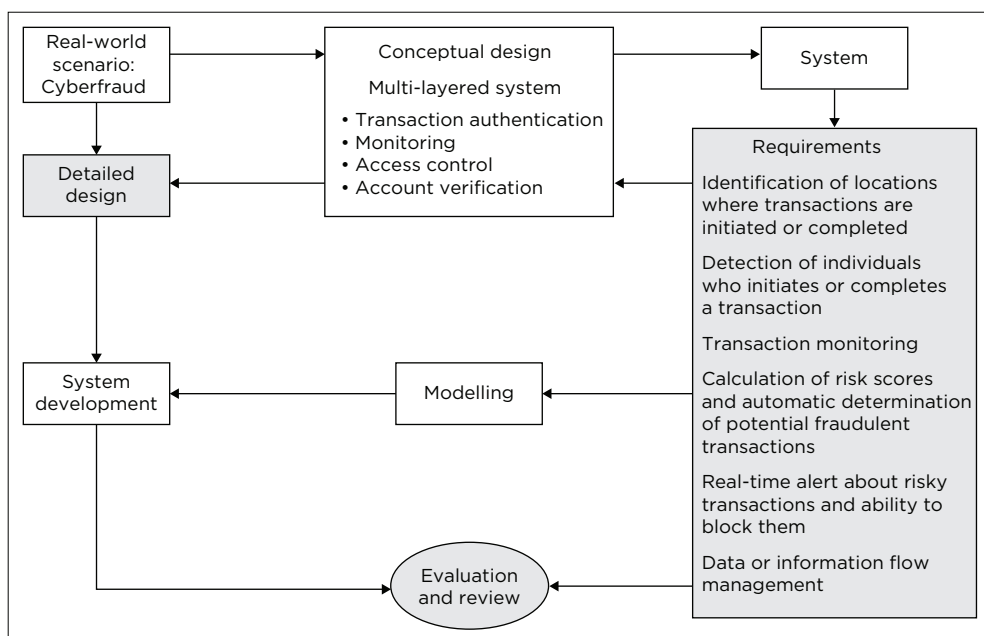
- **B2:** The time spent by the managers for intervention and overtime must be balanced so as not to jeopardise other activities of the managers to avoid loss of productivity and the creation of loopholes for fraud perpetration.
- **B3:** There is a need to ensure balance in the time the managers use in multitasking and invention in other activities of the employees. This ensures that other managers' responsibilities, such as internal controls, are not jeopardised.
- **B4:** There is also a need to match the employee incentives provided to boost their morale with their level of productivity. This will ensure that the employee is neither under- nor over-rewarded.

Information and cybersecurity framework development

Important entries in financial institutions are identified as customers' information and banking details, reimbursement, invoices or transactions related activities, journal entries and financial or accounting records.

This is followed by the identification of the method for measuring the activities. This leads to the design of an information security framework based on the defined measurement.

The information security framework is designed as a multilayered system comprising transaction authentication and monitoring, access control and account verification (Figure 11.3).



Source: Authors' own work.

FIGURE 11.3: Conceptual information security framework for internal and cyberfraud mitigation.

The functional requirements of the information security framework are:

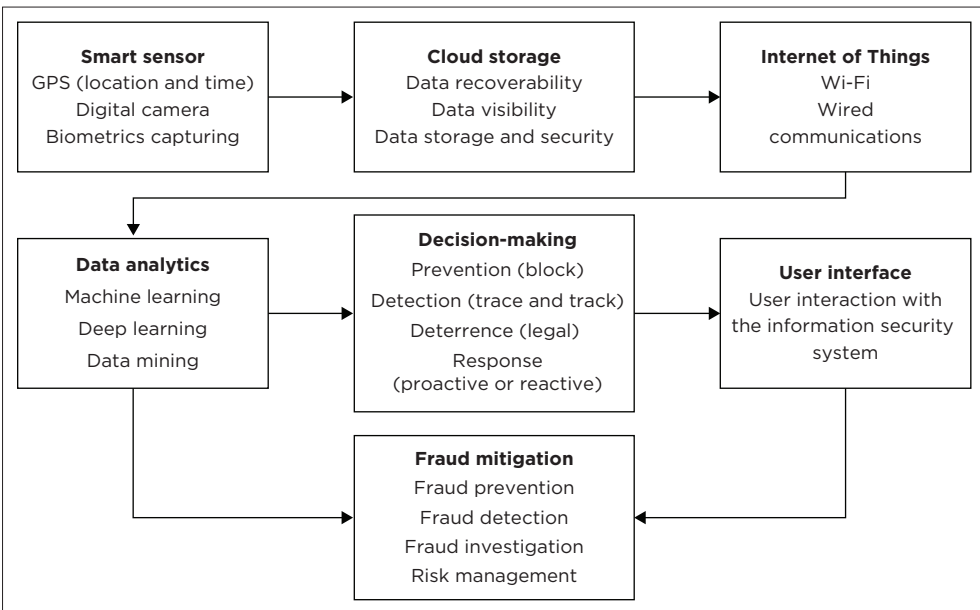
- identification of locations where transactions are initiated or completed
- detection of individuals who start or complete a transaction
- transaction monitoring
- calculation of risk scores and automatically determine potential fraudulent transactions
- real-time alert about risky transactions and the ability to block them
- data or information flow management.

■ Systems' component

The components of the designed system are displayed in Figure 11.4.

■ Sensor

A sensor is one of the significant components of the integrated information security system. Sensors such as the global positioning system (GPS) will be enabled to capture the location of the individual initiating a transaction once the 'location' icon on the mobile or digital app is activated. An individual cannot access the account or complete the transaction without triggering the 'location' on the mobile or digital app. For internal fraud or



Source: Authors' own work.

FIGURE 11.4: Components of the designed information security system for internal and cyberfraud mitigation.

fraud within the vicinity of the bank or at the ATM environment, a digital camera installed will aid in capturing the individual making transactions, including the behaviour and movements. The sensors will help gather the necessary information to track the perpetrator's identity and location. Upon activating the sensor terminal by the central controller (in this case, the Arduino microcontroller), the sensors are actuated for data collection. The data collected may be transmitted through electrical signals or impulses, which embedded software algorithms can interpret.

■ Connectivity

A connection is established to send the acquired data to a server, such as cloud storage or other safe storage or repositories. There is a need to establish connectivity to the server so that the acquired data can be transmitted to the database and other terminals and managed effectively. The data are stored in a cloud and can be recovered when needed. All the information captured can be exported to the data analytics software for analysis. The data are analysed for anomaly detection, pattern recognition, double entries, and unusual or duplicate transactions. Nonstandard (Akinbowale, Mashigo & Zerihun 2023d):

[O]r suspicious journal entries, activities in dormant or controversial accounts, consistent errors, alterations, or discrepancies in financial or accounting records, incomplete documentations of transactions, false documentations or forgery, unauthorised transactions. (p. 4)

Furthermore, the organisation's data are stored on a centrally hosted server. A remote connection must be established between each organisation's system and the server via the Internet. This will enable the capturing of other important information that characterises banking operations, such as reimbursement, invoices or transaction-related activities, journal entries, financial or accounting records, customers' information and banking details.

■ Big data analytics

Internet of Things devices can enable the sharing of the acquired information with other authorised and compatible devices, such as big data analytic platforms, to analyse the data obtained in real time.

■ User interface

This will enable the user to interface and relate with the functions of the developed information security system. The control room can be linked to the users' interface, where the outcome of the data analytics can be monitored. This will assist the bank managers and others saddled with fraud detection, investigation and mitigation responsibilities, such as

forensic accountants, to monitor ongoing activities in real time. It will also promote a real-time response to suspected fraud cases.

■ Procedure for information security system implementation

The following procedures are proposed as part of the digital information security system for fraud and cyberattack mitigation in the banking sector.

■ Use of a checkpoint firewall with good processing capability

This type of security firewall runs on dedicated hardware. It can secure an organisation's information or data against intrusion and malware attacks. The checkpoint firewall secures the organisation's data by permitting only trusted programs to access the organisation's network while preventing untrusted or potentially harmful programs. This software has two packages: state inspection and application layer filtering. A state is established when communication (information and response) between two or more connected devices. Hence, the state can be monitored by communication between these connected devices. For the application layer filtering, the checkpoint firewall scans all the information or data that passes through the organisation's network or system. The information that can cause an organisational system vulnerability to attack is denied, while others considered safe will be allowed to pass. The websites that are deemed harmful to banking activities can be blocked. By doing this, the employee will not be able to gain access to these websites while working on the systems. The checkpoint firewall can monitor network traffic on an application-by-application basis. It also has a tracked capability to trail all sessions and monitor online or offline information. Depending on the application, checkpoint firewalls can be used in the firewalls that will be discussed in the following sections.

■ Network firewall

This security device guards against intrusion into the organisation's network via the Internet. With this, users can safely connect remotely with smart devices and work anytime, even outside the organisation's vicinity. This type of firewall secures the local-area network from intrusion and attacks. It can distinguish between a secure and an unsecured zone and establish communications between them. This will guard the systems with a public IP address from vulnerability to attack from external networks.

Sometimes, cyberattackers attack with viruses or other forms of malware. The network firewall can also enable data security against attackers by blocking malware over public networks with Internet protocol security (IPSec) and virtual private networks (VPNs). The IPSec is a group of networking protocols that can offer the security of encryption connection over publicly shared networks. This minimises the risk of data breaches by the organisation's employees or external attackers. This will enable customers to safely access the Internet with the provision of secured services.

■ Endpoint security firewall

This type of firewall can guide against the entrance of viruses, spyware and keyloggers from attacking the organisation's system when an infected file is opened. This is a form of device control that can prevent introducing viruses into the organisation's system through corrupt flash drives, USBs or other removable devices. The checkpoint firewall has strict rules that can block these devices from accessing the network.

■ Network access control

The network access control can provide another security layer by preventing connections not authorised by the firewall rules.

The checkpoint firewall has three significant capabilities, namely the control capability, security capability and management capability.

The control capability of the checkpoint firewall can assist organisations in controlling traffic monitor or managing access to the organisation's network. On the other hand, the security capability can inspect the traffic communications and block any potentially harmful networks detected or intrusion into the organisational system. The management capability can ensure the management of firewalls remotely using a central management tool. This approach will be practical for banks with many branches across different locations as it will promote ease of administration. The implementation of the checkpoint firewall can be achieved with two-factor authentication. For instance, the organisational employee may provide a strong password and token to access the network.

The firewall used should be able to offer the following services:

- identify users (user's identity awareness)
- offer control application to detect and block a threat
- provide intrusion prevention capability
- provide access control
- inspect the nature of traffic entering or leaving the system
- offer web filtering to block access to certain domains that are risky
- provide antivirus functions.

The checkpoint firewall can have internal, external and firewall connection ports to enable Internet banking. The following should be ensured to safeguard the organisational system and network:

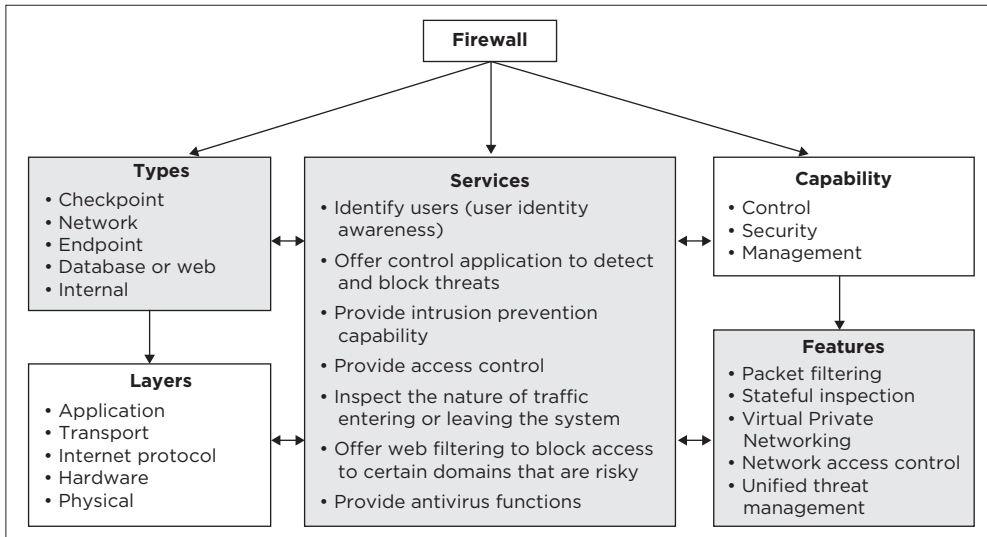
- only the port used for Internet communications should be open
- web applications should be blocked
- enabling the IPSec software to protect the system from intrusion
- periodically update the installed firewall
- database and web application server firewall to secure the organisational database with organisational and client information
- using a separate host such as data manipulation language (DML) to host a web server accessed by the customers (this will prevent clients from accessing the organisation's sensitive information).

■ Acquisition of a database or web server firewall

Database firewalls are a form of application firewalls with the capability to monitor traffic specific to a database to detect and protect the sensitive data stored in the database from attacks.

Information security is necessary to protect the database and the web server from attack. Data theft or leakage can affect data analytics and expose the organisation to the risk of attacks. The database or web server firewall can protect customers' and organisations' information. Banking activities nowadays are data-driven; hence, the banking sector is responsible for providing confidentiality by securing sensitive data and customers' information. Using a database or web server is a data protection strategy that can enhance data protection and security against cyberattacks and fraud such as phishing, hacking or identity theft.

The database firewall has predefined and configurable security and audit policies that can secure an organisation's database against threats based on established threat trends or patterns or past occurrences (signatures). The signatures are already captured on the firewall and will be compared with the queries received to establish potential fraud cases. The threats or queries that match the signature will be blocked from accessing the database, while others that do not match may be granted access. Thus, the database can securely detect the vulnerabilities of the protocols, organisational system and database and provide a real-time alert to the users or administrators. Some database firewalls are equipped with capabilities to detect the IP address, location, time and type of activities. When irregular movements are detected, a real-time alert can be sent to the users to block them. The database firewall can block unsolicited Internet data or other contents that can corrupt an organisation's database. It can also foster effective business operations through ease of access and data modification capability granted to the users.



Source: Authors' own work.

FIGURE 11.5: Firewall and its specifications for cybersecurity.

Figure 11.5 presents an overview of the firewall required as a cybersecurity technology, its types, service requirements, capability, layers and features:

1. **Internal firewall:** This is necessary to deal with internal attacks and inspect internal communications.
2. **Load balancer:** This is important for distributing high-traffic sites among the servers for operational or service efficiency.

■ Conclusion

This chapter aims to design information and cybersecurity frameworks for internal and cyberfraud mitigation in financial institutions. This was achieved using the systems-thinking approach as a diagnostic tool to examine the internal and cyberfraud challenges and provide sustainable measures to mitigate them. The causal loop diagram was employed to gain insight into the causes and effects of internal and cyberfraud. From a causal perspective, the probable causes of internal and cyberfraud were established concerning an organisation's goal of fraud mitigation. This led to the development of information security and cybersecurity frameworks to mitigate them.

The causal loop diagram can assist organisations in understanding the relationship and interdependencies among the internal and cyberfraud variables identified. Furthermore, the information security and cybersecurity frameworks developed can aid decision-making relating to fraud mitigation

and be adjusted to suit an organisation's need to mitigate internal and cyberfraud. This chapter adds to the existing information about using the system's thinking approach to visualise the challenges of internal and cyberfraud. It also highlights the multiple and interdependent effects of managerial efforts at mitigating internal and cyberfraud.

Towards cyberfraud risk mitigation: A bow tie approach

■ Introduction

The purpose of this chapter is to develop a cyberfraud risk-mitigation approach to contain the threats of cyberfraud effectively. In this chapter, we employed the bow tie technique. The bow tie method is used to visualise potential red flags that could lead to cyberfraud, the impacts of cyberfraud occurrence, its associated risks, the consequences and the controls that financial institutions should be in place to mitigate cyberfraud. The results show that the likelihood of cyberfraud risks and the effects resulting from such risks tend to reduce when preventive and control actions are implemented. Visualising the cyberfraud risks and possible mitigation approaches can assist financial institutions in risk analysis and management. The existing literature has not sufficiently highlighted the use of the bow tie for cyberfraud mitigation. Thus, this study adds to the current knowledge of cyberfraud risk management.

Cyberfraud risk generally refers to the danger emanating from a threat to data integrity or intrusion into an organisation's system

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Towards cyberfraud risk mitigation: A bow tie approach', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 235–250. <https://doi.org/10.4102/aosis.2024.BK485.12>

through cyberspace. This may result in data theft, financial loss, disruption of operation, reputational damage to an organisation and customer dissatisfaction. Financial institutions' increasing use of IT-enabled technologies aggravates cyberfraud-related risks by increasing organisational systems' vulnerability to cyberattacks (Ali et al. 2017). Although financial institutions are developing resilience approaches to tackle cyberattacks, the dynamic nature of cyberspace coupled with the digitalisation of services by the institutions open up avenues for cyberfraud perpetration. This calls for an effective risk management approach and cybersecurity. Besides, financial institutions also need continuous improvement and appraisal of their risk management approaches and cybersecurity measures. The gradual trend towards cashless policy and the noncontact nature of online transactions are possible factors that can increase the activities of cyber fraudsters. This has given rise to many forms of cyberfraud, such as 'the use of malicious software, computer hacking and DoS attacks, phishing, data theft, spamming, card theft, online fraud, vishing, spying is becoming more common' (Akinbowale, Klingelhöfer & Zerihun 2023b, 2023c; Ali et al. 2017; Rao et al. 2019; Tiwari, Bhalla & Rawat 2016; UN 2013). Dzomira (2015a, 2015b) states that with the inventions of cyber fraudsters, online banking security measures are relatively inadequate to curb cyberfraud. Cyber fraudsters usually invent new ways to perpetrate fraud and exploit loopholes to beat security measures (PwC 2011). The emergence of new ways to commit cyberfraud comes with new risks that financial institutions need to contain. Some fraudsters may attack the organisation's network or servers to increase their chances of accessing sensitive information, such as system passwords. Sometimes, the attack on the network can cause disruption of communications and transactions, breach of protocols and overrides of controls with the tendency to damage the organisation's IT infrastructure, such as the website or to corrupt the database. Besides launching network attacks, hackers devise means to intrude into the organisation's system to access customers' information to commit fraud or completely hijack the account (EMC 2013). With access to customers' sensitive information, a fraudster may attempt to hijack the account. For instance, in 2012, a sum of US\$455m was lost by financial institutions globally because of cases of account hijacking by fraudsters (EMC 2013). In 2018, UK Finance (2018, p. 5) estimated the global annual loss because of cyberfraud-related activities to be over US\$450bn.

In some cases, fraudsters commit crimes using false identities (Jegade 2014, p. 13; KPMG 2011, p. 4). Balan et al. (2017, pp. 64-65) identified some probable reasons for customers' vulnerability to cyberfraud. These include a lack of information flow, poor sensitisation on cyberfraud,

threat actors' activities, mitigation measures, lack of online monitoring systems and poor real-time responses to cyberfraud incidences. These explain why financial institutions must adequately reinforce their security and intelligent systems to make them more effective. The vulnerability of cyberspace because of the lack of strict regulation for entry and exit can promote cyberfraud-related occurrences (Uma & Padmavathi 2013, p. 390).

Protecting IoT devices from cyberattacks necessitates carefully considering the associated risk factors. This is because cyberattacks also target organisational IoT devices. Without adequate security measures deployed by financial institutions, cyberspace could be a target for cyberfraud, such as identity theft, malware, data theft, cash theft, unauthorised acquisition of sensitive information, impersonation, network disruption and generation of fake links.

Dzomira (2014, p. 24) suggested the need to make the IT infrastructure of financial institutions more resilient to cyberattacks through real-time monitoring and other emerging technologies. In addition, the KPMG (2019, p. 6) global banking fraud survey indicated a low recovery rate for losses incurred via cyberfraud. The study considered cyberfraud perpetrated via scams, credit cards, cyber/online fraud, identity theft, impersonation and data theft. The dynamics of cyberspace increase business risks; hence, financial institutions must understand the drivers of cyberfraud to come up with resilience and sustainable approaches to contain it. Prabowo (2011) categorises the measures to contain cyberfraud into five distinct aspects: development and implementation of fraud prevention policy, awareness and sensitisation about fraud, technology-based protection, identity management and legal deterrence. Furthermore, Kritzinger and Von Solms (2012) propose a cybersecurity framework encompassing policy formulation and implementation, procedure, awareness, research and deploying technologically based security measures. Aldasoro et al. (2022) identify the drivers of cyber risks as an organisation's size, connected events, malware incidences, security incidences, data breaches, phishing or skimming, violation of privacy and others. Identifying these drives is critical in achieving a sustainable fight against cyber risk. Despite the prevalence of cyberfraud-related incidences and risk, the information about the potential red flags, impacts of cyberfraud, its associated risks, the consequences and the controls have not been sufficiently highlighted by the existing literature. Thus, this study aims to develop a cyberfraud risk-mitigation approach to effectively contain the threats of cyberfraud via the use of the bow tie technique. Visualising the cyberfraud risks and possible mitigation approaches can assist financial institutions in risk analysis and management. In addition, this study adds to the existing knowledge on cyberfraud risk management.

■ Risk management

A risk is the likelihood of an event occurring. According to the ISO (2018), it is the combination of probability and consequences of an event. The likelihood of an event is a function of the threat level, vulnerability and the consequences according to Equation (12.1).

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequences}) \quad [\text{Eqn 12.1}]$$

The risk factor can be obtained by analysing the event's threats, vulnerability and impact (consequence).

Risk management, therefore, refers to identifying, controlling and eliminating the likelihood of an event that can adversely affect an individual or organisation. In the context of cyberfraud, it is the identification, management, reduction or elimination of the likelihood of any event that can undermine an organisation's information system and cybersecurity. To manage risk, there is a need for risk assessment. This entails risk analysis, evaluation, monitoring and control, communication and consultation. To effectively manage cyberfraud risk, clarifications of the potential threats to the organisation's information system, computer and networks must be identified. To achieve this, there is a need to determine if there is an existing risk and ascertain the scope of the identified risk on the information system's confidentiality, integrity and availability. Furthermore, risk management is incomplete without consideration of the risk assessment process.

This involves a detailed understanding of the potential or identified risk and the consequences of its adverse effect on the organisation's information security. Thus, necessary control measures that are suitable to reduce or eliminate the risky situation must be put in place. A control action, whether in the form of a detective, deterrent, corrective or preventive control, can minimise the risk by reducing the likelihood of occurrence of an event or the impact of occurrence.

Financial institutions are highly vulnerable to cyberfraud risk because of using IT-enabled devices and cyberspace for business operations; hence, effective risk assessment and management are crucial in mitigating cyberfraud-related risks. Hopkin (2010, p. 5) and Mohammed and Knapkova (2016) state that an organisation's lack of risk assessment and management plan can affect the smooth running of operations. Risk management encompasses three major phases: risk assessment, analysis, control and evaluation (Stoneburner, Goguen & Feringa 2002). Organisations must develop and implement risk management processes

as part of their responsibilities. Stoneburner et al. (2002) further stress the need to develop strategies for risk assessment, mitigation and review of actions taken. Risk assessment's first phase of risk management involves evaluating all potential risks and their impacts on an organisation (Stoneburner et al. 2002). The knowledge of the potential risk has implications for an organisation and will result in the development of mitigation plans. In the context of cyberfraud, risk assessment involves identifying all the threats to the organisation's system and data confidentiality, integrity and availability. It encompasses all the threats to the organisation's systems, applications, network, data and devices. The components of the cyberfraud risk assessment plan will include:

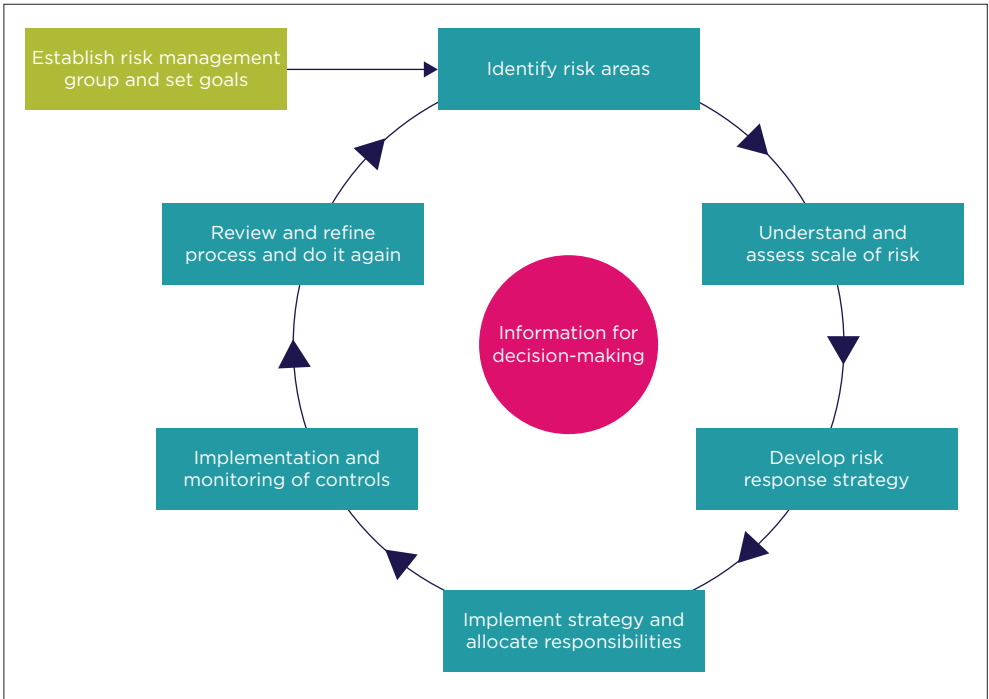
- Identify the organisation's essential and vulnerable data creation, storage and transmission assets.
- Create a risk profile for each asset.
- Assess cybersecurity risks for all the identified assets and their interconnectivity.
- Prioritise the critical assets to address in any event of cyber breach.
- Develop mitigation plans and controls for all the identified risks.
- Develop prevention plans to minimise the chances of cyberfraud occurrences and system vulnerability.
- Create a system of risk monitoring and evaluation.
- Review of the risk assessment procedures holistically.

During the risk analysis phase, each previously identified risk will be evaluated regarding the features and impact on the organisational or other stakeholders. Furthermore, the identification of *'what'* and *'who'* could be affected by the occurrence of cyberfraud will be ascertained. For instance, the organisational system, database, customers' sensitive information, IT infrastructure and network could be affected. The organisational, customers, employees and other stakeholders could also be involved. Analysing the probable causes and the motivations for the perpetrators is an integral part of the risk analysis phase. The control and evaluation phase develops strategies to eliminate the possibility of risk occurrence or to minimise the impact after an event (Stoneburner et al. 2002). During risk analysis, a score is usually assigned to the identified risk quantitatively or qualitatively. These scores will assist organisations in prioritising the risks to address first and in determining the best ways to manage them. This risk analysis process requires the quantification of uncertainties. The estimation of their potential impacts helps to develop a risk analysis framework. With the risk analysis framework, action plans can be effectively implemented to prevent or mitigate risks.

The control actions can be preventive, detective, corrective or directive control measures (Hopkin 2010). Hasham, Joshi and Mikkelsen (2019) identify the essential steps in developing preventive controls against cyberfraud. This includes the identification and authentication of customers and transaction monitoring, while the detective and corrective control involves anomaly detection and response to cyberfraud incidences (Hasham et al. 2019). Fraud control presents measures to ensure no deviation from everyday activities and correct suspected anomalies before they escalate. The phase is necessary to prevent losses and can be preventive and detective (Hopkin 2010). Preventive controls are strategies to avoid occurrences of fraud, while detective control is to identify the event of fraud. It is crucial to identify and deal with all potential sources of risks before they culminate into fraud by implementing preventive control measures.

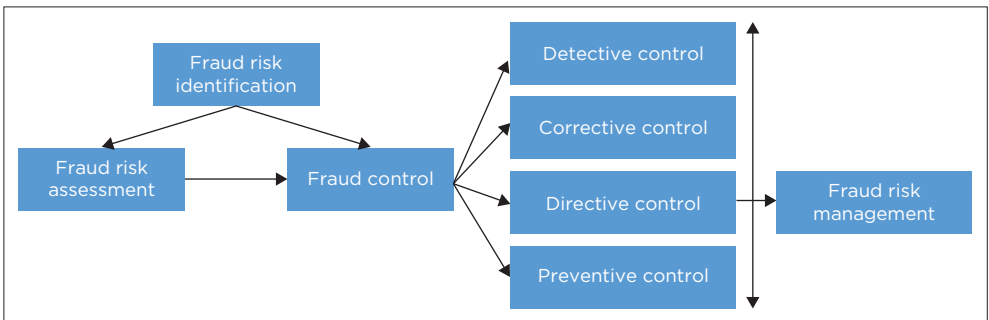
Financial institutions are confronted with various risks, but developing and implementing an effective risk management plan is essential to the survival and performance of the institutions. In the risk taxonomy developed by Leo, Sharma and Maddulety (2019), cyberfraud risk is classified under operational risk. This is because risk could result from the weakness of the internal system or through external channels with the capacity to affect the organisation's operation. Developing cyberfraud risk management plans will give financial institutions an overview of the potential risks they are liable to and their scope. This will aid the decision-making processes relating to risk mitigation. Therefore, risk management processes and controls are plans for protecting an organisation and the stakeholders from the occurrence or impact of fraud risk. Thus, risk management involves systematic risk identification, assessment, analysis, control and evaluation (Hopkin 2010; Stoneburner et al. 2002). Firstly, assess the probability and criticality of the potential risks. Secondly, develop and implement controls and risk response plans for risk prevention and mitigation. The fact that the business environment is dynamic necessitates the need for a periodic review of the risk assessment plans. At this stage, the effectiveness of each strategy will be evaluated, and new risks with their control measures will be included. Figure 12.1 presents the risk management cycle encompassing systematic risk-mitigation procedures. These include establishing risk goals, identifying potential risk areas, assessing the scope of risk, developing a risk response strategy, implementing a risk mitigating strategy, allocating responsibilities, implementing and monitoring control plans, process review and decision-making.

Figure 12.2 presents the link between fraud control, risk assessment, risk management and investigation.



Source: CIMA (2008).

FIGURE 12.1: Risk management cycle.



Source: Authors' own work.

FIGURE 12.2: Link between fraud control, risk assessment, risk management and investigation.

■ Methodology: Bow tie technique

In this chapter we employed the bow tie technique. The bow tie method is used to visualise potential red flags that could lead to cyberfraud, the impacts of cyberfraud occurrence, its associated risks, the consequences and the controls that financial institutions should be in place to mitigate cyberfraud. The bow tie technique is employed to visualise and assess cyberfraud risks for easy comprehension and to allow for the implementation

of risk management plans. The method provides an overview of the different probable scenarios and the controls put in place to mitigate the systems. This technique aids the understanding of how cyberfraud risks and its consequences can be effectively controlled.

As shown in Figure 12.3, at the centre of the bow tie framework is the description of the challenge to be mitigated (cyberfraud). At the same time, the consequences and the preventive measures are captured on the left side of the framework. The right side of the framework grasped the implications of taking preventive actions and the possible reactive steps that can be taken in any event of cyberfraud.

From the literature review, possible causes of cyberfraud risks have been identified as lack of ethical culture, poor management and internal controls, the use of ICT devices and other emerging technologies, cyberinsecurity, lack of awareness and public sensitisation as well as the vulnerability of personal or organisational systems. Many financial institutions lack ethical culture and, as a result, expose customers' data and sensitive information to the public in breach of their data protection and privacy. Cyber fraudsters may use the information acquired to perpetrate fraud. Thus, one of the proactive measures to mitigate this risk for financial institutions is to develop human capacity in personnel training on data protection and privacy. In addition, many data and privacy protection Acts are enacted by various countries, and financial institutions must ensure that these Acts are implemented to prevent a breach in data and privacy of their customers. For instance, the South African government enacted the *Protection of Personal Information Act 4 of 2013* (POPIA) to ensure data privacy. Furthermore, the South African government passed a cyber-defence framework called the National Cyber Security Policy Framework (NCPF), enforced by the Ministry of State Security, in 2015 (Sutherland 2017).

Cyberfraud could also be because of weak management and internal controls. Langfield-Smith (1997) defines MCSs as the process by which managers ensure that an organisation's resources are effectively used to achieve targeted objectives. Existing studies indicate that a sound MCS can enhance an organisation's performance (Carenys 2012; Mohammed & Knapkova 2016; Slavoljub, Srdjan & Predrag 2015). Concerning fraud risk management, a good MCS strategy, such as access control, use of updated software, periodic system updates, effective monitoring of cyber-related activities, and use of a real-time alert system for potential cyberfraud detection can be a proactive approach to minimising cyberfraud risk.

Another major cause of cyberfraud risk is the use of emerging technologies. However, using emerging technologies by financial institutions has made their operations and service more efficient but with increased cyberfraud risk (Ali et al. 2017; Dzomira 2014; Kshetri 2019). The use of anti-fraud technologies for the detection and blocking of suspected cyberfraud cases

Causes	Prevention actions		Risk event description	Loss reduction actions		Consequences	
	Treatment	Treatment		Treatment	Treatment		
Lack of ethical culture; data breaches	Training	Protection of Personal Information Act 4 of 2013	Cyberfraud: Unauthorised access into personal or organisational information or accounts via cyberspace to perpetrate fraud	Customer support/relationship	Real-time alert to cyberfraud	Customer dissatisfaction	
Poor management and internal control systems	Access control and use of updated software	Supervision, real-time detection and prevention of attack		Cyber vault; implement a cyber incidence response plan	Data/information recreation or recovery, use safe backups	Infrastructure damage/ disruption of operations	
Emerging technologies	Use of digital anti-fraud technologies	Artificial intelligence/ data analytics		Deploy more resources	Hire experts: forensic	Loss of productivity	
Cyberinsecurity	Collaboration and cyber intelligence	Network access control		Service/security improvement	Litigation and branding	Loss of reputation/ good will	
Lack of awareness	Public sensitisation	Training		Fraud investigation	Block cyber attacks in real time	Financial loss	
System vulnerability	System security	Firewall		Likelihood after prevention actions:	4	Consequence after loss reduction actions:	5
Likelihood, if nothing is done, to prevent risk:	4			Treatment effectiveness (qualitative)	Needs improvement		
Consequences if nothing done to reduce losses:	5						

Source: Authors' own work.

FIGURE 12.3: Bow tie framework for cyberfraud risk management.

can be helpful in minimising cyberfraud risk. Data analytics, artificial intelligence and data-mining techniques can also be employed as a predictive and preventive approach. For cyber insecurity identified here as one of the major drivers of cyberfraud risk, the organisation implements network access control, collaborates with the relevant stakeholders on cybersecurity and employs cyber intelligence to gather reports on cyberfraud and their perpetrators. Furthermore, lack of awareness and public sensitisation is another major cause of cyberfraud, and this can be tackled by raising the awareness levels of customers and the public on cyberfraud, their perpetrators and the preventive measures that customers can use to prevent its occurrence. In addition, personal and organisational system vulnerability to cyberattacks can be proactively handled via firewalls or other system protection software.

The consequences of cyberfraud identified in Figure 12.3 are customers' dissatisfaction, infrastructural damage, service or operation disruption, loss of productivity, loss of reputation and goodwill, as well as financial loss (Goel & Shawky 2009; Kraemer-Mbula, Tang & Rush 2013; Lagazio, Sherif & Cushman 2014; Malik & Islam 2019; Martin & Rice 2011; Saini, Rao & Panda 2012). Customers' dissatisfaction can be addressed via effective customer support, relationships and real-time alerts to cyberfraud incidents. Financial institutions must develop and implement a cyber incidence response plan to tackle infrastructural damage service or operational disruption, highlighting the pathway to recovery from cyberattacks. More resources (time, human, material and financial) must be deployed to address the loss of productivity. Furthermore, an organisation can promote its goodwill and reputation after a cyberattack through service and security improvement, recovery of funds stolen via cyberfraud, uncovering the perpetrators and bringing them to book. In addition, financial losses may be minimised by blocking cyberfraud incidences in real time, thorough fraud investigation and implementing a cyber incidence response plan.

It is necessary to ascertain if the control:

- appears on multiple threat lines or multiple consequence lines
- is preventive
- is on a high probability threat line
- is on a high-severity consequence line
- is the only control on a threat line or consequence line
- is being audited, monitored and reported.

Critical safety activities are added for each control and mitigation step. This includes the activities an organisation must implement to ensure that the control or mitigation steps effectively combat cyberfraud and the personnel responsible for implementation. Each control is ranked high, medium or low in terms of its effectiveness in mitigating cyberfraud. Next to this is the specification of the control attributes and control hierarchy. It is necessary to establish the degree of automation of each control, whether or not it requires human intervention. Table 12.1 presents the cyberfraud

TABLE 12.1: Cyberfraud risk and risk scores.

Risk	Description	Business impact	Probability of occurrence	Priority
		(1, 3, 5)	(1, 3, 5)	
Social engineering	This encompasses a group of activities taken by fraudsters, aimed at deceiving people to divulge sensitive information for the purpose of theft	5	5	25
Malware	Malware is a form of attack perpetrated through the use of software that is deliberately designed to disrupt personal or organisational systems, networks or servers to leak confidential information, gain unauthorised access to information or to deprive authorised users of access to information	5	5	25
Data theft	Data theft involves the authorised access, transfer or storage of personal or organisational sensitive or financial information. This could include the acquisition of passwords, software code or algorithms and proprietary processes or technologies	5	5	25
Hacking	Unauthorised access or compromising of personal or organisational computer systems or private networks, or an attempt to take over the control of the computer network security systems for fraudulent purpose	5	3	15
Spamming and Phishing	These are acts of sending unsolicited messages in the form of electronic mails, instant messages or social media messages disguised as messages from legitimate sources but having malicious content for the purpose of obtaining sensitive information from unsuspecting recipients	3	1	3
Online theft	This usually occurs in the form of illegal cash transfers or credit card theft. The online cash transfer involves the unlawful transfer of cash from the account of an unsuspecting customer once the necessary confidential information relating to the user or such account is obtained. Online credit card fraud involves the unauthorised use of the secret PINs, debit or credit card or login credentials of an unsuspecting user for fraudulent activities.	5	3	15
Skimming	Skimming occurs when a device is unlawfully installed on ATMs, POS terminals or fuel pumps to record or capture confidential information on the cardholders' PINs. The acquired data can be used by fraudsters to create fake debit or credit cards to steal from the original owners' accounts.	1	1	1
Spying	Cyber spying, sometimes referred to as cyber espionage, occurs when fraudsters target computers or IT networks to gain access to information via the use of codes or software. The goal is to acquire sensitive information exchanged between an organisation's computers or IT networks and other websites or systems.	1	1	1
Denial-of-service	This is a deliberate disruption of service, system or network resources for the purpose of capturing information from the intended victims. For instance, the disruption of the services of a host connected to an organisation's network.	5	3	15
Cyberstalking	Cyberstalking is a broad term for a series of unlawful activities, including threats, libel, defamation and sexual harassment aimed at intimidating the target to syphon money	3	3	9

Table 12.1 continues on the next page →

TABLE 12.1 (cont.): Cyberfraud risk and risk scores.

Risk	Description	Business impact	Probability of occurrence	Priority
		(1, 3, 5)	(1, 3, 5)	
Vishing	<i>Vishing</i> involves the use of mobile phones to steal personal or organisational confidential information	3	1	3
Pharming	Involves the use of malicious code executed on the device to redirect a victim to an attacker-controlled website	3	1	3
Spoofing	The use of fake IP addresses by fraudsters with the aim of disguising or hiding locations to perpetrate fraud	1	3	3
Whaling	A whaling attack is a method used by cybercriminals to disguise themselves as top management of an organisation, with the aim of stealing money or sensitive information or gaining access to their computer systems for fraudulent purposes	1	1	1
Software supply chain attack	This is a threat that targets an organisation's software developers or suppliers to access secret codes for the purpose of fraud	3	3	9
Password attack	Unauthorised access into an organisation's files or accounts by guessing or cracking the password	3	3	9
Identity theft	Unauthorised use of another person's personal identifying information, such as the name, identification number, or credit card number, without their permission, to commit fraud or other crimes	3	3	9

Source: Authors' own work.

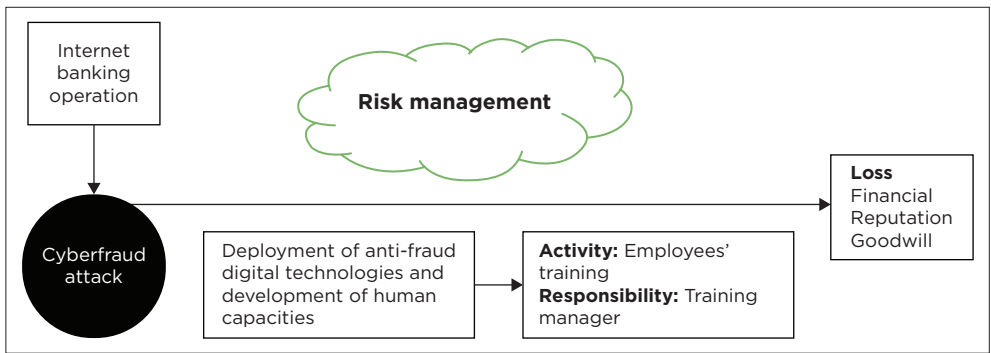
Key: ATM, automatic teller machine; POS, point-of-sale; PIN, personal identification number.

risk and the risk scores. Scores are allocated subjectively to the identified cyberfraud risk, and the corresponding risk scores are calculated. The essence is to identify the risks with top priority. This will assist managers in making decisions to mitigate its impact on business operations or probability of occurrence.

The essence of Table 12.1 is for organisations’ top management, risk managers or decision-makers to prioritise the necessary risk-mitigation approaches based on the calculated values of the risk priority.

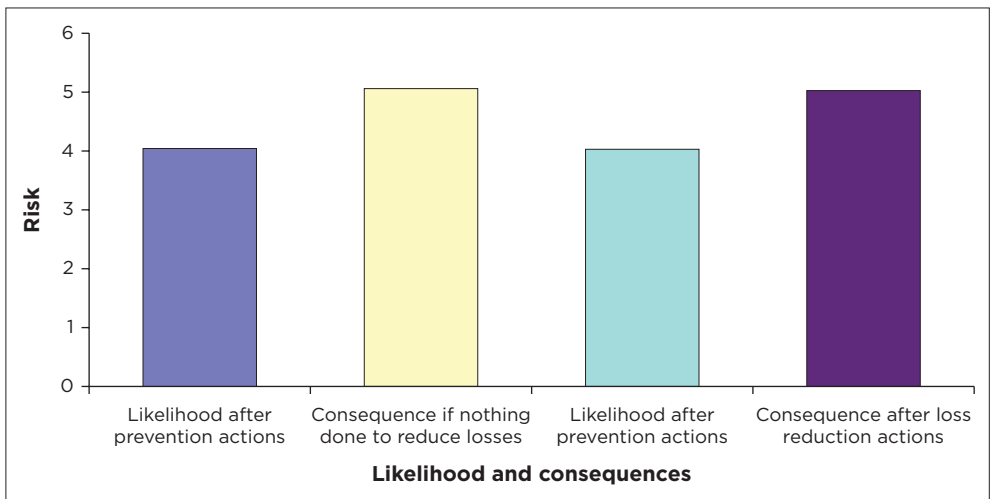
■ Results and discussion

Based on the example presented in this study, Figures 12.4 and 12.5 show the cause-effect diagram and the likelihood and consequences of



Source: Authors' own work.

FIGURE 12.4: Cause-and-effect diagram.



Source: Result generated using Bowtie XP (2022 version, Wolters Kluwer).

FIGURE 12.5: Likelihood and consequences of cyberfraud risk.

cyberfraud risk occurrence after preventive action because of a lack of preventive measures. It also indicates the probability and the consequences of not implementing the control actions after implementation. Figure 12.4 shows that the likelihood of cyberfraud risks and the effects resulting from such risks tend to reduce when preventive and control measures are implemented. Conversely, the example demonstrated that the nonimplementation of prevention or control actions can result in severe losses and other consequences.

To effectively implement the bow tie technique, the personnel or team responsible for the control actions will be included in the loop and held accountable for the control actions. This makes the process of cyberfraud more transparent and effective because of proper information flow as each personnel or team knows the tasks allocated to them and the consequences of nonexecution or poor execution of the functions. Each activity in the bow tie framework is linked to the control that identifies the actions to mitigate the associated risks. The display of this information enables proper comprehension and visualisation of the risks and the management concepts. Furthermore, analysing the control's effectiveness will provide insight into its robustness.

The application of the bow tie technique demonstrated in this study assists in visualising the cyberfraud risks and how they can be dealt with. The method communicates essential information about the threats, risks and actions through a cause-effect logic, which is necessary for making an informed decision on risk management. The technique also provides the possible outcomes for an organisation's proactive or reactive risk management.

Table 12.2 presents the risk matrix for this example to assist the organisation in determining if the risks have been effectively managed. The risk matrix allows for customisation to organisational standards based on their peculiarities. The matrix shows the inherent and residual risk assessments that call for improvement by implementing risk management measures. As shown in Table 12.2, an organisation may highlight the primary risk control measures and ensure that the risk communication is integrated into the organisation's control structure.

TABLE 12.2: Risk matrix.

Score		Survey opinions					Risk category
Description	A	B	C	D	E		
	Never heard of cyberfraud in the banking industry	Cyberfraud incidence has occurred in the banking industry	Cyberfraud incidence has occurred in our organisation	Cyberfraud incidence has occurred several times in our organisation per year	Cyberfraud incidence has occurred several times in our organisation per month		
0 No loss						No impact	
1 Light loss						Incorporate risk reduction measures	
2 Minor loss						Incorporate risk reduction measures	
3 Medium loss						Manage risk and seek continuous improvement	
4 Major loss						High-impact, undesirable risk	

Source: Result generated from the Bow Tie Software.

■ Conclusion

In this chapter our objective was to develop a cyberfraud risk-mitigation approach to contain the threats of cyberfraud effectively. This was achieved with the aid of the bow tie technique. The bow tie method was used to visualise potential red flags that could lead to cyberfraud, the impacts of cyberfraud occurrence, its associated risks, the consequences and the controls financial institutions should have to mitigate cyberfraud. The results show that the likelihood of cyberfraud risks and the effects resulting from such risks tend to reduce when preventive and control actions are implemented. Visualising the cyberfraud risks and possible mitigation approaches can assist financial institutions in risk analysis and management.

Cyberfraud occurrences: Africa's experience

■ Introduction

The African continent is unique because of the increasing population and increasing rate in the number of Internet users. This chapter presents Africa's trends and statistics in the rate of cyberfraud. The chapter also probes some African countries' efforts in tackling cyberfraud and the success rate. The findings indicate that the impact of cyberfraud is far-reaching, especially in Africa. Many perceive the African continent as a haven for perpetrating cyberfraud because of the low apprehension rate and prosecution of the culprits. Some significant factors affecting the fight against cyberfraud in Africa include a lack of technological requirements, absence of regulatory and control frameworks, weak internal controls and resources (human, capital and financial). However, efforts are being made in many African countries regarding cybercrime legislation, deployment of enabling technologies, regulatory framework and government intervention in combatting cyberfraud, but the battle is far from being won. This study provides insight into the current developments in the African continent in terms of cyberfraud perpetration and mitigation. It also offers possible recommendations on how the fight against cyberfraud can be more

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Cyberfraud occurrences: Africa's experience', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 251-272. <https://doi.org/10.4102/aosis.2024.BK485.13>

proactive and sustainable in the continent. Thus, the findings may be helpful to African governments and stakeholders in combatting cyberfraud.

■ Cyberfraud: Africa's experience

The International Finance Corporation (IFC) report projected that Africa's Internet economy has the potential to reach \$180 billion by 2025, which accounts for 5.2% of the continent's GDP. Furthermore, it was also projected that by 2050, the potential contribution could reach US\$712bn, accounting for 8.5% of the continent's GDP (Thomas 2022). This implies the increasing growth in the continent's population and the number of Internet users. However, the challenge associated with the growing number of Internet users is the risk of individuals and private and public corporations falling victim to cyberfraud. Therefore, according to Kaspersky, an analysis of a Russian company specialising in antivirus software indicates a notable rise in data loss threat-related attacks in Africa during Q2 of 2022 when compared to the preceding quarter. These threats include phishing, scams and social engineering attacks, where users are enticed to websites and deceived into divulging their personal information (Thomas 2022). For instance, Kaspersky detected 10,722,886 phishing attacks in Africa in the second quarter of Q2 (Thomas 2022). Out of these, Internet users from Kenya were mainly affected by this threat. A total of 5,098,534 phishing attacks were detected in three months, representing a growth of 438% compared to the first quarter of 2022. Next to Kenya is South Africa, where 4,578,216 phishing attacks were detected in the second quarter of 2022, accounting for 144% compared to the first quarter of 2022. Third on the list is Nigeria, where 1,046,136 phishing attacks were detected in the same quarter, which represents a growth of 174% compared to the first quarter of 2022 (Thomas 2022).

The annual cost of cybercrime in Africa has been pegged at US\$3.5bn a year, which is likely to increase with the number of people who use the Internet for commercial transactions, banking and other things (Thomas 2022). Hence, cyberfraudsters are poised to exploit Africa's Internet growth for fraud perpetration without a robust cybersecurity effort. This section highlights some financial institutions' experiences, including those of their stakeholders, concerning cyberfraud occurrences in some selected African nations.

In Botswana, Chimuka and Mashumba-Paki (2016, pp. 114, 117) reported an increasing rate of cybercrime and emphasised the need for more proactive measures to combat crime. Dzomira (2014, p. 16) investigates cyberfraud risks in the Zimbabwean banking industry. The study identified various forms of cyberfraud perpetrated against banking institutions and the associated problems. The study's outcome identified the multiple forms

of cyberfraud performed against Zimbabwean banking institutions as unauthorised intrusion, credit and debit card fraud, money laundering, pharming, phishing, malware, hacking, virus, spam and advance fee fraud. Dzomira (2014, p. 16) further identifies some loopholes leading to cyberfraud incidences as nonimplementation of recent technological advances, lack of resources, low-level enforcement of cybercrime laws and inadequate sensitisation. The authors recommended improving cybersecurity through the effective collaboration of all the stakeholders involved in the fight against cyberfraud.

In Kenya, Njeru and Gaitho (2019, p. 512) indicate that cyberfraud occurrences have greatly influenced commercial banks' performance. The authors reveal that most participants in the survey stated that cyberfraud constitutes a significant threat to the Kenyan banking sector. Furthermore, the results obtained from the survey indicated that insurance costs paid by banks in Kenya to protect customers against cyber-related crimes are too high and could affect their financial performance. Besides the insurance costs, banks also invest in IT to meet regulatory and compliance standards. Thus, the insurance, regulatory, and cyberfraud prevention or detection costs could affect the profitability of the Kenyan banking industry.

Kweyu and Ngare (2013, p. 1) analyse the customers' perceptions of mobile banking services in Kenya. The authors found no gender bias in customers' perceptions of mobile banking services. The study also shows no discrepancy in gender-based decisions related to the risk and simplicity of Internet banking. However, the authors stated that some critical factors are necessary to implement mobile banking services in Kenya, such as the availability of Internet connectivity and safety.

In South Africa, the losses incurred by the banking industry because of customers' dissatisfaction following cyberfraud incidences decrease the bank's revenue level. This implies that customers' complaints can lead to a loss of reputation and goodwill, further leading to a loss of organisational profitability.

As of 2021, the number of Internet users in Africa exceeds 500 million, implying that 38% of her population is online (INTERPOL 2020). This number exceeds the population of Internet users in the Middle East, South America and North America (Council of Foreign Relations Report 2019). Gady and Austin (2010, n.p.) describe Africa's cyberspace as 'a weapon of mass destruction potentially posing a menace to the world'. Kenya leads the number of Internet users in Africa with 83% of her population online, followed by Nigeria (60%) and South Africa (56%) (Council of Foreign Relations Report 2019). Africa is substantially visible within the digital financial services landscape via digital or mobile banking, although this has increased the risk and threats of cyberattacks.

Many African countries have embraced digital transformation, which cuts across major spheres such as education, economy, health and banking. Thus, there is a need to ensure cybersecurity to minimise the vulnerability to cyberattacks. Unfortunately, many African businesses operate without cybersecurity protocols (CGTN Report 2020). This significantly threatens profitability, reputation and sustainability. The African Union Commission (2016) reports that eleven countries on the African continent have specific laws or provisions to fight cybercrime. These countries are Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. Furthermore, twelve countries have taken legislative steps to fight cybercrime, while cyber laws have been drafted in some other countries as bills awaiting passage in parliament.

In 2016, the African economy reported having lost a total of \$2 billion to cybercrime, with the annual losses in South Africa estimated as US\$573m, Nigeria US\$550m, Kenya US\$175m, Tanzania US\$85m, Ghana US\$50m and Uganda US\$35m (Scidenet Report 2016; SERIANU 2016). The cost of cybercrime in Africa increased with US\$649m and US\$210m losses attributed to Nigeria and Kenya, respectively, while South Africa reportedly incurred an annual loss of US\$2.2bn to cyberattacks (Accenture 2020). In terms of GDP, SERIANU (2021) reports that Africa witnessed a reduction in GDP by 10% at an estimated loss of US\$4.12bn because of cybercrime. The primary form of cyberattack in Africa relates to spam emails with 679 million detections), website attacks (14.3 million detections) and files (8.2 million detections) between January 2020 and February 2021 (INTERPOL 2020). South Africa has an estimated 230 million threats detected between January 2020 and February (230 out of which 219 relate to email threats). Kenya and Morocco follow with an estimated threat detection of 72 million and 71 million, respectively.

The most prevalent Internet fraud in Africa is phishing and credit card fraud, which involves the theft of confidential information and banking details of the victims used by threat actors to syphon money or transact business. The Institute of Security Studies (2020) reported that the continent witnessed a surge in cyberattack volume by 238% on online banking platforms in 2020 because of COVID-19. Other forms of Internet fraud emerging in Africa are cryptocurrency scams and Ponzi schemes. For the cryptocurrency scams, the Institute of Security Studies (2021) reported that Mirror Trading International defrauded thousands of African investors to US\$588m in Bitcoin in 2020. In the Ponzi scheme case, the Africrypt trading company allegedly absconded with US\$3.6bn in investors' money in April 2021 (Institute of Security Studies 2021). Table 13.1 presents the business email compromise (BEC) recorded from January 2020 to April 2022 (INTERPOL 2020).

TABLE 13.1: Business email compromise recorded from January 2020 to April 2022.

Countries	Business email compromise record (%)
South Africa	34
Tunisia	20
Morocco	12
Mauritius	12
Nigeria	11
Kenya	9
Gabon	1
Central African Republic	1

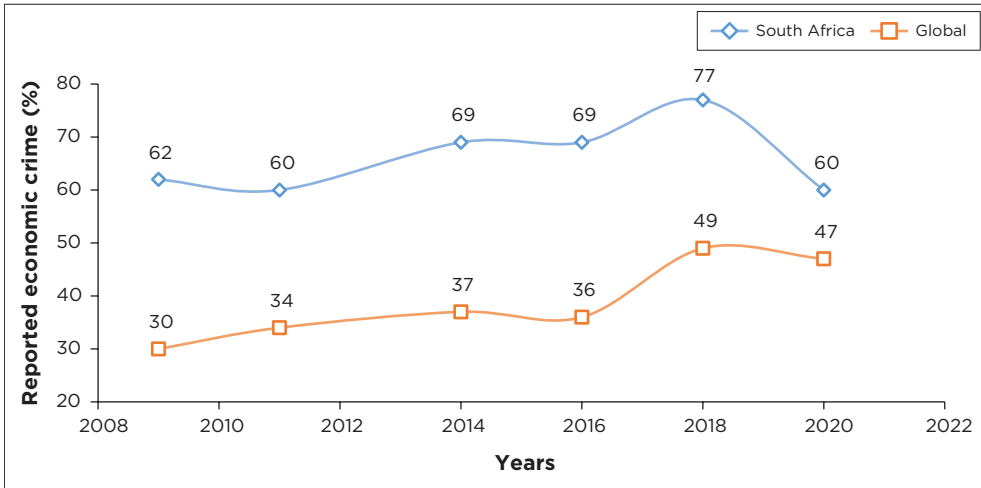
Source: INTERPOL (2020).

The major forms of cyberattack faced in Nigeria are data breaches and hacking. The NCSI of Nigeria as of November 2022 was 54.55 (ranked 61st in the world and 6th in Africa in terms of NCSI) (E-Governance Academy Report 2022). In 2020, Nigeria was ranked 16th among the countries gravely affected by cybercrime. In the third quarter of 2022, Nigeria experienced an increase in data breaches, from 35,472 in the second quarter to 608,765 in the third quarter, accounting for a 1,616% increase (AAG Report 2022a). Part of the Nigerian government's efforts in tackling cybercrime is the establishment of the Economic and Financial Crimes Commission (EFCC), which has so far secured over 5,629 convictions in connection with cyber-related crimes (TransparencIT Report 2022).

The prevalence of economic and financial crimes and their gravity on the economy led to the establishment of EFCC. The Commission has high-level support from the Presidency, the Legislature and fundamental security and law enforcement agencies in Nigeria in combatting economic and financial-related crimes. Chimuka and Mashumba-Paki (2016) report that Botswana is persistently affected by cybercrime and emphasise the need for FA expertise and resources to combat crime.

Figure 13.1 highlights the economic crime rate reported in South Africa compared with the economic crime rate globally in 2020 (PwC's Global Economic Crime Survey 2020, p. 8). According to the statistics, South Africa came third among the ten top countries with the highest reported economic crime rate globally. This is an improvement in the economic crime rate in South Africa, which was ranked first in 2018 (PwC's Global Economic Crime Survey 2020). This indicates that between 2018 and 2020, South Africa witnessed a 17% decrease in the rate of economic crime. However, compared with the global statistics, South Africa still exceeds the average global rate by 13%.

Cassim (2016) identifies some reasons for the increasing rate of economic crime in South Africa: (1) poorly equipped law enforcement agencies, (2) inadequate intelligence gathering and (3) nonimplementation of the common and cyber laws in South Africa.



Source: PwC (2020).

FIGURE 13.1: Reported economic crime in South Africa and global average rate in 2020.

Some laws have been enacted in South Africa to promote information security and regulate electronic communication and transactions, such as the *Promotion of Access to Information Act 2 of 2000* (PAIA) and the *Electronic Communication and Transaction Act 25 of 2002* (ECT). Implementing these laws could protect financial institutions, customers and the public from incessant cyberattacks (Cassim 2016); however, these laws have not been adequately implemented, coupled with the fact that they are perceived as not being stringent enough (Cassim 2016).

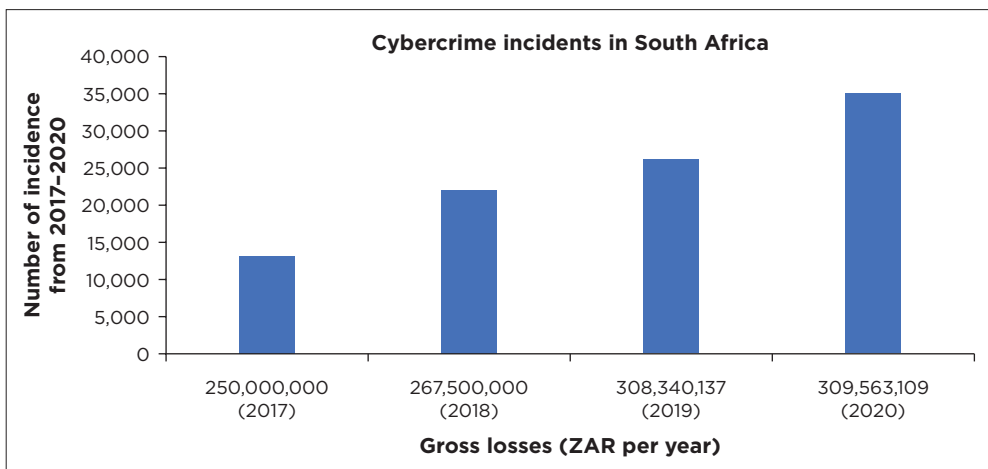
Another effort of the South African government to curb cybercrime was establishing SABRIC and the Computer Security Incident Response Team (CSIRT). The CSIRT was established to respond swiftly to incidents of cybercrime (Cassim 2016). The South African Banking Risk Information Centre provides banking institutions with information related to crime and risk management. It also promotes interbank collaboration to reduce the risk of cyberfraud or other forms of organised crime (Cassim 2016). The South African Police Services' (SAPS) involvement in the fight against cybercrime has also been described as a positive move (Cassim 2011). The police collaborate with financial institutions, government institutions such as the SABRIC and CSIRT, and the IT sector to clamp down and prosecute perpetrators (Cassim 2016). The South African Banking Risk Information Centre (2018) reported that 13,438 cybercrime cases involving smart devices and online banking cost the banking sector a gross sum of over ZAR250m in 2017 in South Africa. In 2019, the number of reported cybercrime incidents increased by 49.41% compared to 2017, costing the

banking industry approximately ZAR308m in gross losses. In 2020, the number of reported cybercrime incidents increased by 61.94% compared to the 2017 statistics, costing the banking industry about ZAR309m in gross losses (SABRIC 2020).

The South African Banking Risk Information Centre (2019) reported an increase in cyberfraud-related cases from January to August 2018 by 64%, with a 7% increase in gross losses compared to the same period in 2017. Comparing the statistics of January to August 2017 with the same period in 2018, the magnitude of losses incurred was found to be doubled. For instance, for the fraud perpetrated via online banking, there was a 44% increase in reported cases, with approximately 73.60% increase in gross losses (African Union Commission 2016). Most of the losses emanating from cyberattacks have been linked to Internet banking operations in the form of online, mobile banking, and credit or debit fraud. The South African Banking Risk Information Centre (2020) reported that between 2018 and 2019, the gross loss incurred on credit or debit cards increased by 20.5%.

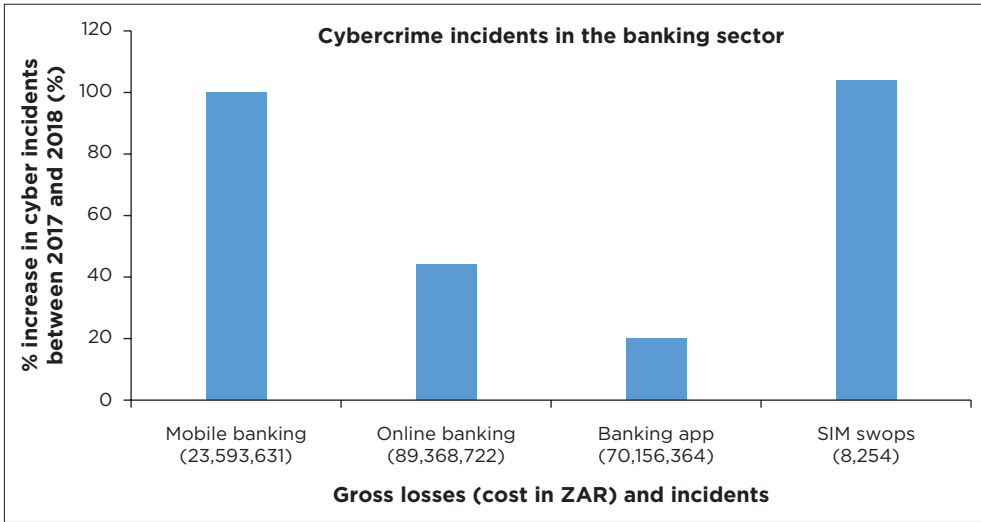
Figure 13.2 highlights the total number of cyberfraud incidents reported from 2017 to 2020 and the losses incurred.

Figure 13.3 highlights the types of Internet banking operations where cyberattacks took place. The statistics show that most incidences occurred via mobile banking, followed by the SIM swap. For the SIM swap, subscribers who fail to delink the previous SIM or mobile number linked to their accounts or used for transaction purposes may suffer cyberfraud attack from a new



Source: SABRIC (2018, 2020).

FIGURE 13.2: Total cyberfraud incidents reported from 2017 to 2020 and the losses incurred.



Source: SABRIC (2019).

FIGURE 13.3: Type of cyberfraud and the losses incurred.

user when the SIM or phone number is recycled. Regarding gross losses, online banking tops the list, followed by the losses incurred via banking apps.

■ Cybersecurity in Africa

The Global Cybersecurity Index (GCI) report (2017) provided an insight into cybersecurity in Africa, which anchored its five pillars, namely, legal, technical, organisational, capacity-building and cooperation (Figure 13.4).

These five pillars of the GCI report are explained as follows:

- **Legal:** This probes the existence of legal institutions and frameworks for tackling cyberfraud and cybersecurity.
- **Technical:** This probes the existence of technical frameworks and institutions and frameworks for tackling cyberfraud and cybersecurity.
- **Organisational:** This probes the existence of strategies and policy coordination institutions for the development of cybersecurity development at the national level.
- **Capacity-building:** This probes the existence of research and development (R&D), education and training programmes or other forms of capacity-building aimed at tackling cyberfraud and cybersecurity.
- **Cooperation:** This probes the existence of partnerships, cooperative frameworks and information-sharing networks at the national, regional and international levels for tackling cyberfraud and cybersecurity.

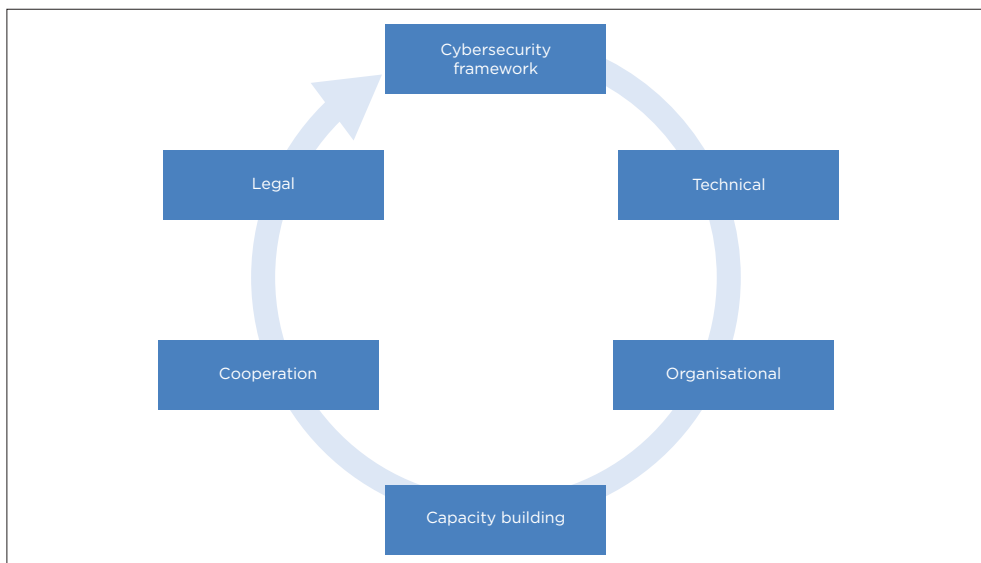


FIGURE 13.4: Five pillars of cybersecurity assessment in Africa.

There seems to be a gap between countries regarding knowledge, awareness and capacity to implement technologies and strategies in cybersecurity. Furthermore, many African countries are still lagging in developing and implementing initiatives to tackle cyberfraud and improve cybersecurity.

Based on the legal, technical, organisational and capacity-building cybersecurity indicators, the GCI report (2017) ranked some selected African member states as presented in Table 13.2.

The GCI (2017) report further categorised African member states into three categories with their respective GCI score based on their efforts in tackling cyberfraud and improvement in cybersecurity (Table 13.3). The first and leading category comprises six countries demonstrating a high commitment to tackling cyberfraud and improving cybersecurity. The second category is maturing, with eleven countries that have developed commitments and continuous engagement in cybersecurity programs and initiatives. The last category is initiating, with 27 countries showing signs of commitment to cybersecurity by commencing measures to tackle cyberfraud and improve cybersecurity.

TABLE 13.2: Cybersecurity security ranking of selected African countries.

Country	Cybersecurity indicators			
	Legal	Technical	Organisational	Capacity-building
Mauritius	0.848	0.964	0.794	0.914
Rwanda	0.600	0.712	0.794	0.657
Kenya	0.753	0.731	0.357	0.408
Nigeria	0.643	0.708	0.531	0.501
Uganda	0.629	0.690	0.165	0.717
South Africa	0.610	0.622	0.416	0.525
Côte d'Ivoire	0.640	0.343	0.334	0.523
Cameroon	0.605	0.560	0.435	0.317
Botswana	0.701	0.278	0.470	0.304
Ethiopia	0.168	0.282	0.333	0.416
Zambia	0.199	0.228	0.167	0.475
Ghana	0.523	0.558	0.344	0.044
Togo	0.364	0.038	0.317	0.132
Zimbabwe	0.424	0.078	0.167	0.116
Burkina Faso	0.062	0.164	0.391	0.282
Sierra Leone	0.031	0.346	0.167	0.033

Source: GCI (2017).

TABLE 13.3: The GCI report on cybersecurity for African member states.

Stage	Country	GCI score
Leading stage	Mauritius	0.830
	Rwanda	0.602
	Kenya	0.574
	Nigeria	0.569
	Uganda	0.536
	South Africa	0.502
Maturing stage	Botswana	0.430
	Côte d'Ivoire	0.416
	Cameroon	0.413
	Ghana	0.326
	Tanzania	0.317
	Senegal	0.314
	Zambia	0.292
	Ethiopia	0.267
	Togo	0.218
	Burkina Faso	0.208
	Mozambique	0.206

Table 13.3 continues on the next page→

TABLE 13.3 (cont.): The GCI report on cybersecurity for African member states.

Stage	Country	GCI score
Initial stage	Zimbabwe	0.192
	Seychelles	0.184
	Niger	0.170
	Madagascar	0.168
	Liberia	0.149
	Sierra Leone	0.145
	Gabon	0.139
	Gambia	0.136
	Burundi	0.120
	Lesotho	0.094
	Guinea	0.090
	Malawi	0.080
	Angola	0.078
	Chad	0.072
	Benin	0.069
	South Sudan	0.067
	Namibia	0.066
	Mali	0.060
	Cape Verde	0.058
	Swaziland	0.041
	Sao Tome and Principe	0.040
	Democratic Republic of the Congo	0.040
	Congo	0.040
	Guinea-Bissau	0.034
	Central African Republic	0.007
	Equatorial Guinea	0.000

Source: GCI (2017).

■ Leading African countries in tackling cyberfraud and improving cybersecurity

This subsection captures some of the leading African countries, including their efforts to tackle cyberfraud and improve cybersecurity in their countries.

■ Mauritius

Mauritius is ranked first in the GCI (2017) report in Africa and 17th globally around cyberfraud mitigation and cybersecurity. The country is reportedly making giant strides in the legal and technical areas relating to cybersecurity. The government embarked on a botnet tracking and detection project that allows the Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to checkmate threats on different networks within the country. In capacity-building, training and awareness on cybersecurity, the Mauritius government IT

Security Unit has conducted over 180 awareness sessions for some 2,000 civil servants in 32 government ministries and departments as of 2017 (GCI report 2017). Mauritius also developed the 'Mauritian Cybercrime Online Reporting System (MAUCORS)'. This national online system allows the public to report cybercrime incidences on social media. It also has advisory capability that provides advice that can assist the public in recognising and avoiding prevalent forms of cybercrime on social media and websites. Furthermore, the country has passed the Cybersecurity and Cybercrime Bill to protect its citizens from cybercriminals, in line with the government's vision to transform Mauritius into a high-income, inclusive and green economy, including a safe and secure cyberspace.

■ Rwanda

Rwanda was ranked second in Africa in the GCI (2017) report. The country reportedly scores high in the organisational pillar and cybersecurity policy that protects the public and private sectors from cyberfraud. Furthermore, the GCI (2017) report indicated some commitment to developing a more robust cybersecurity industry to ensure cyberspace resilience. Part of the government's efforts in ensuring cyber resilience is the passage of the law establishing the National Cyber Security Authority (NCSA) in 2017 and the NCSA becoming operational in 2020. The authority is responsible for building skills and capabilities to secure Rwanda's cyberspace and promote economic sustainability and social development. The NCSA also coordinates national cybersecurity functions in the private and public sectors to ensure the security of Rwanda's ICT (NCSA 2022).

■ Kenya

In the GCI (2017) report, Kenya was ranked third in Africa. This is because of the efforts devoted by the Kenyan government to international cooperation and alliance through the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC). The CIRT coordinates computer incidents with other national, regional and global stakeholders. Computer Incident Response Team is a multi-agency collaboration established to mitigate cyber threats and foster a safer Kenyan cyberspace under the provisions of the *Kenya Information and Communications Act*. Furthermore, the passage of the *Computer Misuse and Cybercrimes Act 5 of 2018* has strengthened CIRT in the quest for national cybersecurity resilience. Since 2017, CIRT has been detecting and preventing cyberfraud while responding to various cyber threats targeted at the country in real time.

Some essential functions of the CIRT include the following:

1. Implementation of national cybersecurity policies, laws and regulations.
2. Capacity-building and cybersecurity sensitisation.
3. Early warning and technical advisories on cyber threats in real time.
4. Technical coordination and response to cyber incidents in real time (locally and internationally).
5. Research and development in cybersecurity.
6. Effective management of critical Internet resources.

Regionally, CIRT works with the East African Communications Organisation and liaises internationally with the International Telecommunication Union (ITU) and Forum of Incident Response and Security Teams (FIRST) and bi-laterally with the US and Japan, among others.

Thus, the CIRT acts as the interface between local and international ICT services providers that cyberfraud perpetrators engage in committing cyberfraud and the Kenyan Judiciary, which investigates and prosecutes cybercrimes (Communication Authority of Kenya 2022).

■ Nigeria

Nigeria's cyberfraud is committed mainly by young people, often called the 'Yahoo Boys' or '419s'. Fraudsters increasingly take undue advantage of the rise in online transactions, electronic shopping, e-commerce and electronic messaging systems to engage in cyberfraud activities. Part of the government's effort to curb the activities of cyberfraudsters includes the passage of the *Cybercrimes Act* in 2015. The law criminalises various cyberfraud offences ranging from ATM card skimming, phishing and identity theft to possession of child pornography. It stipulates seven years imprisonment for all kinds of cyberfraud offenders, an additional seven years for online crimes resulting in physical harm and life imprisonment for crimes that lead to the death of a victim. Another effort by the Nigerian government to curb economic-related crimes was establishing the EFCC, which has secured over 5,629 convictions in connection with cyber-related crimes (TransparencIT Report 2022).

■ Uganda

Uganda's technology is growing and has witnessed abuse and misuse of cyberspace to commit or facilitate cyberfraud. Fraudsters usually target Facebook and emails, ATMs, hacking, social engineering attacks and networking, among others, to commit crimes. The Ugandan government enacted the *Electronic Transactions Act 2011* to curb this trend. This Act provides for the use, security, facilitation and regulation of electronic communications and transactions and encourages the use of e-government

services (Wanyama 2013). In 2011, the Ugandan government passed the *Computer Misuse Act 2011* to strengthen the growing technology sector. However, with the recent rise of cyberfraud in the country, the Ugandan Parliament passed an amendment to the Computer Misuse Bill in 2022, prescribing stricter penalties for those perpetrating cyberfraud (Kanali 2022).

■ South Africa

Allen (2021) indicated that the country's well-developed financial infrastructure makes it a target for cybercriminals. Existing literature on the causes of cybercrime has traced one of the causes that recent innovations and technological development in this digital age are responsible for the increasing risks of cybercrime in South Africa (Coetzee 2017, p. 3; Dagada 2013, p. 148; Dlamini & Mbambo 2019, p. 1; Dzomira 2017, p. 143; Herselman & Warren 2004, p. 263; Sutherland 2017, p. 84).

Cassim (2016, p. 127) indicated that inadequately equipped law enforcement agencies, poor intelligence gathering and the ineffectiveness of the common law in South Africa to curb cybercrime are some factors that inhibit an effective fight against cybercrime. In South Africa, the lack of a clear definition of cybercrime has also hindered effective investigations and prosecutions (Allen 2021).

Part of the government's effort in mitigating cyberfraud is the enactment of the PAIA and ECT, as well as the establishment of SABRIC and CSIRT. The NCPF was developed to create a framework for tackling and investigating cybercrime. The key objectives of the NCPF are to (Budapest Convention, Council of Europe 2022)⁵:

- Centralise the coordination of cybersecurity-related activities by facilitating the establishment of relevant structures, policy frameworks and strategies supporting cybersecurity. This is aimed at combatting cybercrime and addressing national security imperatives.
- Foster cooperation and coordination between government, the private sector and civil society by stimulating and supporting a strong interplay between policy, legislation, societal acceptance and technology.
- Promote international cooperation.
- Develop requisite skills, R&D capacity.

5. Budapest Convention, Council of Europe 2022, Article 10, 'Offences related to infringements of copyright and related rights', Cybercrime Programme Office (C-PROC) of the Council of Europe, [South Africa] Cybercrime legislation Domestic equivalent to the provisions of the Budapest Convention, version August 2022, viewed 26 October 2023, from https://www.coe.int/en/web/octopus/-/south-africa?p_p_col_count=1&p_p_col_id=column-4&p_p_lifecycle=0&p_p_mode=view&p_p_state=normal&redirect=https%3A%2F%2Fwww.

- Promote a culture of cybersecurity.
- Promote compliance with appropriate technical and operational cybersecurity standards.

Allen (2021) states that South Africa has witnessed legislation implementation challenges. However, the new legislation indicates the country's commitment to cybersecurity. Allen (2021) noted that the new cybercrime legislation promotes South Africa to the international standard in the fight against cyberfraud.

In 2013, the South African government enacted the POPIA to ensure data privacy, while in 2015, the government also passed a NCPF enforced by the Ministry of State Security (Sutherland 2017, p. 83). Sutherland (2017, p. 83) also opines that South Africa is still lagging behind advanced nations in the enactment and implementation cybersecurity law. In a bid to combat cybercrime effectively in South Africa, a collaborative national cyber defence effort involving the public and private sectors, military and national security, government and citizens has been identified as a critical requirement (Dlamini & Mbambo 2019, p. 10; Grobler et al. 2013, p. 39).

Together with POPIA, the new cyber law is crucial to South Africa's measures to tackle cybercrime. Allen (2021) demonstrated that at the heart of the legislation lie the offences encompassing cybercrimes. In South Africa, cybercrime is presently characterised as encompassing a range of activities, including but not confined to the unauthorised access to computer systems or devices, such as USB drives or external hard drives; unlawful data interception; the illicit acquisition, possession, receipt or utilisation of passwords; as well as forgery, fraud, online extortion and malicious online communications. The law provides the scope and approach by which investigators can search and seize computer hardware, software and other items. It also describes how the South African authorities should conduct international investigations, including evidence collection, sharing and preservation. Since cybercrime cuts across borders, the legislation prescribes an approach to international cooperation and information-sharing. It also permits the South African police to conduct domestic investigations and be part of international cooperation.

The *Cybercrimes Act* and the POPIA are closely interconnected. The POPIA concerns data privacy, while the *Cybercrimes Act* concerns cybersecurity. Thus, balancing privacy, security and personal freedom is required for proper cybercrime activities that are presentable in the court.

Allen (2021) decries the decisive implementation of the Act and indicates that the lack of the required knowledge, experience and staffing of the SAPS are significant hindrances.

The Centre of Excellence in Financial Service (2017, pp. 129–131) indicates that, in South Africa, the emergence of digital technology has continued to change the structure of the financial market and transform business operations. The report explains that the infusion of technology into the financial sector has improved customers' experience with fast, constant and convenient services even though there are new risks in the form of threats to privacy and cyberattacks on consumers, which lead to a bad reputation of the financial institution.

Standard Bank South Africa prioritises human resource development. This enables their employees to acquire relevant skills and expertise to manage digital operations effectively. The bank constantly develops training and skills development programmes for their employees and collaborates with various universities and research institutes in South Africa to develop IT curricula and upskilling programmes. This is to get their employees informed about the emerging IT business models (Standard Bank Group Ltd. 2016a, p. 60). The Standard Bank Group (2016a, p. 60) states in the annual report of 2016 that the need to prioritise human capacity development was informed by the need to keep their employees abreast of emerging technologies and techniques to enhance effective banking operation and customers' satisfaction. For ABSA, emerging technologies have increased the rate of cybersecurity risk; hence, the bank relies on the expertise of the staff to achieve efficiency (Barclays Africa Group Ltd. 2017a, p. 4). This notion is corroborated by the PwC report (2022b) that the use of emerging technologies continues to increase cybersecurity risks. The bank decries the emerging digital technologies that have increased the scarcity of exceptional skills in the areas of data analytics, IT, forensics, cybersecurity and risk management (Barclays Africa Group Ltd. 2017a, p. 14). To tackle the challenges of cyber insecurity, ABSA continues to invest in human capacity development and recruitment of employees who specialise in IT, data analytics and cybersecurity (Barclays Africa Group Ltd. 2017b, p. 39). The banks also stress the need for effective collaborations among the relevant stakeholders to sustain the fight against cyberfraud (Barclays Africa Group Ltd. 2017b, p. 35).

First National Bank (FNB) in South Africa reports that their investment in human capacity development increased by 240% in 2017 (FirstRand Group Ltd. 2017, p. 9). Comparing the digital transactions of 2016 and 2017, FNB indicates that, in 2017, the number of electronic transactions increased by 88%. Banking applications accounted for 68%, and mobile devices accounted for 20% of the increase (FirstRand Group Ltd. 2017, p. 52).

Capitec Bank focuses on technologies to simplify banking operations cost-effectively, and the bank recruits staff with the capacity to interact and support their clients (Capitec Bank Ltd. 2017, p. 36). The bank is also

devising means to develop digital channels for accessing banking services (Capitec Bank Ltd. 2017, p. 12).

For Nedbank, digital solutions have optimised the branch floorspace to promote smart services (Nedbank Group Ltd. 2017). The bank also seeks to develop innovative solutions to assist their clients in migrating to digital channels with the development of human capacity so that they can service their clients effectively (Nedbank Group Ltd. 2017, p. 47). Nedbank also indicated the introduction of 336 electronic branches across South Africa (Nedbank Group Ltd. 2015). It was reported that, in 2017, Nedbank unveiled a self-service electronic branch known as the 'NZone', which offers an interactive virtual wall with a secured video kiosk for effective interaction with the clients, thus exposing customers to innovative products and electronic banking operations (Khumalo 2017). Coetzee (2016) explained that banks in South Africa are gradually migrating their clients to cost-effective digital platforms powered by emerging technologies. This study confirms that South African banks gradually embrace technology for effective bank-client relationships with a remote interaction strategy. South African banks now employ digital facilities such as self-service booths, quick-chat banking, robot advisers, smart depositors, video-banking, virtual and augmented reality, biometrics, BDA, cloud computing, artificial intelligence, blockchain, biometrics and quantum computing in their branches (Capitec Bank Ltd. 2017; Nedbank Group Ltd. 2017, p. 37; Standard Bank Group Ltd. 2016b).

Akinbowale, Klingelhöfer and Zerihun (2022a, 2022c, 2023d) indicated that cyberfraud impact seriously affects the South African banking industry's profitability, customer satisfaction, goodwill and reputation. The use of the Balanced Scorecard performance measurement of the cyberfraud mitigation and FA for detailed investigation of cyberfraud incidences has been proposed (Akinbowale et al. 2022, 2023b). Existing literature on cybercrime in South Africa has traced one of the causes to recent innovations and technological development (Coetzee 2017, p. 3; Dagada 2013, p. 148; Dlamini & Mbambo 2019, p. 1; Dzomira 2017, p. 143; Herselman & Warren 2004, p. 263; Sutherland 2017, p. 84). In South Africa, Mbelli and Dwolatzky (2016, p. 1) explain that information security challenges because of cyberattacks continue to pose a severe economic threat to financial institutions and the country. Therefore, the authors suggested continuous investment in up-to-date anti-fraud technologies and security measures as a proactive way.

The report of the Centre of Excellence in Financial Service (2017, pp. 129-131) indicated that, in South Africa, the emergence of digital technology has continued to change the structure of the financial market and transform business operations, improving the experience of customers with fast, constant

and convenient services despite new risks in the form of threats to privacy and cyberattacks on consumers, which lead to a bad reputation of the financial institution. Therefore, the 'big five' banks in South Africa (Standard Bank, FNB, ABSA, Nedbank, Capitec) are gradually developing approaches to facilitate consistent relevance in the market by prioritising critical operational innovations like digital technology and data-mining concepts:

- Standard Bank reports on using digital technologies and solutions for operational excellence, protecting clients' information and enhancing clients' experience (Standard Bank Group Ltd. 2021, pp. 22, 27).
- ABSA relies on continued investment in technological solutions and digitalisation to counter the increased cyber-related security risks (Barclays Africa Group Ltd. 2021).
- The FirstRand Group indicates their continuous investment in technology and digital platforms to improve business operations. This has reportedly caused an increase in IT expenditure by 3% in 2022 (FirstRand Group Ltd. 2022, p. 31).
- For Nedbank, the digital transformation has benefited the employees, clients and stakeholders (Nedbank Group Ltd. 2021). Nedbank also indicated introducing more electronic branches across South Africa and an interactive virtual wall known as the 'NZone' for adequate client interaction (Khumalo 2017).
- For Capitec Bank, technology is an integral part of the bank's strategy to create tailored, user-friendly solutions for effective banking and financial decision-making by the clients. The bank is also devising more means to develop digital channels for accessing banking services to enhance clients' digital experience (Capitec Bank Ltd. 2022, p. 13). The bank focuses on becoming entirely paperless by adding new digital functionalities to the banking app. Thus, it has become one of South Africa's leading digital banks, with 16 million clients and 8 million digital users (Capitec Bank Ltd. 2022).

Coetzee (2017) explained that banks in South Africa are gradually migrating their clients to cost-effective digital platforms powered by emerging technologies. This study confirms that South African banks are slowly embracing technology for effective bank-client relationships with a remote interaction strategy. South African banks nowadays employ digital facilities such as self-service booths, quick-chat banking, robot advisers, smart depositors, video-banking, virtual and augmented reality, biometrics, BDA, cloud computing, artificial intelligence, blockchain, biometrics and quantum computing in their branches (Capitec Bank Ltd 2022; FirstRand Group Ltd 2022; Nedbank Group Ltd 2021; Standard Bank Group Ltd 2021).

Furthermore, regarding the rising risk of cyberfraud in the retail banking sector, the 'big-four banks' in South Africa as of 2019 (Standard Bank, FNB,

ABSA, Nedbank) are gradually developing approaches to facilitate a consistent relevance in the market by prioritising critical operational innovations like digital technology and data-mining concepts (PwC 2020, p. 9). These will aid the development of better ways to deliver quality services to their customers and adequately compete successfully with other competitors in the industry (PwC 2020a, p. 9, 2020b).

Table 13.4 summarises the attempts made by certain selected African countries to fight cybercrime and some of the resulting challenges.

TABLE 13.4: Attempts made by selected African countries to fight cybercrime and the limitations.

Country	Attempts made at tackling cybercrime	Limitation
South Africa	Enacted the PAIA and ECT, as well as the establishment of SABRIC and CSIRT	Lack of stringent measures on cybercriminals and implementation of cybercrime laws
Namibia	Presentation of the Namibian electronic and communication bill to regulate electronic, communication and information system management	The bill is yet to be passed
Botswana	Passage of the <i>Cybercrime and Computer Related Crime Act 22 of 2007</i> to combat cybercrime	Effective enforcement of this law is a major concern
Kenya	Enacted <i>Kenyan Information Communication Amendment Act of 2009</i> (Section 83 W-Z & 84 A-F) which prohibits cybercrime. Introduction of the Computer Emergency Response Teams in collaboration with Uganda, Tanzania, Rwanda and Burundi to tackle cybercrime.	The Act does not address cross-border cybercriminal activities
Uganda	Presentation of three bills, namely, electronic transaction bill, electronic signature bill and computer misuse bill in 2010, to promote cyber security and the security of transactions and devices with tough sanctions prescribed for the offenders	Lack of adequate forensic lab expertise and investigations, inadequate infrastructure and enforcement personnel and a lack of public sensitisation about cybercrime
Rwanda	Preparation of Information, Communication and Criminal Bill draft which covers electronic signature, protection of customers, as well as personal and organisational privacy. Presentation of bills on digital copyright and electronic contracting.	Bills awaiting passage by the Rwandan parliament
Nigeria	Establishment of Economic and Financial Crime Commission to tackle economic-related crimes	Slow implementation of <i>Cybercrime Act of 2015</i>
Cameroon	Presentation of a bill to criminalise cybercrime. Establishment of the National Agency for Information and Communication Technologies to promote ICT and to regulate activities in cybersecurity. This institution has two main objectives: to facilitate and accelerate the development of ICTs and to harmonise its exploitation and the second is to contribute to the development of Cameroon through the safe use of ICT.	No specific legislation and to combat cybercrime

Table 13.4 continues on the next page →

TABLE 13.4 (cont.): Attempts made by selected African countries to fight cybercrime and the limitations.

Country	Attempts made at tackling cybercrime	Limitation
Ghana	Development of computer emergency response team, which assists in implementing proactive measures to reduce the cyber-related incidents across the country. Furthermore, the establishment of a cybercrime unit as a specialised unit at the Criminal Investigations Department of the Ghana Police Service. The cybercrime unit focuses on the detection and investigation of crimes where digital device(s), network(s) and other telecommunication device(s) or the Internet space is/are the target(s) used. In addition, the passage of <i>2008 Electronic Transactions Act (Act 772)</i> and <i>2012 Data Protection Act</i>	The legislations against cybercrime lack adaptability to new forms of cybercrime and pose some difficulties in collecting evidence to persecute perpetrators. Thus, this results in a low rate of apprehension of cyber fraudsters and prosecution.
Sierra Leone	Regulation of the telecoms sector by the Act of Parliament and the establishment of the National Telecommunications Commissions in 2006 to protect customers. Enactment of the <i>Cybercrime Act in 2021</i> to prevent abusive use of computers and a timely and effective collection of electronic evidence for investigation and prosecution of cyber criminals	Implementation of cybercrime legislations
Zambia	Introduction of the National Policy Framework on cybercrime, which criminalises cybercrime and other computer-related offences. Acceded to the Global Security Agenda aimed at coordinating the international response to cybercrime.	Implementation of cybercrime legislations. Lacks the required skills, expertise, equipment, infrastructure and organisation's ability to fight cybercrime.
	Zambia established the Zambia Information and Communications Technology Authority to help the nation become a digital society through quality, security and access to ICT services and products. Zambia Information and Communications Technology Authority is mandated to regulate and monitor the performance of electronic communication services, set standards for ICT and protect the rights of consumers, providers, etc. Enactment of <i>Cybersecurity and Cybercrime Acts in 2021</i>	

Source: Cassim (2016), GCI (2017) and Kargbo (2021).

Key: PAIA, *Promotion of Access to Information Act 2 of 2000*; ECT, *Electronic Communication and Transaction Act 25 of 2002* SABRIC, South African Banking Risk Information Centre; CSIRT, Computer Security Incident Response Team, ICT, information and communication technology.

For African countries to effectively tackle cybercrime, there is a need to endorse the Council of Europe Convention on Cybercrime's (CECC) role in ensuring consistency in the various cybercrime laws of the different countries. The primary goal of the CECC is to put in place a collective criminal policy aimed at protecting public cybercrime via the development of suitable legislation and the adoption of international collaboration in prosecuting cybercriminals (Cassim 2016).

It is also necessary for African countries to adopt a balanced strategy that preserves fundamental human rights when enacting laws against cybercrime during the investigation and prosecution of the culprits.

Many African countries need international support with technical, legal or financial assistance to sustain the fight against cybercrime. There is also a need to pass the pending cybercriminal bills and impose stringent penalties on perpetrators as a deterrent. Cassim (2016) emphasises the need for the introduction of adequate cybercrime legislation, integration of legal frameworks aimed at combatting cybercrime, development of international cooperation and partnership aimed at curbing cybercrime, sensitisation of the public about the threat of cybercrime, use of cyberspace and online transactions. This recommendation is because of a lack of awareness and public sensitisation, which are significant contributors to the increasing rate of cybercrime in African countries (Cassim 2016). There is also a need to regulate activities in public cyber cafés' development of human capacity and skills training offerings, with continuous research in finance, cybersecurity, FA, legislation and enforcement of laws to prevent cybercrime. This will also enable organisations to become aware of emerging anti-fraud technologies. It will also improve the forensic capabilities of personnel to uncover fraud. Developing collaboration strategies with other nations at the regional and international levels to purposely combat Internet fraud will also assist in the fight against cybercrime. For instance, in September 2019, the FBI disrupted a coordinated cyberfraud scheme, which resulted in the arrest of 281 threat actors across the UK, the US, Nigeria, Japan, Turkey, France, Italy, Ghana, Malaysia and Kenya. This resulted in the seizure of US\$3.7m and the recovery of US\$118m fraudulent wire transfer funds (FBI 2019). This shows the importance of synergy and international cooperation among police and other law enforcement agencies to sustain the fight against cyberfraud. Finally, there is a need for effective collaboration with stakeholders (both in the public and private sectors) and financial and government institutions to sustain the fight against cybercrime (Cassim 2016).

■ Conclusion

This chapter presented Africa's trends and statistics in the rate of cyberfraud. The impact of cyberfraud is far-reaching, especially on the African continent. This is because of a lack of the technological requirements and resources (human, capital and financial) to combat cybercrime. In addition, the increasing rate of the population in the Africa, coupled with the growing rate of Internet users, makes the continent more vulnerable to cyberattacks. However, efforts are being made in many African countries regarding legislation, deployment of enabling technologies, regulatory framework and government intervention in combatting cyberfraud, but the battle is far from being won. Some of the studies reviewed identified some of the possible causes of the surge in the African countries as follows: lack of required expertise and enabling digital technologies, absence or

inadequately implemented cybercrime legislation with a low rate of prosecution, lack of synergy among the stakeholders combatting cybercrime, absence of national, regional and international collaborations, lack of public awareness and sensitisation, weak internal controls, socio-economic factors among other factors. Thus, it is recommended that African countries review their strategies in combatting cyberfraud and make them more holistic and proactive in line with some of the approaches developed in many advanced countries. The development of human capacities and the deployment of more digital technologies are recommended. Furthermore, effective collaboration of all the stakeholders in combatting cyberfraud will be helpful. In addition, synergy at all levels (national, regional and international) will make the fight against cyberfraud more sustainable.

Investigating the effectiveness of management control systems employed for fraud mitigation in the South African banking industry⁶

■ Introduction

This chapter investigates the effectiveness of some MCSs strategies employed for cyberfraud mitigation by the South African banking industry. Secondary data relating to the fraud identification methods and organisational fraud programme was collected, and statistical analysis was

6. The following chapter is based on the first author's PhD thesis:

Akinbowale, OE 2022, 'The integration of forensic accounting and management control systems as a tool for combating cyberfraud in the South african banking sector', Submitted in fulfilment of the requirements for a Doctor of Business Studies in Finance in the Department of Finance and Investment, Faculty of Economics and Finance at the Tshwane University of Technology under the supervision of Professor Heinz Eckart Klingelhöfer & Professor Mulatu Fekadu Zerihun.

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Investigating the effectiveness of management control systems employed for fraud mitigation in the South African banking industry', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 273–299. <https://doi.org/10.4102/aosis.2024.BK485.14>

carried out in the SPSS 2022 environment. Specifically, Spearman's correlation, cross-tabulation and Fischer's exact non-parametric statistics were carried out to determine the relationship between the rate of cyberfraud occurrence (dependent variable) and the methods of fraud identification and organisations' fraud programmes (independent variable).

The results indicated that the rate of cyberfraud occurrence in South Africa might not reduce with an increase in the investigation rate, disclosure to the board and regulator and the engagement of forensic accountants. Conversely, the results also show that, to a certain extent, the engagement of an auditor, legal counsel, stakeholders and public disclosures may promote a reduction in the rate of cyberfraud perpetration or mitigation in South Africa. The results further show that the rate of cyberfraud may not reduce with an increase in the rate of governance resources, third-party management, risk assessment, and policies and procedures in South Africa. On the other hand, the findings indicate that, to a large extent, implementing organisational fraud programmes such as training and communication, monitoring and auditing, investigation, and incentives may promote reduced cyberfraud perpetration or mitigation in South Africa. The findings in this chapter may assist financial institutions in identifying the areas that need improvement concerning the methods of fraud identification and the organisation's fraud programme. The study also adds to understanding MCSs strategies for effective cyberfraud mitigation.

■ Management control systems fight against cyberfraud

'Management control systems' is a broad and encompassing term that relates to the entire organisation's business processes (internal and external activities). It provides the necessary impetus that drives an organisation towards achieving the set goals (Kloof 1997, p. 49; Langfield-Smith 1997, p. 215). Internal control is a subset of the MCS limited to the internal activities related to the organisation's resources and employee management, reporting and controls. Internal control is perceived as a system capable of providing adequate and timely feedback on the progress of an organisation's objectives. Still, it cannot independently guarantee the realisation of the objectives. On the other hand, the MCS primarily deal with realising objectives and implementing strategies (Otley 2016, p. 50).

Shahabuddin, Alam and Azad (2011, p. 58), in their attempt to distinguish between internal control and MCS, state that internal control is a process affected by the organisation's structure, workflow, hierarchy, employee and management information systems. It is developed to assist in achieving a particular set of targets or objectives. Thus, an organisation's resources are managed, measured, directed and monitored through a well-developed

internal control system (Shahabuddin et al. 2011, p. 58). An effective internal control plays a significant role in the detection and prevention of fraud as well as in the protection of the organisation's resources.

According to Punitha et al. (n.d., p. 59), internal control refers to the whole control system employed by the organisation's management to perform the organisation's business effectively. It includes the financial and administrative controls set up by the management to ensure an effective operation, security of assets and accuracy of records (Punitha et al. n.d., p. 59). The internal control system provides information about the accuracy and reliability of information received. It also ensures the safety of organisational assets against misappropriation and that there is no deviation in the management policies. Thus, auditors and fraud investigators rely on the internal control system to determine their work's timing, nature and scope.

Dutta (2007, p. 7) indicates that at the organisational level, MCS can be designed to assist the management in running the business in a coordinated way geared towards realising the organisation's goals in a timely and cost-effective manner. Thus, the MCS could be useful in combatting cyberfraud provided it is tailored towards the goal of cyberfraud mitigation.

Prabowo (2011, p. 378) explains that organisations need to formulate and implement effective strategies that can drive activities such as fraud prevention policies, risk management, fraud-awareness, implementation of anti-fraud technologies and legal deterrence to achieve fraud prevention. Resources can be allocated to all these activities, coordinated and monitored through the MCS. However, the implementation of these activities partly depends on the availability of robust internal control systems (Prabowo 2011, pp. 375, 382).

Internal controls can be executed at the organisational or transactional levels. At the organisational level, the goals of internal control are to ensure the reliability of financial reporting and to provide adequate feedback on how the organisation's goals are achieved concerning regulatory standards. Conversely, at the transaction level, internal control is the set of activities related to the control procedures aimed at minimising process variation to achieve a more productive result with effective monitoring of business transactions. Shahabuddin et al. (2011, p. 60) explain that internal control can substantially ensure that the objectives of an organisation will be met through a systematic improvement in business performance. However, realising an organisation's strategic objectives is not only a function of reasonable internal control as other factors such as technology, business environment, competition and innovation need to be considered (Shahabuddin et al. 2011, p. 60). Hence, robust internal control can only provide timely feedback on the progress of business activities in relation to

the organisation's goal but cannot independently guarantee the realisation of organisation's goals (Shahabuddin et al. 2011, p. 60).

Internal control plays a significant role in fraud mitigation. It can uncover the situations that could lead to fraud and determine whether the organisation puts adequate control measures to mitigate the fraud risk to a permissible limit. It has been reported that weak internal controls can promote fraud perpetration. The threat actors can exploit weak internal controls such as poor supervision, improper document control processes and poor access control to commit fraud (Andoh, Quaye & Akomea-Frimpong 2017, p. 411; Dellaportas 2013, p. 29; Zakaria, Nawawi & Salin 2016, p. 1154). Furthermore, Kamande Kiragu and Musumba (2017, pp. 109, 110) indicate that robust internal control can identify red flags for suspected fraud cases. It can also be used to raise fraud-awareness levels. It can also promote a good organisational culture to mitigate the identified red flags or potential fraud causes (Schuchter & Levi 2013, p. 107). Hence, a robust internal control system is important to combat the sustainability of the fight against cybercrime.

The identified elements of internal controls consist of the following, among others: risk assessment, control system, information and communication structure, monitoring and review activities (Mohd-Sanusi et al. 2015; Oguda, Odhiambo & Byaruhanga 2015). The internal control measures will assist fraud investigators in observing the code of conduct and reviews of transactions. According to Dutta (2007, p. 4), MCS consists of a system of information processes which verifies and validates the organisation's physical processes. Management control systems can provide direction for the entire organisational business processes and drive the organisation towards the realisation of the set goals (Dutta 2007, p. 5). Akinbowale, Klingelhöfer and Zerihun (2021, p. 2) explain that the MCS can be the right step to sustain the fight against cyberfraud. Otley (2016, p. 50) indicates that MCS encompass management accounting as the centrepiece of several organisations' control methods and decision-making strategies. Existing studies have reported that an adequately designed MCS could promote an organisation's performance regarding information security and fraud mitigation (Carenys 2012, p. 12; Mohammed & Knapkova 2016, pp. 276, 277; Slavoljub, Srdjan & Predrag 2015, p. 48). In addition, MCS can ensure that the organisation's resources are effectively utilised to achieve an organisation's goal of cyberfraud mitigation. Management control systems can also promote organisational performance and services (Dutta 2007, p. 6) since they can enable strategic planning where the organisation's goals and vision are aligned. Through an organisation's MCS, corrective actions can be taken whenever there is a deviation from the ideal or expected performance. The MCS can also enable the control and integration of activities. For example, individual tasks at all business levels are integrated into the business objectives. Furthermore, a robust MCS provides a strategic

road map for the employees and ensures that business operations are controlled along the right path.

To achieve a sustainable fight against cyberfraud, an organisation's MCS can be developed to acquire information and measure the performance of all organisational resources (physical, human and financial) pertaining to the goal of cyberfraud mitigation pursued. The MCS can also promote the achievement of the following: social objectives, robust system of communication and information flow, delegation of responsibilities, coordination of internal and external activities, and optimum utilisation of the organisation's resources through a system of effective internal control and information system. Therefore, this study aims to investigate the effectiveness of some MCS strategies employed for cyberfraud mitigation by the South African banking industry.

The findings in this study may assist financial institutions in identifying the areas that need improvement concerning the methods of fraud identification and organisational fraud programme. The study also adds to understanding MCS strategies for effective cyberfraud mitigation.

■ Methodology

The analysis in this chapter used secondary data from the PwC (2020) report on economic crime in South Africa. The analyses included the non-parametric and inferential statistics using the SPSS version 2022. The analyses were carried out to identify the relationships between or among the variables and for a comprehensive understanding of the organisation's method of fraud identification and its fraud programmes. Inferential statistics can be used to establish cause-effect relationships among the identified factors. The SPSS is a versatile and comprehensive statistical tool for converting data into meaningful information. The software is also embedded with programs that can be useful in organising, analysing and interpreting data sets. The fact that SPSS is flexible makes it easy to modify existing variables to create new ones and to import data sets from other sources (Arkkelin 2014, p. 10; Paura & Arhipova 2012, p. 11). The SPSS software has programs for performing non-parametric statistics, including inferential statistics carried out in this study with a quick display of the results.

The inferential statistical analysis is a basic statistical technique which uses data to explain the current situation and to draw a valid conclusion or project future occurrences (Sutanapong & Louangrath 2015, p. 22). The cross-tabulation, Spearman's correlation and Fischer's exact statistics were the inferential statistics employed in the SPSS environment to draw correlations among the variables to conclude. The statistical analyses on the data set are ultimately non-parametric due to the categorical data obtained without an unknown distribution.

■ Non-parametric analysis

The non-parametric analysis is usually suitable for categorical data sets; that is, a nominal data set employed in this study (Kampen & Swyngedouw 2000, p. 91; Wilson 1971, p. 136). Non-parametric tests typically do not require any underlying population and distribution for assumptions. Thus, the choice of this non-parametric test was informed by the type of the qualitative nominal data (YES or NO) collected from the secondary data source with an unknown distribution (Kampen & Swyngedouw 2000, p. 91; Wilson 1971, p. 136). The non-parametric analysis carried out in this study includes the cross-tabulation, the chi-square statistical analysis, Fischer's exact test, cross-tabulation and Spearman's correlation. The data collected were coded for ease of handling and analysis. Data analysis and interpretations are carried out in this study to generate patterns and examine the relationship among the variables. The relationships in the opinions are identified to obtain an insight into the phenomenon investigated (fraud), the method of identification and organisational programmes in combatting it.

■ Cross-tabulation

A cross-tabulation comprises two or more dimensional tables that record respondents' frequency with specific characteristics described in the table's cells. It provides a wealth of information about the relationship existing between the variables. It also presents the results of the entire group of respondents and those from the subgroups of respondents. This enables a precise investigation of the relationships within the dataset, which might not be apparent when looking at total survey responses (White 2004, p. 179). This study employed cross-tabulation to determine whether the relationship between two categorical factors is significant. With the cross-tabulation, the data are summarised in tables to ascertain the significance of the relationship existing between them (White 2004, p. 179). The relationship between the variables can be established from the actual cell values in the frequency table. Cells with zero correlation correspond with statistical independence and vice versa (White 2004, p. 179). It is vital to establish the significance of the relationship between two or more variables relating to the method of fraud identification and organisational programmes in combatting fraud. The variable of the method of fraud identification and organisational programmes can exert a positive effect on other dependent variables, thus promoting a significant reduction in fraud occurrences.

■ Fisher's exact test

Fisher's exact test is appropriate to determine the presence of a nonrandom association between two categorical variables. It is applied

in this study to determine whether the variables are dependent or independent (Kim 2017, p. 152). Fisher's exact test is used for data with small sample sizes, although practically valid for all sample sizes (Kim 2017, p. 154). While the chi-square test relies on approximation, Fisher's exact test is exact. Since the chi-square test determines the relationship between variables by approximation, it may not sufficiently define the association of the variables. Hence, Fisher's test was further employed. Fisher's exact test assesses the independence of the variables by evaluating the possible combination of the data in the table's cells to compute the p -value. The Fisher's exact test values were computed using Equation (14.1) (Amigo-Dobaño, Garza-Gil & Varela-Lafuente 2020, p. 6).

$$p = ((a + b)!(c + d)!(a + c)!(b + d)!)/a!b!c!d!N! \quad [\text{Eqn 14.1}]$$

where a, b, c and d are the frequencies of the categorical variable of the 2×2 contingency table while N is the total frequency.

■ Spearman's correlation analysis

This is a non-parametric analysis used for measuring the degree of association between two variables of ranked scores (Choi, Peters & Mueller 2010, p. 459). It was employed in this study to determine the degree of interdependence between two variables. According to Choi et al. (2010, p. 460), Spearman's correlation coefficient (ρ) ranges from -1 to $+1$. A value of $+1$ denotes a perfect correlation between the variables, while -1 means a perfect negative correlation. On the other hand, a value of 0 means there is no correlation between the variables.

A positive coefficient means there is a direct relationship between the variables. At the same time, a negative result implies an inverse relationship between the variables. The Spearman's correlation coefficient provides a measure of the strength of a monotonic association between two categorical variables (Sedgwick 2014, p. 1). A monotonic association is an association between two variables whereby an increase or decrease in one variable may result in an increase or decrease in the other variable as the value of one variable increases (Sedgwick 2014, p. 1). The increase, or decrease, in the variable may proceed throughout the range of the measured values but not necessarily at the same rate. Hence, Spearman's correlation is employed in this study to determine whether an increase or decrease in some variables is established from the secondary data set responses. The dataset is not normally distributed and is not measured on a continuous scale. Hence, it cannot be assumed that a linear association exists between them. Therefore, Spearman's correlation is more suitable when a linear association cannot be assumed (Sedgwick 2014, p. 2).

The Spearman's correlation coefficient (ρ) can be obtained from Equation (14.2) for observation without ties (Chalil 2000, p. 14):

$$\rho = 1 - \frac{6 \sum d_j^2}{n^3 - n} \quad [\text{Eqn 14.2}]$$

For observations with ties (which is our case), Equation (14.3) holds as follows (Chalil 2000, p. 11):

$$\rho = \frac{\sum (X_i - X')(Y_i - Y')}{\sqrt{\sum (X_i - X')^2 (Y_i - Y')^2}} \quad [\text{Eqn 14.3}]$$

where d_j is the difference between each of the ranks of the corresponding values of the variables X and Y, and n is the number of pair of values when there is no tied ranks.

■ Results and discussion

Table 14.1 presents the secondary data obtained for the methods of fraud identification.

The results of Fischer's exact statistics and Spearman's correlation for fraud investigation methods are presented in Table 14.2.

The results for Fischer's exact statistics and Spearman's correlation coefficient show that their p -values were significant levels less than 0.05 ($p < 0.05$) at a 95% confidence level (Table 14.2). This implies that the pairs of the identified factors are dependent variables. It means that the rate of cyberfraud perpetration can either increase or decrease by implementing any method of fraud identification.

TABLE 14.1: Methods of fraud identification.

Methods of fraud identification	Response (%) action taken	Response (%) no action taken	Total response (%)
Conducted an investigation or fact-finding	58	42	100
Disclosure to board	41	59	100
Disclosed to regulator or law enforcement	34	66	100
Hired external forensic accountant or specialist	30	70	100
Disclosure to auditor	28	72	100
Preparation of insurance claim	17	83	100
Hiring of external counsel	14	86	100
Disclosure to other stakeholders	12	88	100
Public disclosure or notification	10	90	100

Source: PwC (2020).

TABLE 14.2: Statistical analysis for the pair of significant factors for cyberfraud occurrence and method of identification.

Paired factors	Fischer's exact sig. (2 tailed)	Spearman's correlation coefficient	Relationship
Cyberfraud occurrence and investigation	<0.001	0.868	Positive and strong
Cyberfraud occurrence and disclosure to board	<0.001	0.804	Positive and strong
Cyberfraud occurrence and disclosure to regulator	<0.001	0.934	Positive and strong
Cyberfraud occurrence and external forensic accountant	<0.001	0.977	Positive and strong
Cyberfraud occurrence and disclosure to auditor	<0.001	-0.356	Negative and weak
Cyberfraud occurrence and external counsel	0.004	-0.270	Negative and weak
Cyberfraud occurrence and disclosure to stakeholders	0.016	-0.248	Negative and weak
Cyberfraud occurrence and public disclosure	0.029	-0.223	Negative and weak

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

To further justify that there is a relationship between the dependent variable (rate of cyberfraud occurrence) and the independent variables (investigation, disclosure to board, disclosure to regulator, external forensic accountant, disclosure to auditor, external counsel, disclosure to stakeholders and public disclosure), the cross-tabulation statistical technique was employed, and the results obtained are presented in Table 14.3 and Table 14.4. From Table 14.3 to Table 14.4, the variations between the 'counts' and 'expected counts' in the tables show that the cyberfraud perpetration and its method of identification (taken as the independent variables) variables are dependent. This further lends credence to a relationship between cyberfraud perpetration and its identification method.

The Spearman's correlation coefficient was employed to probe the nature of the relationship between the dependent variable and the independent variables. For Spearman's correlation coefficient, the relationship between the rate of cyberfraud occurrence and speed of investigation, disclosure to the board, disclosure to the regulator and external forensic accountant was positive and strong (Table 14.2). This implies that the rate of cyberfraud may not reduce with an increase in the investigation rate, disclosure to the board and regulator, and the engagement of forensic accountants. This also means that these four identification methods may not significantly influence the reduction of cyberfraud occurrences or cyberfraud mitigation in South Africa. Conversely, the relationship between the rate of cyberfraud occurrence and disclosure to the auditor, external counsel, disclosure to stakeholders and public disclosure was negative but weak. This implies that, to a certain extent, the engagement of an auditor, legal counsel, stakeholders and public disclosures

TABLE 14.3: Cross-tabulation for variables with positive and strong relationship with cyberfraud perpetration.

		Investigation			Disclosure to board			Disclosure to regulator			External forensic accountant		
Cyberfraud		Yes	No	Total	Yes	No	Total	Yes	No	Total	Yes	No	Total
		Yes	Count	31.0	0.0	31.0	31.0	0.0	31.0	31.0	0.0	31.0	30.0
	Expected count	14.9	16.1	31.0	12.7	18.3	31.0	10.5	20.5	31.0	9.3	21.7	31.0
No	Count	17.0	52.0	69.0	10.0	59.0	69.0	3.0	66.0	69.0	0.0	69.0	69.0
	Expected count	33.1	35.9	69.0	28.3	40.7	69.0	23.5	45.5	69.0	20.7	48.3	69.0
Total	Count	48.0	52.0	100.0	41.0	59.0	100.0	34.0	66.0	100.0	30.0	70.0	100.0
	Expected count	48.0	52.0	100.0	41.0	59.0	100.0	34.0	66.0	100.0	30.0	70.0	100.0

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

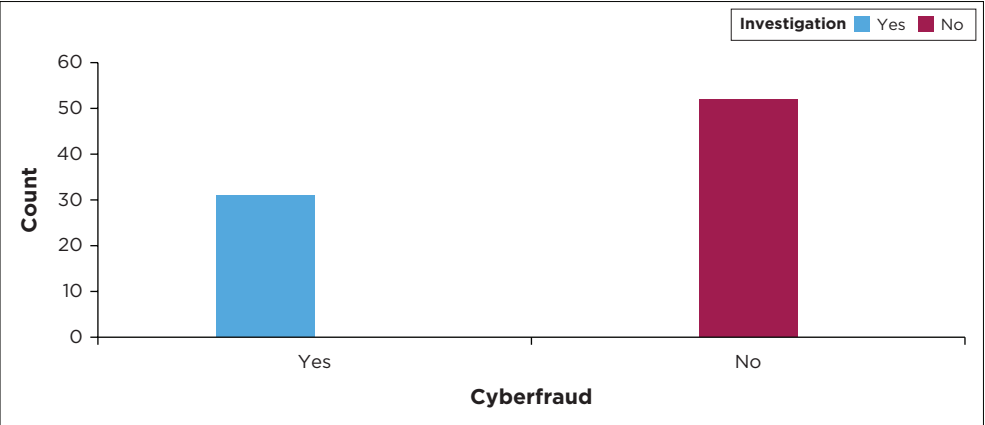
TABLE 14.4: Cross-tabulation for variables with negative but weak relationship with cyberfraud perpetration.

		Auditor			External counsel			Stakeholder's disclosure			Public disclosure		
Cyberfraud		Yes	No	Total	Yes	No	Total	Yes	No	Total	Yes	No	Total
		Yes	Count	31.0	0.0	31.0	0.0	31.0	31.0	0.0	31.0	31.0	0.0
	Expected count	6.8	24.2	31.0	4.3	26.7	31.0	3.7	27.3	31.0	3.1	27.9	31.0
No	Count	22.0	47.0	69.0	14.0	55.0	69.0	12.0	57.0	69.0	10.0	59.0	69.0
	Expected count	15.2	53.8	69.0	9.7	59.3	69.0	8.3	60.7	69.0	6.9	62.1	69.0
Total	Count	22.0	78.0	100.0	14.0	86.0	100.0	12.0	88.0	100.0	10.0	90.0	100.0
	Expected count	22.0	78.0	100.0	14.0	86.0	100.0	12.0	88.0	100.0	10.0	90.0	100.0

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

may promote a reduction in the rate of cyberfraud perpetration or mitigation in South Africa.

The plots of the cross-tabulations for the effect of independent variables (method of fraud identification) on the rate of cyberfraud occurrence are presented in Figure 14.1-Figure 14.8.



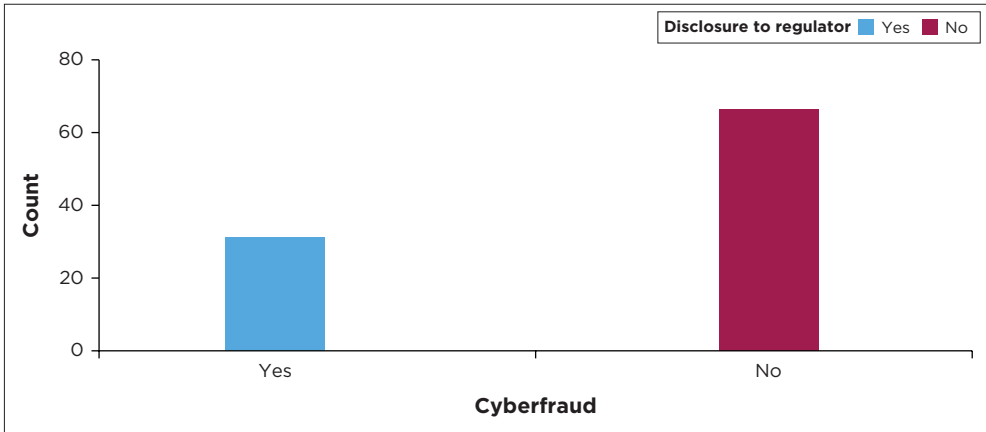
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.1: Cross-tabulation of the effect of investigation on the rate of cyberfraud occurrence.



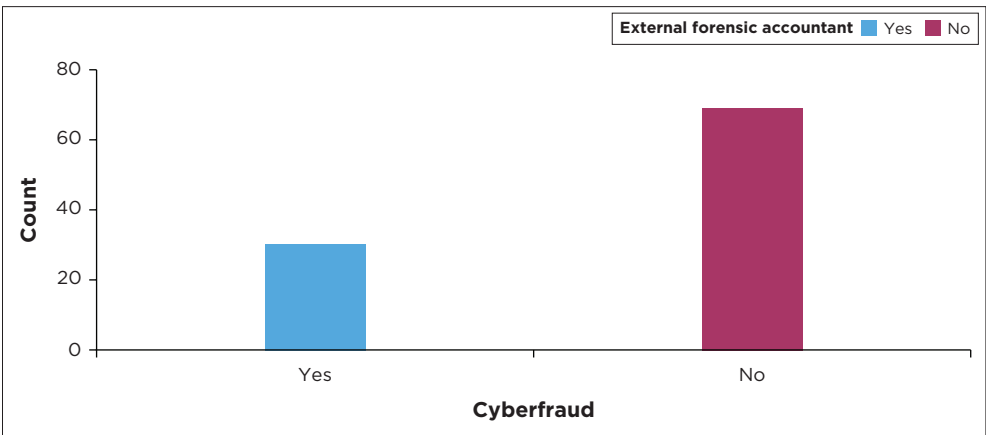
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.2: Cross-tabulation of the effect of disclosure to the board on the rate of cyberfraud occurrence.



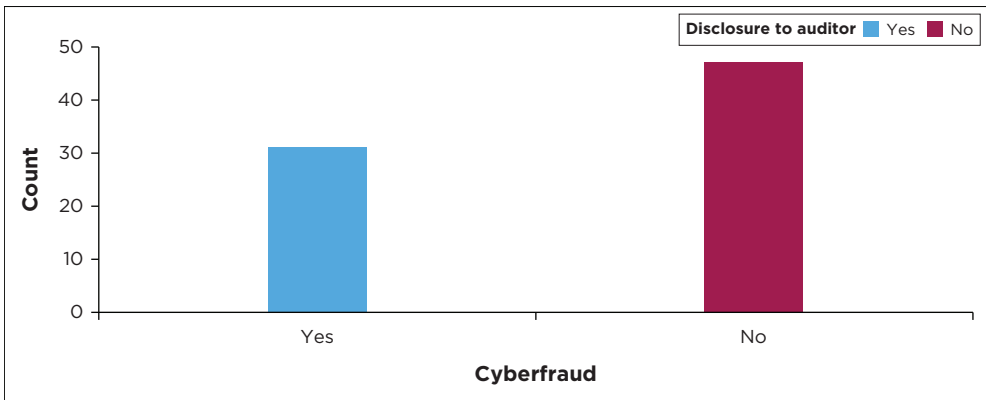
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.3: Cross-tabulation of the effect of disclosure to the regulator on the rate of cyberfraud occurrence.



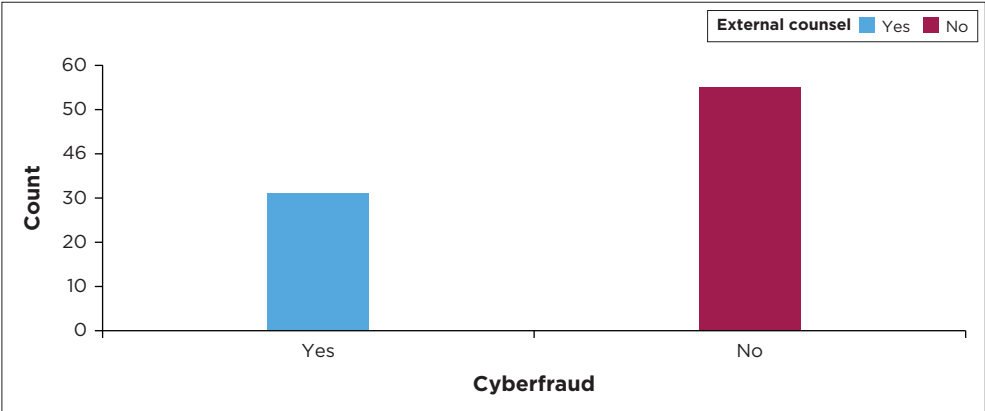
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.4: Cross-tabulation of the effect of disclosure to the regulator on the rate of cyberfraud occurrence.



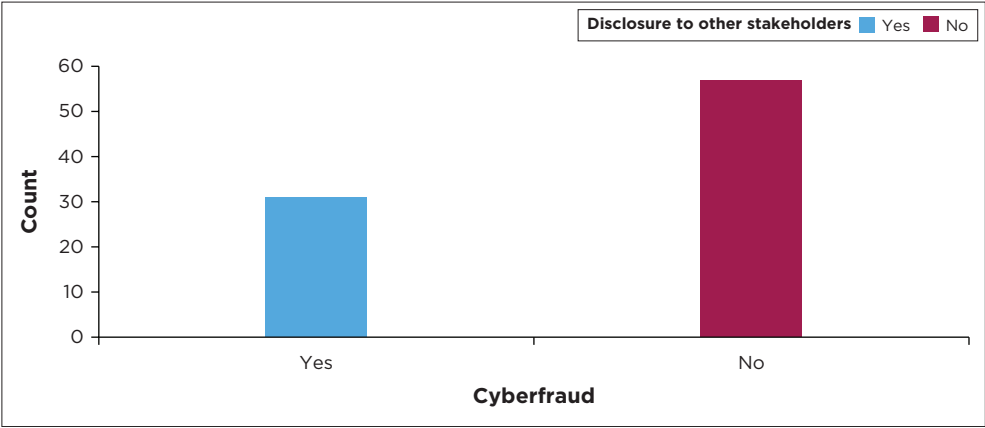
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.5: Cross-tabulation of the effect of disclosure to the auditor on the rate of cyberfraud occurrence.



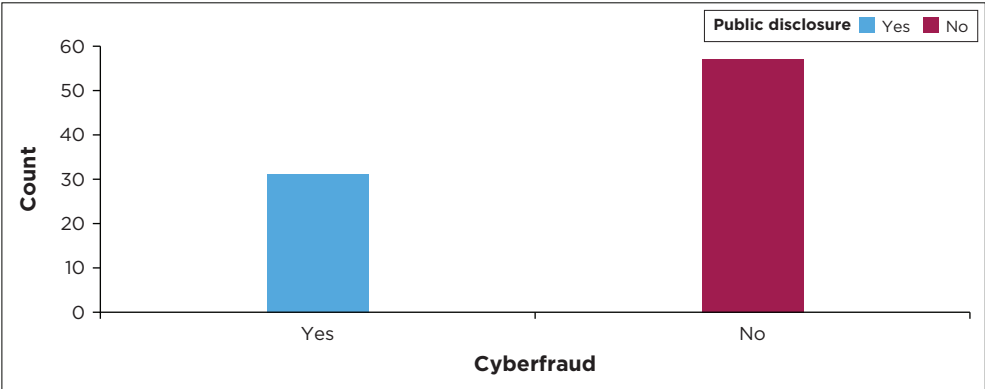
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.6: Cross-tabulation of the effect of external counsel on the rate of cyberfraud occurrence.



Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.7: Cross-tabulation of the effect of disclosure to other stakeholders on the rate of cyberfraud occurrence.



Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.8: Cross-tabulation of the effect of public disclosure on the rate of cyberfraud occurrence.

Suppose an organisation is not investigating cyberfraud or disclosing the outcome of an investigation. In that case, the rate of cyberfraud perpetration or mitigation may increase. In some situations where disclosures are made, it may fall short of what is required for the organisational or other bodies to perform their oversight roles. The PwC (2020) report indicates that poor reporting might result from insufficient information, lack of proper investigation or inconclusive nature of the investigation. The data analysis showed that the cyberfraud investigative processes in South Africa have not contributed significantly to the reduction in cyberfraud perpetration or mitigation.

Da Vinci Cybersecurity (2023) states that investigating cybercrime-related activities in South Africa is becoming increasingly imperative due to the surge in cyberattacks and online crimes that the country continues to experience. In South Africa, cybercrime investigation includes the analysis of network and digital devices to identify and uncover the perpetrators of cybercrimes. In addition, Da Vinci Cybersecurity (2023) further states that in South Africa, the SAPS is the primary government agency responsible for investigating cybercrimes. The SAPS has a dedicated unit, the South African Police Service Computer Crime Unit (SAPS CCU), which collaborates with other law enforcement agencies and the private sector to investigate and prosecute cybercriminals. However, the investigation and prosecution of cybercriminals in South Africa face some challenges. One of these challenges is the lack of resources and skilled personnel. For instance, Da Vinci Cybersecurity (2023) indicates that the SAPS CCU is poorly funded and short-staffed, making it difficult for the unit to investigate and prosecute cybercriminals effectively. This often leads to a backlog of cyber-related cases and a low successful prosecution rate.

Another challenge is the lack of understanding and awareness among the public and law enforcement agencies in South Africa. Many people in South Africa are uninformed about the risks connected to online activities, and many may not even report cybercrimes when they fall victim. This usually makes it difficult to gather evidence and build cases to prosecute cybercriminals. In addition, lack of awareness among mobile banking users regarding the adherence to security guidelines continues to contribute to the surge in the rate of cyberfraud (Arachchilage & Love 2014, p. 304; Balan et al. 2017, pp. 64–65; Cassim 2016, p. 138; Kshetri 2019, p. 78). Dlamini and Modise (2012, p. 1) explain that the South African banking industry needs to prioritise cybersecurity to combat cyberfraud effectively. Although the rate of cyberfraud activities in South Africa is increasing, South Africa has also witnessed some remarkable feats in cybercrime investigations. For instance, Da Vinci Cybersecurity (2023) reports that in 2019, the SAPS CCU arrested a group of hackers responsible for high-profile cyberattacks in the country. The hackers were prosecuted for fraud, extortion and intrusions

into personal and organisational computer systems. In addition, some South African private sector organisations now specialise in cybercrime investigations. These organisations often work with law enforcement agencies and provide resources, DF and expertise that can aid the investigation and prosecution of complex fraud cases. The organisations also offer cybercrime investigation services to individuals and organisations in South Africa through their team of experts trained for collecting, analysing and presenting digital evidence in court to prosecute cybercriminals. Therefore, the involvement of the private sector in organisations can aid the effectiveness of investigations in South Africa. More importantly, individuals and financial institutions in South Africa need to be aware of the risks associated with online activities and to report any cybercrimes they experience promptly (Da Vinci Cybersecurity 2023).

The results of Fischer's exact statistics and Spearman's correlation for the organisation's fraud programme are presented in Table 14.5.

Pricewaterhouscoopers (2020) indicates that, on average, only 55% of South African organisations have formal governance over anti-fraud programmes. Furthermore, only half of the organisations report formal governance over their fraud risk assessments and fewer than that report formal governance over fraud resources. This may contribute to a surge in cyberfraud-related activities.

The results for the Fischer's exact statistics and the Spearman's correlation coefficient for the rate of cyberfraud occurrence in relation to the organisational fraud programme show that their p -values were significant level less than 0,05 at a 95% confidence level (Table 14.6). This implies that the pairs of the identified factors are dependent variables. It means that the rate of cyberfraud perpetration can either increase or decrease by implementing any identified fraud organisational programme.

TABLE 14.5: Organisation's fraud programme.

Organisation's fraud programme	Percentage response (%) Informal or no governance with limited or no budget	Percentage response (%) Formal governance with adequate or prioritised budget	Total percent response (%)
Governance resources	53	47	100
Third-party management	53	47	100
Risk assessment	49	51	100
Training/communication	43	57	100
Monitoring and auditing	42	58	100
Investigations, disciplinary measures and incentives	41	59	100
Policies and procedures	35	65	100

Source: PwC (2020)

TABLE 14.6: The statistical analysis for the pair of the significant factors for cyberfraud occurrence and organisation's fraud programme.

Paired factors	Fischer's exact sig. (2 tailed)	Spearman's correlation coefficient	Relationship
Cyberfraud occurrence and governance resources	<0.001	0.712	Positive and strong
Cyberfraud occurrence and third-party management	<0.001	0.712	Positive and strong
Cyberfraud occurrence and risk assessment	<0.001	0.657	Positive and strong
Cyberfraud occurrence and training and communication	<0.001	-0.772	Positive and strong
Cyberfraud occurrence and monitoring and auditing	<0.001	-0.788	Negative but strong
Cyberfraud occurrence and investigation and incentives	<0.001	-0.804	Negative but strong
Cyberfraud occurrence and policies and procedures	<0.001	0.501	Positive and moderate

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

To further justify that there is a relationship between the dependent variable (rate of cyberfraud occurrence) and the independent variables (governance resources, third-party management, risk assessment, training and communication, monitoring and auditing, investigation and incentives, policies and procedure), the cross-tabulation statistical technique was employed, and the results obtained are presented in Table 14.7 and Table 14.8. From Tables 14.7 to 14.8, the variations between the 'counts' and 'expected counts' in the tables show that the cyberfraud perpetration (dependent variable) and organisational fraud programmes (taken as the independent variables) variables are dependent. This further lends credence to the fact that a relationship may exist between the cyberfraud perpetration and the implementation of the organisational fraud programme in South Africa.

The Spearman's correlation coefficient was employed to probe the nature of the relationship between the dependent variable and the independent variables. For Spearman's correlation coefficient, the relationship between the rate of cyberfraud occurrence and governance resources, third-party management, risk assessment, and policies and procedures was positive and strong (Table 14.6). This implies that the rate of cyberfraud may not reduce with an increase in the rate of governance resources, third-party management, risk assessment, and policies and procedures in South Africa. This also means that these four organisational fraud programmes may not significantly influence the reduction of cyberfraud occurrences or mitigation in South Africa. Conversely, the relationship between the rate of cyberfraud occurrence and training and communication, monitoring and auditing, investigation and incentives was negative but strong. This implies that, to a large extent, implementing

TABLE 14.7: Cross-tabulation for variables with positive and strong relationships with cyberfraud perpetration.

			Governance resources			Third-party management			Risk assessment			Policies and procedures		
			Yes	No	Total	Yes	No	Total	Yes	No	Total	Yes	No	Total
Cyberfraud	Yes	Count	31	0	31	31	0	31	31	0	31	31	0	31
		Expected count	14.6	16.4	31.0	14.6	16.4	31.0	15.8	15.2	31.0	20.2	10.9	31.0
	No	Count	16	53	69	16	53	69	20	49	69	34	35	69
		Expected count	32.4	36.6	69.0	32.4	36.6	69.0	35.2	33.8	69.0	44.8	24.2	69.0
TOTAL		Count	47	53	100	41	47	53	51	49	100	65	35	100
		Expected count	48.0	53.0	100.0	41	48.0	53.0	51.0	49.0	100.0	64.0	36.0	100.0

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

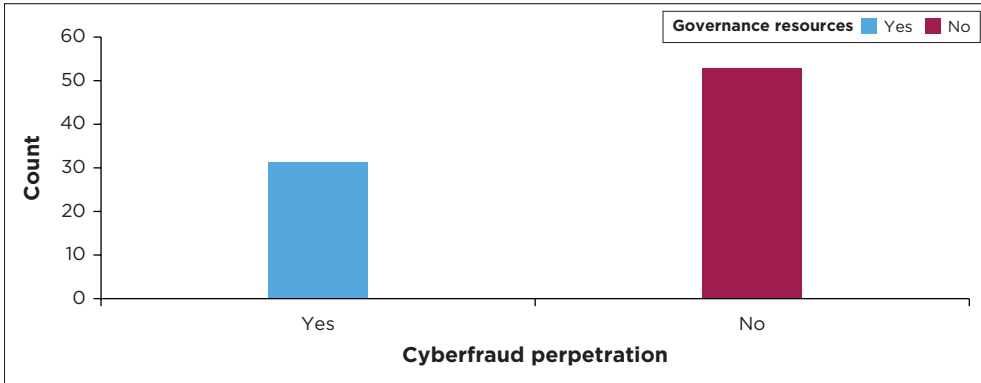
TABLE 14.8: Cross-tabulation for variables with negative and strong relationships with cyberfraud perpetration.

			Training and communication			Monitoring and auditing			Investigation and incentives		
			Yes	No	Total	Yes	No	Total	Yes	No	Total
Cyberfraud	Yes	Count	0	31	31	0	31	31	0	31	31
		Expected count	17.7	13.3	31.0	18.0	13.0	31.0	18.3	12.7	31.0
	No	Count	57	12	69	58	11	69	59	10	69
		Expected count	39.3	29.7	69.0	40.0	29.0	69.0	40.7	28.3	69.0
Total		Count	57	43	100	58	42	100	59	41	100
		Expected count	57.0	43.0	100.0	58.0	42.0	100.0	59.0	41.0	100.0

Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

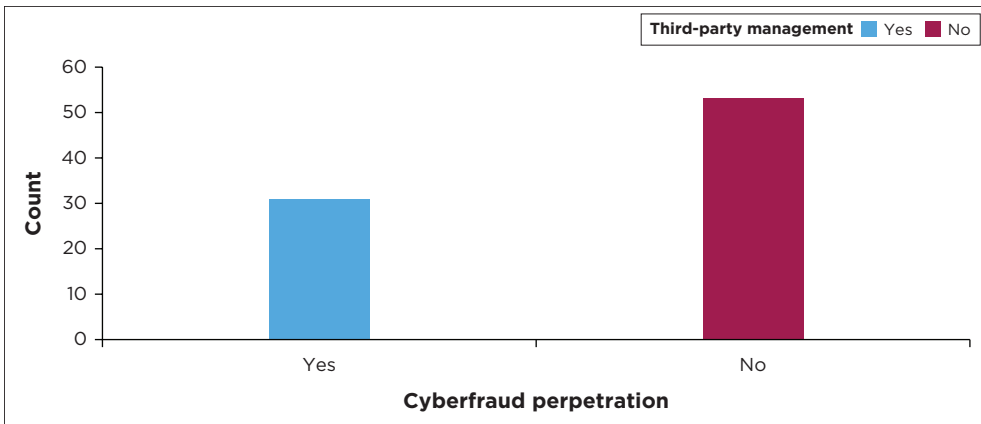
organisational fraud programmes such as training and communication, monitoring and auditing, investigation, and incentives may promote reduced cyberfraud perpetration or mitigation in South Africa.

The plots of the cross-tabulations for the effect of independent variables (organisational fraud programme) on the rate of cyberfraud occurrence are presented in Figure 14.9–Figure 14.15.



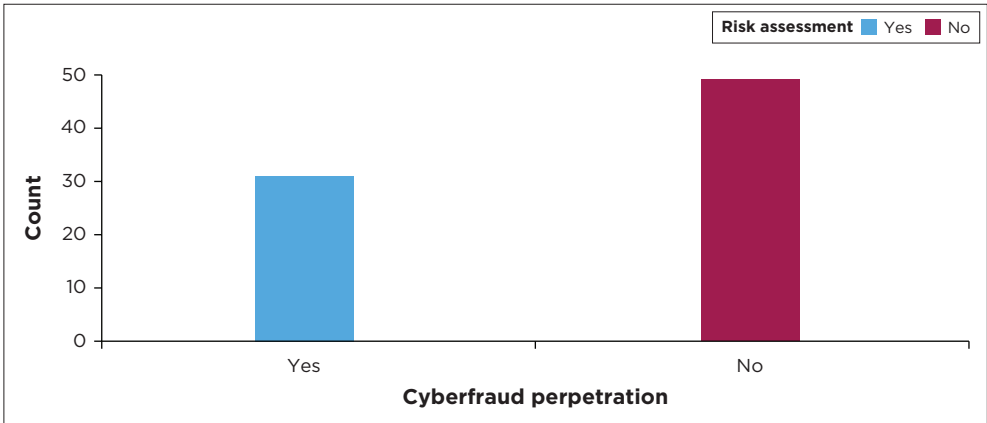
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.9: Cross-tabulation of the effect of governance resources on the rate of cyberfraud perpetration.



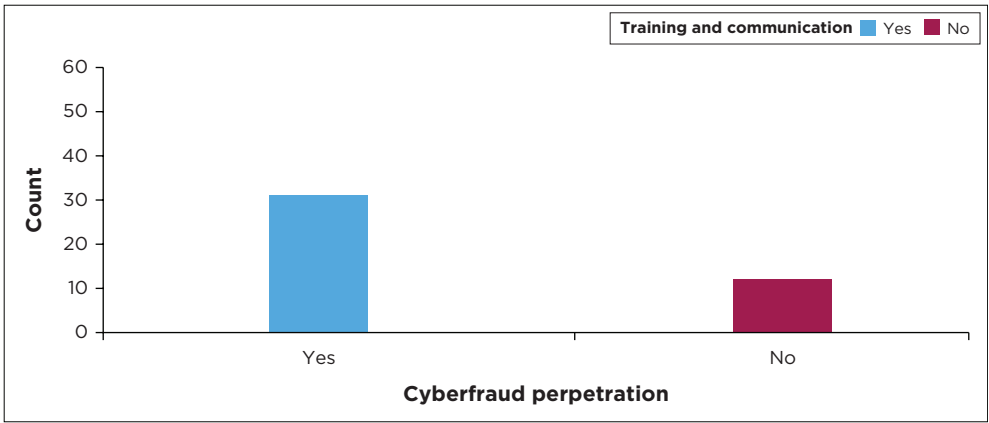
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.10: Cross-tabulation of the effect of third-party management on the rate of cyberfraud perpetration.



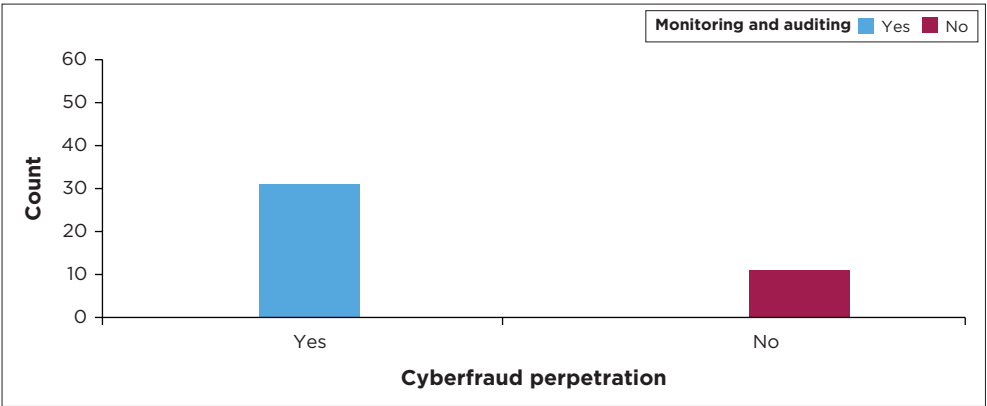
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.11: Cross-tabulation of the effect of risk assessment on the rate of cyberfraud perpetration.



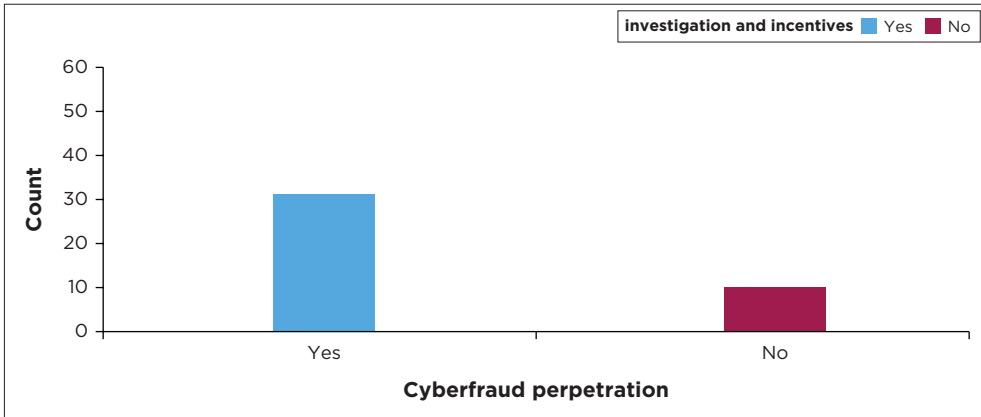
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.12: Cross-tabulation of the effect of training and communication on the rate of cyberfraud occurrence.



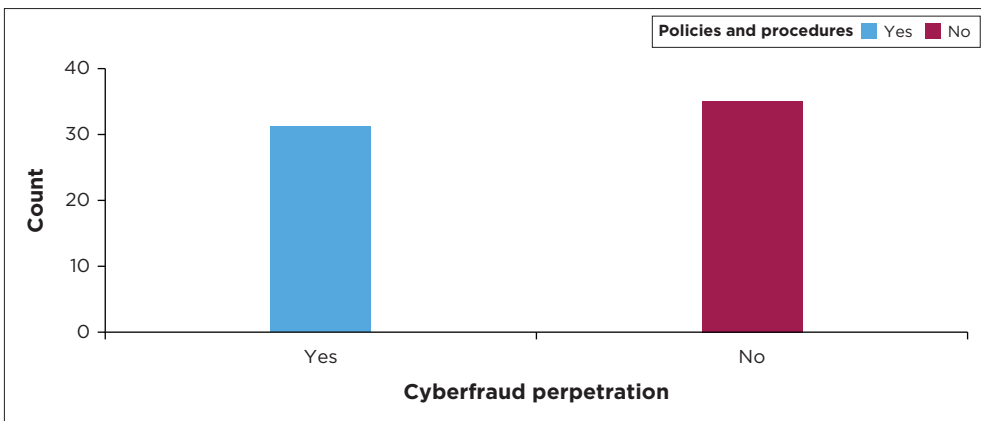
Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.13: Cross-tabulation of the effect of monitoring and auditing on the rate of cyberfraud occurrence.



Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.14: Cross-tabulation of the effect of investigation and incentives on the rate of cyberfraud occurrence.



Source: Statistical analysis obtained from SPSS (version 2022 developed by IBM).

FIGURE 14.15: Cross-tabulation of the effect of policies and procedures on other stakeholders on the rate of cyberfraud occurrence.

The statistical analysis presented in Table 14.6 shows that the organisational resources in South Africa are still not at the level where they can ensure effective mitigation of cyberfraud. Dzomira (2014, p. 16) identifies a lack of resources as one of the factors affecting the sustainable fight against cyberfraud occurrences. To achieve a sustainable fight against cyberfraud, an organisational MCS can be designed to obtain information and assess the performance of all organisation's physical, human and financial resources concerning cyberfraud mitigation. There is a need to ensure the optimum utilisation of the organisation's resources through effective internal control and information systems. Thus, management must ensure

resource availability and effective allocation to assess, mitigate and evaluate risk. Furthermore, the commitment of the organisation's resources to information security and cyberfraud detection is meagre (PwC Crime Survey 2016, p. 14).

Dlamini and Mbambo (2019, pp. 1, 2) state that South Africa lacks human resources (police officials) and the expertise to adequately implement policy and combat cybercrime.

The report of the Barclays Africa Group Limited (2017a, p. 14) in South Africa indicates that emerging digital technologies have increased the scarcity of human resources in data analysis, IT and risk management. To tackle the challenges of cyberinsecurity, ABSA continues to invest in human capacity development and recruitment of employees who specialises in IT, data analytics and cybersecurity (Barclays Africa Group Ltd. 2017b, p. 39). The banks also stressed the need for effective collaborations among the relevant stakeholders to sustain the fight against cyberfraud (Barclays Africa Group Ltd. 2017b, p. 35).

The FirstRand Group (FNB) in South Africa reports that their investment in human capacity development increased by 240% in 2017 (FirstRand Group Ltd. 2017, p. 9). Makgatho (2013, p. 97) explains that organisations can achieve a successful fraud investigation as well as an efficient allocation and monitoring of financial resources only if an effective internal control system is put in place. The findings agree significantly with the AICPA's (2012) position that the internal control measure is a significant player in monitoring, detecting and preventing fraud through enforcing internal controls.

Regarding third-party management of cyberfraud-related risks, Kopp, Kaffenberger and Wilson (2017, p. 13) state that this risk transfer strategy can be implemented at the management level. It involves buying cyber liability insurance or transferring the risks associated with the business operations to a third-party service provider through outsourcing. Outsourcing third-party vendors or service providers to handle cyberfraud risks can assist in analysing and reducing cyberfraud. Financial institutions which do not have the required expertise to combat cyberfraud-related threats may consider outsourcing it. However, the organisation may be vulnerable when third-party risk management services are not as expected. The statistical analysis in Table 14.6 shows that the third-party management of cyberfraud-related risks in South Africa needs to be upgraded to minimise cyberfraud-related risks.

A risk is the probability that a threat will adversely affect an organisation (Stoneburner, Goguen & Feringa 2002, p. 8). Thus, risk management is an essential factor of an organisation's strategic decision-making system that

ensures that the organisation's objectives follow the proper risk-mitigation approach (Boateng et al. 2014, p. 43; Hopkin 2010, p. 47). In the opinion of Hopkin (2010, p. 3), risk management is an approach by which the various risks faced by an organisation are identified, measured, analysed, monitored and managed effectively. The dynamic nature of business and the business environment demand that strategies be put in place to minimise the effect of risk so that the organisation's objectives are not jeopardised. Risk is associated with every business, but if adequately assessed and managed, it might not affect the organisation's objectives (Hopkin 2010, p. 3). Otherwise, it can eventually result in poor operational efficiency, poor financial performance and the inability of the organisation to meet the set goals (Hopkin 2010, p. 5; Mohammed & Knapkova 2016, pp. 271-272).

Stoneburner et al. (2002, p. 4) indicate that risk management is one of the primary responsibilities of an organisation's management, which involves acquiring and deploying all the resources required to identify, assess and mitigate risk. Furthermore, the risk management procedures must also be integrated into the organisational strategic decision-making (Stoneburner et al. 2002, p. 6). Kopp et al. (2017, p. 6) agree that risk management is multifaceted and should not be left for the management only; rather, it should be perceived as a collective responsibility of all the organisation's stakeholders.

According to Stoneburner et al. (2002, p. 4), risk management comprises three major phases: risk assessment, analysis, control and evaluation. Risk assessment is the first phase of any risk management procedure (Stoneburner et al. 2002, p. 8). This involves identifying and evaluating all the potential threats that can affect an organisation. The risk analysis determines the risk level and the extent to which each identified risk can affect an organisation. At the risk analysis phase, the possibility of the occurrence of the threat and the impact on the organisation is verified. Therefore, the outcome of this phase will be used as input into the next phase of control and evaluation to identify the appropriate control measures for risk mitigation). The control stage is essential for mitigating the risk occurrence or reducing the impact of the risk occurrence. According to Stoneburner et al. (2002, p. 8), the effect of risk is the extent of damage caused by an adverse occurrence, and the impact level can be reduced through proper risk assessment and implementation of control measures. According to Stoneburner et al. (2002, p. 4) and Hopkin (2010, p. 3), risk management is a systematic process to identify, assess, control and evaluate risks.

In fraud mitigation, risk assessment involves identifying and evaluating the opportunities, pressure and incentives to commit fraud. This is necessary

to protect an organisation and its stakeholders from being victims of fraud. Hopkin (2010, p. 255) states that fraud risk management comprises the set of activities directed toward identifying potential risks in business processes and developing action plans to minimise or mitigate the identified threats. Some action plans include preventive, corrective, directive and detective control measures (Hopkin 2010, p. 255).

Fraud identification is connected to fraud detection involving activities to establish a fraud case after fraud occurrence (KPMG 2010, p. 24). On the contrary, fraud assessment is essentially to investigate the extent and impact of such risk on the organisation and the stakeholders. Furthermore, fraud control comprises proactive or reactive measures to prevent or minimise the impact risk, while the evaluation phase reviews the effectiveness of the preceding phases and control measures employed. Richards, Melancon and Ratley (2019, p. 7) state that fraud risk management processes must be aligned to the organisational structure (such as the size, complexity and goals) and should be implemented and reviewed regularly. Hasham, Joshi and Mikkelsen (2019, pp. 4–9) attempted to classify cyberfraud risk control processes into three significant steps: customers' identification and authentication, transaction monitoring and anomaly detection and swift response to cyberattacks.

Financial institutions face diverse risks; however, effectively mitigating them is vital to their overall performance. According to the risk taxonomy developed by Leo, Sharma and Maddulety (2019, p. 4), fraud risk is classified under operational risk. This is because operational risk encompasses the risk of loss that could arise due to the failure of an internal system or other external occurrences (Leo et al. 2019, p. 3).

Kopp et al. (2017, p. 13) explain that cyberfraud risk management is essential for ensuring the relevance and effectiveness of cybersecurity-related measures in relation to the underlying risk. Hence, organisations must decide on the risk management approach based on the nature of the risk they are vulnerable to. After that, the risks must be identified, assessed and evaluated through risk reduction, transfer, and avoidance approaches depending on the outcome of the assessment (Kopp et al. 2017, p. 7). Thus, the development of internal risk management processes and controls can be a valuable strategy to protect the organisational and the stakeholders from the impact of fraud risk. While developing internal risk management processes and controls, Kopp et al. (2017, p. 10) identify the phases of cyberfraud occurrence that should be considered. These include the prevention, reaction, mitigation, impact management, and recovery or remediation phases.

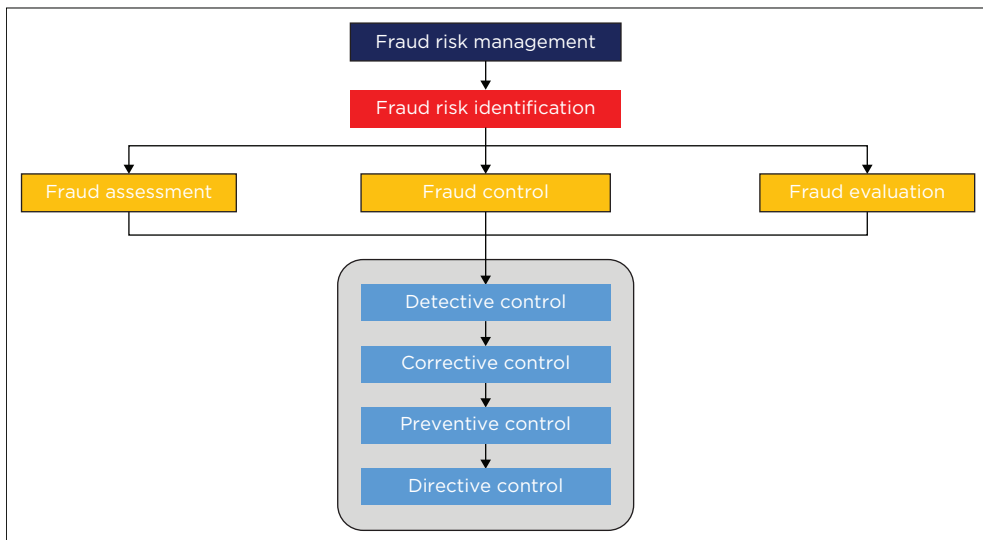
The prevention phase comprises securing organisational systems and data from cyberattacks. On the other hand, the reaction phase encompasses

all the activities that follow the occurrence of a cyberattack. It may include an initial forensic analysis, measures to prevent further intrusion into the organisation's system or information and the system's recovery. At this phase, communications are initiated with the stakeholders, legal team and the public to sensitise them about the fraud incidence. The impact management phase comprises the activities aimed at addressing the direct or indirect impacts of the cyberattack on the organisation, stakeholders and the general public. At this phase, some measures may be implemented to safeguard the organisation's infrastructure and processes and extract the required evidence for forensic investigation and litigation (Deloitte 2016).

The business recovery or remediation phase concerns reconfiguring or repairing the affected infrastructure to forestall future cyberattacks. The efforts at this stage involve reconfiguring or designing the organisation's information systems and business processes, renewing damaged relationships and goodwill, and investing in proactive security measures and technological competencies to prevent a future occurrence (Kopp et al. 2017, p. 11).

Figure 14.16 presents the link among fraud control, risk assessment, risk management and fraud investigation. The figure clearly shows that fraud risk management is incomplete without fraud control.

Fraud control is necessary because it guards against deviation from everyday activities and is essential in correcting suspected anomalies. Fraudulent activities will increase without implementing fraud control



Source: Authors' compilation design based on Hopkin (2010, p. 255).

FIGURE 14.16: Link between fraud control, risk assessment, risk management and investigation.

measures (Hopkin 2010, p. 236). Fraud control can be preventive or detective in nature investigation (Hopkin 2010, p. 255). Preventive control is a control process to defend the organisation against fraud occurrences, while detective control is usually employed to uncover fraudulent processes whenever the preventive measure fails. To avoid failure of the preventive measure, the risk assessment processes must be effective so that potential risks are identified and dealt with accordingly.

From Figure 14.16, the fraud management process starts with fraud risk identification (identification of the threats that can lead to fraud). After that, the identified threats can be assessed to determine the risk levels and impact before fraud control techniques can be employed for mitigation. Fraud control techniques can be preventive, detective, corrective and directive. The type of control used can be determined by the nature of the business environment, the kind of fraud the business is vulnerable to and the nature of potential evidence that can be gathered during the investigation. In this regard, Hopkin (2010, p. 255) stated that preventive measures can minimise or eliminate the source of the risks. For instance, as part of fraud preventive measures, an organisation can practice separation of duties, access control and limit the authorisation by staff. The detective measure can employ technologies for identifying fraud indicators to establish a fraud case. At this stage, fraud identification can also be through periodic auditing, reviews or whistleblowing.

The corrective measure is aimed at containing the risk level. Depending on the fraud case established, corrective measures can be in the form of staff rotation access controls in the organisation's system, among others. On the other hand, directive control is usually a policy framework aimed at averting future occurrences. Human capacity development, staff supervision and absolute compliance with standard regulations and procedures (Hopkin 2010, p. 255). Some control initiatives that fall under the directive control initiatives include risk reduction, risk avoidance and risk transfer. Risk reduction can be practised to minimise the chances and impact of a risk to a permissible level (Hopkin 2010, pp. 255–256). This could be by implementing security measures such as physical restrictions to the organisation's facilities or information, use of security software or human control measures (Kopp et al. 2017, p. 13).

The risk avoidance strategy includes a series of activities implemented by the organisation's management to prevent the occurrence of a potential threat. It may consist of redesigning activities, services and process pathways, change in the organisation's business model, or change in access controls. The risk transfer strategy involves buying cyber liability insurance or transferring the risks connected with the business operations to a third-party service provider through outsourcing. Organisations with inadequate

resources and capacity expertise to fight cyberfraud-related risks may consider outsourcing it to a third-party. However, when the third-party risk management service is not provided to the level expected, the organisation may be vulnerable to the risk.

According to Kopp et al. (2017, p. 14), cyber insurance *can help mitigate cyber-related risks by providing* implementable solutions to the problem of information and cybersecurity. Through cyber risk transfer, an organisation can be assisted in developing a robust cyber defence, thereby increasing transparency in an organisation's activities.

In terms of cyberfraud, as it relates to this study, fraud risk management involves the activities aimed at identifying and developing activities to minimise the risks resulting from potential or actual cyberfraud cases. 'It includes preventive, corrective, directive and detective control measures with the appropriate feedback where necessary' (Hopkin 2010, p. 255 in Akinbowale, Klingelhöfer & Zerihun 2023, p. 4).

■ Conclusion

Cyberfraud risks constitute a threat to the operations of the banking industries globally. Thus, this aimed to investigate the effectiveness of some MCS strategies employed for cyberfraud mitigation by the South African banking industry. This was achieved using secondary data related to the fraud identification methods and organisational fraud programme. Furthermore, a statistical analysis such as Spearman's correlation, cross-tabulation and Fischer's exact non-parametric statics were carried out in the SPSS 2022 environment to determine the relationship between the rate of cyberfraud occurrence (dependent variable) and the methods of fraud identification and the organisation's fraud programme (independent variable). The results indicated that the rate of cyberfraud occurrence in South Africa might not reduce with an increase in the investigation rate, disclosure to the board and regulator and the engagement of forensic accountants.

Conversely, the results also show that, to a certain extent, the engagement of an auditor, legal counsel, stakeholders and public disclosures may promote a reduction in the rate of cyberfraud perpetration or mitigation in South Africa. The results further show that the rate of cyberfraud may not reduce with an increase in the rate of governance resources, third-party management, risk assessment and policies and procedures in South Africa. On the other hand, the findings indicate that, to a large extent, implementing organisational fraud programmes such as training and communication, monitoring and auditing, investigation and incentives may promote reduced cyberfraud perpetration or mitigation in South Africa. This implies that for

the fight against cyberfraud to be effective and sustainable in South Africa, the banking industry needs to improve significantly in the areas of fraud investigation, disclosure to board and regulator, engagement of forensic accountants, governance resources, third-party management, risk assessment as well as policies and procedures among others. The findings in this study may assist financial institutions in identifying the areas that need improvement concerning the methods of fraud identification and organisational fraud programme. The study also adds to understanding MCS strategies for effective cyberfraud mitigation.

Policy lessons

■ Introduction

This last chapter elucidates the policy lessons on cyberfraud perpetration and the mitigation approach that both emerging and developed economies can implement. As cyberfraud is a global occurrence, it is necessary to implement specific organisational and governmental policies to contain it. This chapter provides insight into implementable cyberfraud mitigation strategies and the practical guidelines for developing cyber-resilient plans. Cyberfraud remains a major threat to both advanced and emerging economies. Thus, there is a need for organisations and countries to step up their fight against cyberfraud and make it more proactive and sustainable. This will reduce the impact of cyberfraud on organisational profitability, customer satisfaction, shareholders, the global economy and reputation. Both economies must also adjust existing policies, internal and management controls and business models to capture newly developed anti-fraud technologies and cyber resilience strategies for mitigating cyberfraud.

■ Policy lessons for combatting and mitigation strategies

Cyberfraud is a global challenge that threatens both emerging and developed economies. Cyberfraud incidents have been summarised as

How to cite: Akinbowale, OE, Mashigo, MP & Zerihun, MF 2024, 'Policy lessons', in *Understanding and mitigating cyberfraud in Africa*, AVARSITY Books, Cape Town, pp. 301-310. <https://doi.org/10.4102/aosis.2024.BK485.15>

attacks against personal or organisational confidentiality, data, computer or systems or other computer-related offences. The attack is usually dependent on or enabled by the Internet and IT communication infrastructure:

For effective mitigation of cyberfraud, the following are necessary, among others.

The development of proactive cybersecurity measures for protecting organisational systems and databases with a performance measurement and evaluation system. Cybersecurity planning should incorporate a security strategy which indicates an organisation's commitment to cybersecurity and provides direction for cybersecurity. This security policy addresses management, personnel, clients, operational and technical issues as well as enforcement of the agency security measures, clarity relating to decision-making, roles and responsibilities, cybersecurity strategies, risk mitigation, response and recovery plans, consistent evaluation and monitoring, training and creating awareness for the clients and employees.

It is also necessary to identify the existing techniques and strategies employed by the organisation for mitigating cyberfraud and ascertain loopholes in the current cyberfraud mitigation techniques or strategies used. This will enable the organisation to develop a compatible new technique capable of providing a solution to the identified loophole. There is a need for increased effectiveness in the investigative process, prosecution and adjudication of cybercrime. Digital technologies such as artificial intelligence (AI), big data technology and data analytics, such as data-mining, can aid the investigative process.

Furthermore, there is a need for holistic government involvement in cyberfraud mitigation. This includes coordinating cyberfraud mitigation efforts at all levels of government data collection. This may include the development of legal frameworks encompassing the passage and implementation of laws that prohibit cyberfraud and promote information, data and cybersecurity. It may also include passing laws that encourage sustainable response and greater deterrence to cyberfraud. In addition, collaborations geared towards mitigating cyberfraud-related risks should be strengthened at the national, regional and international levels. This may include communication among government, law enforcement agencies, financial institutions, the private sector and other stakeholders battling fraud.

Lastly, financial institutions need to take responsibility for tackling cyberfraud. This may include the development of robust internal controls and MCSs for implementing and monitoring cyberfraud mitigation approaches. The controls should also incorporate human capacity development initiatives to promote effective deployment of anti-fraud

technologies by personnel. The controls can also consider increased public awareness about cyberfraud risks and implementing a real-time alert system capable of informing customers and organisations about impending cyberattacks.

■ Policy lessons on minimising economic welfare impacts

Cyberfraud perpetration affects financial organisations in terms of disruption of business activities, increases in the downtime of the organisation's ICT systems, destruction of the organisation's ICT infrastructure, and loss of profitability, productivity and reputation, among others. The cost of cyberfraud on the global economy can be categorised as direct and indirect. Direct cost relates to the cost incurred because of cyberfraud occurrences, such as the cost of investigation, loss of revenue, cost of litigation, cost of systems or data recovery, cost of compensation, cost of cyberfraud insurance, and other cost incurred to strengthen cybersecurity after cyberfraud perpetration occurrence. On the other hand, indirect cost relates to the cost incurred because of reputational loss, adverse effects of cyberfraud on brands, the organisation's name, loss of customer relationships, and loss of public trust and goodwill.

The cost of cyberfraud affects the economic welfare of people globally. Financial institutions are the central backbone of any nation's economy. Thus, any disruption caused to their infrastructure, customers and operations will negatively affect the country's economy. This will also increase certain risks and vulnerabilities such as the fiscal deficit, decline in revenues, increase in the public debt profiles, unemployment, increase in government expenditure, increase in the risk of public debt and the risk of insolvency by the financial sector and the national economy, among others. At the macroeconomy level, the financial institutions' support in job creation, development of vital infrastructure and sustainable development may also suffer significant setbacks. For instance, the direct cost incurred because of cyberfraud perpetration could be used to enhance people's economic and social well-being. Furthermore, financial flows may be affected because of cyberattacks and organisations, especially small and medium-sized enterprises that depend on loans or subsidies from financial institutions, may be grossly affected. Sometimes, financial institution personnel are relieved of their jobs because of cyberattacks, which may cause the rate of unemployment and other social pressures to increase. In addition, when financial institutions incur losses because of cyberattacks, they may invest more in cybersecurity and upgrade existing technology and security infrastructure. This may also affect the availability of funds for sustainable projects that can promote the collective well-being of society.

To minimise the effect of cyberfraud on the national and global economies, there is a need for financial institutions to become more resilient to cyberattacks. Cyber resilience includes the organisation's ability to constantly strengthen its cyber defence and approach to cyberfraud mitigation amidst cyber threats. Some of an organisation's cyber-resilient attributes include minimal disruptions, information security alignment, business continuity and organisational adaptability. Organisations must monitor authorised and unauthorised devices and software inventory to achieve cyber resilience. Developing and managing configurations for all systems and devices are also necessary. Furthermore, there is a need to conduct continuous vulnerability assessment and remediation for all systems and operations. In addition, organisations need to develop effective internal and MCSs to manage and control both internal and external sources of threats.

The following steps summarise the cyber resilience plans an organisation can develop and implement to counter cyberfraud.

The first step in developing cyber resilience plans is identifying systems' vulnerabilities. To achieve this, there is a need to continuously scan the entire organisation's IT architecture. This includes the organisation's computers, servers, endpoints and cloud applications. This can foster early detection and maintenance of any loophole, securing the organisation's IT assets. It also reduces their vulnerability to cyberattacks before the threat actors exploit any loophole in them for cyberfraud perpetration. The second step is safeguarding the organisation's system. To implement this step, financial institutions can have endpoint protection solutions to prevent intrusion into their systems. The endpoint protections, alongside other digital anti-fraud technologies, can automatically block intrusions without affecting the normal routine operational activities of the organisation.

The third step is to detect cyber threats early. Before any cyber threat culminates into a significant cyberattack or security breach, detection technologies such as AI or other threat detectors must be put in place to detect potential threats so that they can be nipped in the bud before they escalate into cyberattacks. The fourth step is to respond swiftly to cyber threats or cyberattacks. In any event of detection of cyber threats or cyberattacks, the response to curtail it must be swift. There is a need to develop an effective response plan to mitigate cyber threats or cyberattacks without disrupting normal business activities. The longer it takes to contain cyberattacks, the costlier it becomes.

The fifth step is to have an effective recovery plan. An organisation must effectively recover the systems, files, information, database or website from the threat actors. Failure to do this may culminate in continuous intrusion and cyberfraud perpetration by the threat actors or the constant

demand for ransom. Threat actors are becoming more sophisticated in hacking and intruding into an organisation's information and security architecture to pave the way for continuous exploitation. To tackle this, firstly, an organisation must ensure that critical endpoints, systems, and servers are continuously backed up. Backing up will minimise losses and make recovering the infiltrated infrastructure easy. Secondly, it makes it easy to prevent further intrusion by the threat actors.

The sixth step is to sensitise the employees and the public. Educating employees and public awareness about cyberattack strategies is a necessary step in developing a cyber resilience plan. This could be through training on preventive or response strategies and risk mitigation. As some of the anti-fraud technologies are emerging coupled with the dynamics of cyberspace and the operation of cyberattackers, there is a need for regular training of employees to ensure strict adherence to standard practices, the effective use of software and emerging technologies and to keep updated data regarding the trends relating to cybersecurity.

The seventh step is to commit resources and implement cyber resilience plans beyond merely developing the cyber resilience plans to implement them. There is a need to commit resources and ensure the translation of the plans into purposeful actions targeted at cyberfraud mitigation. Otherwise, it will remain a mere blueprint.

The eighth and last step is to measure the performance of cyber resilience plans and review them periodically. Following the cyber resilience plans, an organisation needs to implement a system of performance measurements, such as a balanced scorecard, to identify areas where the target is met in line with the organisation's goal of cyberfraud mitigation and areas that require improvement. Based on this, periodic reviews can be undertaken, and corrective actions will be taken.

■ Lessons for African economies

The African continent is a unique continent because of the increasing population and increasing rate in the number of Internet users. The population has been projected to grow in the coming years. This implies increased Internet users and the rate of cybercrime perpetration if the stakeholders do not take urgent steps to prevent the surge. With the current population and the projections, Africa will be the fastest-growing continent regarding Internet penetration and mobile-based financial services. As such, the continent could also become an increasingly attractive region for cybercriminals. Although cyberfraud awareness is gaining momentum in African countries, the success rate is still low regarding the prosecution of cybercriminals, the rate of successfully blocked attacks, and

the rate of law and policy implementation that promotes cybersecurity. Thus, cyberfraud remains one of the top risk factors that can endanger Africa's economy. The continent is developing blueprints to fully transit into e-commerce under the Africa Continental Free Trade Area (AfCFTA). Still, cyberfraud remains a threat to effective transitioning into e-commerce. One significant challenge that has slowed down the sustainability of cyberfraud mitigation in Africa is the lack of synergy at the international and regional levels. Many African countries have made appreciable progress at national levels to contain cyberfraud, but winning the fight against cyberfraud goes beyond national levels as the crime itself is borderless. Many domestic regulations on Internet use in Africa do not consider the global nature of crime and the universal nature of cyberspace exploited by the threat actors for cyberfraud perpetration. The e-commerce and the increasing population of the continent can be potential catalysts for economic growth if the issue of cybersecurity is fixed.

Thus, the following are recommended as part of the measures to make the fight against cyberfraud in African countries more effective.

African governments, financial institutions and all the stakeholders in the fight against cyberfraud should implement the standard cyber norms and international laws that govern people's behaviour in cyberspace. This is a good step towards achieving cybersecurity, which is necessary for online financial or economic transactions. However, there is a need to ensure that the cyber laws enacted are combative and not excessively restrictive. For instance, when the laws and measures implemented by African countries are too strict and restrictive, people may underutilise cyberspace for economic activities, and it will become counterproductive. Thus, there is a need to develop and implement policies that will strike the right balance between cyber governance, cybersecurity and economic viability as the continent transitions into a digital economy. Implementing strict, restrictive laws or measures can affect the continent's digital economy and businesses. It can also discourage foreign investment and impact the customers' digital services. Beyond the enactment of the laws and measures is implementation. African countries should move beyond mere proposals to implement the enacted laws and measures fully, as this will sustain Africa's drive towards a fully digital economy.

Some African countries already have laws and policies on cybersecurity, but the challenge remains the implementation. Therefore, efforts must be geared towards capacity-building and operationalising existing cybersecurity laws and policies. Some of the laws and policies enacted by African countries can no longer sustain the fight against cyberfraud because of the dynamics of cyberspace, economic trends and the sophistication of cyberattackers. Thus, reviewing and updating existing laws and policies will be beneficial in

effectively combatting cyberfraud. Law enforcement agencies, investigators, attorneys and judges should also fulfil their part as stipulated by law. The personnel combatting cyberfraud and those investigating and prosecuting cyberfraudsters must acquire up-to-date technical and legal skills. They also need to develop tools to make their work more effective.

Another important issue worth considering is the ratification of the Malabo Convention conveyed by the African Union on cybersecurity and personal data protection to fight cybersecurity threats. The Malabo Convention on Cybersecurity and Personal Data Protection could promote cybersecurity if implemented. However, the process of ratification of the agreement is slow.

Furthermore, there is an urgent need for the financial institutions, government and private sector to address some loopholes mitigating the fight against cyberfraud. These include the nonimplementation of recent technological advances, lack of resources (skilled personnel, financial and material resources), low-level enforcement of cybercrime laws and inadequate sensitisation.

Finally, cyberfraud is borderless; it can be carried out anywhere in the world if there is a connection to cyberspace. Thus, there is a need for effective synergy at the national, regional and international levels.

■ **Lessons from emerging and developed economies**

Cyberfraud is still a significant threat to both advanced and emerging economies. It continues to affect the organisation's shareholders, profitability, efficiency and reputation of many financial institutions. Emerging economies have a growing Internet penetration rate and significant growth of innovative and mobile device users. With the ever-increasing digital evolution, emerging economies are more susceptible to cyber risks threatening their financial and economic development. Africa currently leads the world in digital finance, thus making the region prone to cyberattacks. Although both the emerging and advanced economies are deploying countermeasures to mitigate crime proactively and effectively, it seems the fight against cyberfraud is more effective and sustainable in the advanced economies than the emerging ones. This is because emerging economies still face challenges, including adopting and implementing recent technological advances to curb cybercrimes, lack of resources, low-level enforcement of cybercrime laws and inadequate sensitisation. However, there is a need for both the advanced and emerging economies to step up their fight against cybercrime to reduce the impact on the shareholders, the global economy, as well as

organisational reputation and profitability. In both economies, there is also a need to adjust existing policies to capture newly developed strategies for mitigating cyberfraud. Emerging economies can reinforce their cybersecurity architecture via digital technologies such as AI. Also, synergy at all levels can help emerging economies gather support for fully deploying digital technologies. The cross-border nature of cyberfraud demands that emerging countries implement a flexible and adaptive legal framework. Cyber fraudsters often hide behind fake identities and the anonymity of cyberspace; thus, combatting cyberfraud effectively requires upskilling and deploying resources that the anti-fraud agencies require. Particularly in emerging economies, financial institutions and the government and private sectors must form a robust and cohesive alliance. This is because private organisations own and control many databases and cyberspace infrastructures. A cohesive alliance can aid timely access to the information required for the investigation and prosecution of the fraudsters. Emerging economies must invest more in technological innovations and keep up with technological advancement trends. Other areas that require government intervention in tackling cyberfraud in emerging economies include the development of a resilient cybersecurity architecture and education. The institutional curriculum in emerging economies can incorporate cybersecurity and FA courses to promote awareness about the operation of the threat actors and the countermeasures. Unfortunately, many Internet fraudsters, especially in West Africa, are graduates of higher institutions who cite poverty and unemployment as reasons for perpetrating cyberfraud. This implies that sustainably tackling cyberfraud encompasses an all-round approach that considers not only cybersecurity and legal frameworks but also the socio-economic well-being of the people.

■ Conclusion

Cyberfraud is a global challenge, although it impacts developing economies more severely because of cybersecurity lapses, nonimplementation of cyber laws and inadequate resources to effectively combat cyberfraud. To achieve a sustainable fight against cyberfraud, there is a need to employ a multidimensional and innovative approach. The responsibility of combatting cyberfraud should not be left to the financial institutions alone but shared among the stakeholders such as government institutions and agencies, nongovernmental organisations, financial institutions, academia and civil society groups. Furthermore, the efforts of all these stakeholders should be integrated and coordinated at all levels: national, regional and international. The role of the private sector, including those who develop cyberspace, ICT architecture and digital products and services, cannot be downplayed.

Their engagement can promote cybersecurity and enhance intelligence sharing necessary to disrupt the threat actors' operations or investigate and prosecute them. As cyberfraud is a cross-border challenge, regional and international alliances will be needed. The synergy between the developing economies is also essential as this can promote technology aid, adoption or transfer, which is required to counter cyberfraud. Efforts must be geared towards achieving cybersecurity and cyber resilience using enabling digital technologies. This is necessary for any digital economy to thrive. Developed economies should also consider enacting and implementing appropriate cyber laws and reinforcing existing cybersecurity architecture to promote a more inclusive, secure and accessible cyberspace. This is also vital in checkmating the threat actors or minimising the impact of cyberfraud occurrences. In addition, human, financial and material resources must be provided. The support of private and public sectors and other national, regional and international stakeholders will be required to provide the resources necessary. For instance, the skills shortage in emerging or developing economies can be addressed through developing human capacities, training on cybersecurity and cyberfraud countermeasures, deployment of digital technologies, risk management, educational programmes and cybersecurity awareness. These require significant funding and cannot be achieved by the financial institutions alone.

Incorporating cybersecurity and digital technologies such as FA, AI and big data technology into the curriculum of educational institutions will also promote knowledge diffusion. To alleviate societal pressures that can lead to cyberfraud, such as unemployment and poverty, the public and private sectors can invest and fund projects that promote cybersecurity. Without robust internal and management controls, financial institutions will still fall prey to the cyberfraudsters. Therefore, financial institutions should review their internal and management control strategies and develop more proactive controls rather than reactive ones. There is a need to ensure compatibility between the deployed anti-fraud technologies and the security standards of the financial institutions and the respective countries.

Some years ago, many emerging digital technologies were used in emerging economies, coupled with cyberspace dynamics and threat actors' operations. Retrofitting cybersecurity measures to incorporate these emerging technologies rather than building them from scratch may be counterproductive to both emerging and developed economies without supporting infrastructures. Developing economies can consider asset digitalisation where there are supporting digital infrastructures or developing more secure digital solutions such as end-to-end encryption from the cybersecurity design phases to promote cyber resilience and reduce their system's vulnerabilities to cyberattack. Developing a cybersecurity solution

from scratch can provide training and job opportunities in developing economies, though it may appear costlier than retrofitting or asset digitalisation at the initial stage. However, the cost incurred by developing security solutions that match global standards will later be offset by providing training and job opportunities and reducing the cost incurred because of cyberattacks. Financial institutions will gain uptime and a more effective operation with minimal cyber risk. Hence, developing countries can choose higher embedded security solutions to enable cybersecurity and resilience. In some countries, upgrading security solutions may necessitate support from the government, private sector, or regulatory bodies at the national, regional or international levels.

References

- AAG 2022a, *Security report*, viewed 12 December 2022, <<https://aag-it.com/security/>>
- AAG 2022b, *The latest 2022 Cyber Crime statistics*, viewed 17 November 2022, <<https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:-:text=The%20country%20with%20the%20next,their%20accounts%20breached%20in%202021>>
- Abdullah, TTY, Alfadhi, MMA, Yahya, S & Rabi, AMA 2013, 'The role of forensic accounting in reducing financial corruption: A study in Iraq', *International Journal of Business and Management*, vol. 9, no. 1, pp. 26-34. <https://doi.org/10.5539/ijbm.v9n1p26>
- Abdulrahman, MD, Faruk, N, Oloyede, AA, Surajudeen-Bakinde, NT, Olawoyin, LA, Mejabi, OV, Imam-Fulani, YO, Fahm, AO & Azeez, AL 2020, 'Multimedia tools in the teaching and learning processes: A systematic review', *Heliyon*, vol. 6, no. 2, pp. 1-14, ae0531. <https://doi.org/10.1016/j.heliyon.2020.e05312>
- Abdullaheem, A, Isiaka, SB & Muhammed, AY 2012, 'Implication of fraud on commercial bank performance in Nigeria', *International Journal of Asian Social Science*, vol. 2, no. 4, pp. 382-387.
- Abdulrasheed, S, Babaitu, D & Tinusa, G 2012, 'Fraud and its implications for bank performance in Nigeria', *International Journal of Asian Social Science*, vol. 2, no. 4, pp. 35-45.
- Abouelmehdi, K, Beni-Hessane, A & Khaloufi, H 2017, 'Big healthcare data: Preserving security and privacy', *Journal of Big Data*, vol. 5, no. 1, pp. 1-18. <https://doi.org/10.1186/s40537-017-0110-7>
- Accenture 2020, *Insight into the cyber threat landscape in South Africa*, viewed 18 November 2022, <<https://www.accenture.com/za-en/insights/security/cyberthreat-south-Africa>>
- Adams, R, Hobbs, V & Mann, G 2013, 'The advanced data acquisition model (Adam): A process model for digital forensic practice', *Journal of Digital Forensics, Security and Law*, vol. 8, no. 4, pp. 25-48. <https://doi.org/10.15394/jdfsl.2013.1154>
- Adegbe, FF & Fakile, AS 2012, 'Economic and financial crime in Nigeria: Forensic accounting as antidote', *British Journal of Arts and Social Sciences*, vol. 6, no. 1, pp. 37-50.
- Adhyansh, J 2021, *History of digital forensics, definition, types, advantages & disadvantages*, viewed 15 April 2022, <<https://www.classmate4u.com/history-of-digital-forensics/>>
- Adom, D, Hussein, EK & Agyem, JA 2017, 'Theoretical and conceptual framework: Mandatory ingredients of quality research', *International Journal of Scientific Research*, vol. 7, no. 1, pp. 438-441.
- African Union 2016, *Report on cyber security and personal data protection*, viewed 18 November 2022, <<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>>
- Agarwal, A, Gupta, M, Gupta, S & Gupta, S 2011, 'Systematic refined digital forensic investigation model', *International Journal of Computer Science and Security*, vol. 5, no. 1, pp. 118-132.
- Agarwal, S 2022, 'Understanding misappropriation of assets at workplaces', *The Daily Guardian*, 14 May, viewed 21 February 2023, <<https://thedailyguardian.com/understanding-misappropriation-of-assets-at-workplaces/>>
- Aggarwal, P, Neha, P & Arora, P 2014, 'Review on cybercrime and security', *International Journal of Research in Engineering and Applied Sciences*, vol. 2, no. 1, pp. 48-51.
- Agnew, R 1992, 'Foundation for a general strain theory of crime and delinquency', *Criminology*, vol. 30, no. 1, pp. 47-88. <https://doi.org/10.1111/j.1745-9125.1992.tb01093.x>
- Ahmed, HM, Awan, MJ, Khan, NS, Yasin, A & Shehzad, HMF 2021, 'Sentiment analysis of online food reviews using big data analytics', *Ilkogretim Online*, vol. 20, no. 2, pp. 827-836.
- Ajayi, EFG 2016, 'Challenges to enforcement of cyber-crimes laws and policy', *Journal of Internet Information System*, vol. 6, no. 1, pp. 1-12. <https://doi.org/10.5897/JIIS2015.0089>

References

- Akabom-Ita, A 2012, 'Empirical analysis of the impact of information technology on forensic accounting practice in Cross River State – Nigeria', *International Journal of Scientific and Technology Research*, vol. 1, no. 7, pp. 25–32.
- Akers, R 2009, *Social learning and social structure: A general theory of crime and deviance*, Routledge, Oxford.
- Akhidime, AE 2017, 'Bridging audit expectation gap with the integration of forensic accounting: A review', *AE-Funai Journal of Accounting, Business and Finance*, vol. 693, pp. 72–82.
- Akhidime, AE & Uagbale-Ekatah, RE 2014, 'The growing relevance of forensic accounting as a tool for combating fraud and corruption: Nigeria experience', *Research Journal of Finance and Accounting*, vol. 5, no. 2, pp. 71–77.
- Akinbowale, OE 2022, 'The integration of forensic accounting and management control systems as a tool for combating cyberfraud in the South African banking sector', PhD thesis, Tshwane University of Technology, Pretoria.
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2020, 'An innovative approach in combating economic crime using forensic accounting techniques', *Journal of Financial Crime*, vol. 27, no. 4, pp. 1253–1271. <https://doi.org/10.1108/JFC-04-2020-0053>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2021, 'The integration of forensic accounting and the management control system as tools for combating cyberfraud', *Academy of Accounting and Financial Studies Journal*, vol. 25, no. 2, pp. 1–14.
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2022a, 'Analytical hierarchy process decision model and Pareto analysis for mitigating cybercrime in the financial sector', *Journal of Financial Crime*, vol. 29, no. 3, pp. 884–1008. <https://doi.org/10.1108/JFC-04-2021-0086>
- Akinbowale, OE, Klingelhöfer, HE and Zerihun, MF 2022b, 'Exploring the impact of corporate social responsibility and human resource accounting on the socioeconomic environment', *International Journal of Business Continuity and Risk Management*, vol. 12, no. 2, pp. 131–153. <https://doi.org/10.1504/IJBCRM.2022.124836>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2022c, 'The use of the balanced scorecard as a strategic management tool to mitigate cyberfraud in the South African banking industry', *Heliyon*, vol. 8, pp. 1–10, ae12054. <https://doi.org/10.1016/j.heliyon.2022.e12054>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2023a, 'Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk', *Cogent Economics & Finance*, vol. 11, no. 2, pp. 1–21, a215341. <https://doi.org/10.1080/23322039.2022.2153412>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2023b, 'Development of a multi-objective integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation', *Journal of Financial Crime*, vol. 30, no. 6, pp. 1720–1735. <https://doi.org/10.1108/JFC-10-2022-0245>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2023c, 'The assessment of the impact of cyberfraud in the South African banking industry', *Journal of Financial Crime*, vol. 31, no. 2, pp. 1–15. <https://doi.org/10.1108/JFC-10-2022-0260>
- Akinbowale, OE, Klingelhöfer, HE & Zerihun, MF 2023d, 'The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry', *Cogent Business & Management*, vol. 10, no. 1, pp. 1–22, a2163560. <https://doi.org/10.1080/23311975.2022.2163560>
- Alagarsamy, K & Wilson, S 2013, 'A study on customer behavior towards banking services with special reference to public sector Banks in Sivagangai District', *Asia Pacific Journal of Marketing & Management Review*, vol. 2, no. 2, pp. 183–196.
- Albano, P, Castiglione, A, Cattaneo, G & De Santis, A 2011, 'A novel anti-forensics technique for the android OS', in *Proceedings of the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, Barcelona, IEEE, Maui, pp. 380–385.

- Albrecht, WS, Howe, KR & Romney, MB 1984, *Deterring fraud: The internal auditor's perspective*, The Institute of Internal Auditors, Altomonte Springs.
- Aldasoro, I, Gambacorta, L, Guidici, P & Leach, T 2022, 'The drivers of cyber risk', *Journal of Financial Stability*, vol. 60, a100989.
- Ali, FMA 2017, 'Forensic accounting and financial fraud: Evidence from Saudi Arabia', *El-Bahit Review*, vol. 17, no. 1, pp. 41-47.
- Ali, L, Ali, F, Surendran, P & Thomas, B 2017, 'The effects of cyber threats on customer's behaviour in e-banking services', *International Journal of e-Education, e-Business, e-Management and e-Learning*, vol. 7, no. 1, pp. 70-78. <https://doi.org/10.17706/ijeeee.2017.7.1.70-78>
- Allen, K 2021, *South Africa lays down law on cybercrime*, viewed 28 February 2023, <<https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime>>
- Alpaydin, E 2020, *Introduction to machine learning*, 4th edn., MIT, Massachusetts, pp. xix, 1-3, 13-18.
- Al-Sharairi, ME 2017, 'The role of forensic accounting in limiting tax evasion in the Jordanian public industrial shareholding companies through the perspective of Jordanian auditors', *International Journal of Economics and Finance*, vol. 10, no. 1, pp. 233-243. <https://doi.org/10.5539/ijef.v10n1p233>
- Alshurafat, H, Al Shbail, OM & Mansour, E 2021, 'Strengths and weaknesses of forensic accounting: An implication on the socio-economic development', *Journal of Business and Socioeconomic Development*, vol. 1, no. 2, pp. 135-148. <https://doi.org/10.1108/JBSED-03-2021-0026>
- Alshurafat, H, Beattie, C, Jones, G & Sands, J 2020, 'Perceptions of the usefulness of various teaching methods in forensic accounting education', *Accounting Education*, vol. 29, no. 2, pp. 177-204. <https://doi.org/10.1080/09639284.2020.1719425>
- Al-Suwaidi, N, Nobanee, H & Jabeen, F 2017, 'Estimating causes of cyber crime: Evidence from panel data FGLS estimator', *International Journal of Cyber Criminology (Diamond Open Access Journal)*, vol. 12, no. 2, pp. 392-407.
- Altamimi, T 2011, 'Information security risks for internet banking in Saudi Arabia', MSc thesis, University of Sheffield, Sheffield.
- Alwan, HA & Al-Zubi, AI 2016, 'Determinants of internet banking adoption among customers of commercial banks: An empirical study in the Jordanian banking sector', *International Journal of Business and Management*, vol. 11, no. 3, pp. 95-104. <https://doi.org/10.5539/ijbm.v11n3p95>
- Alyamani, R & Long, S 2020, 'The application of fuzzy analytic hierarchy process in sustainable project selection', *Sustainability*, vol. 12, no. 8314, pp. 1-16. <https://doi.org/10.3390/su12208314>
- Ambalavanan, V 2020, 'Cyber threats detection and mitigation using machine learning', in P Ganapathi & D Shanmugapriya (eds.), *Handbook of research on machine and deep learning applications for cyber security*, IGI Global, Hershey, pp. 132-149.
- American Institute of Certified Public Accountants (AICPA) 2002, *Statement of auditing standards 99: Consideration of fraud in a financial statement audit*, American Institute of Certified Public Accountants, New York.
- American Institute of Certified Public Accountants (AICPA) 2012, *Fraud prevention*, viewed 01 August 2020, <www.aicpa.org/interestareas/forensicandvaluation/resources/fraudpreventionondetectionresponse/>
- American Institute of Certified Public Accountants (AICPA) 2017, 'How CPAs can protect themselves and their clients', Top Cybercrimes White Paper, viewed 28 February 2023, <www.aicpa.org>
- Amigo-Dobaño, L, Garza-Gil, MD & Varela-Lafuente, MM 2020, 'Analyzing the attitudes of Spanish firms towards Brexit's effects on the management of European fisheries', *Sustainability*, vol. 12, no. 5819, pp. 1-17. <https://doi.org/10.3390/su12145819>

References

- Amshire, V & Meshram, B 2012, 'Digital forensic tools', *IOSR Journal of Engineering*, vol. 2, no. 3, pp. 392-398. <https://doi.org/10.9790/3021-0203392398>
- Anderson, R, Barton, C, Böhme, R, Clayton, R, Van Eeten, MJG, Levi, M, Moore, T & Savage, S 2013, 'Measuring the cost of cybercrime', in R Böhme (ed.), *Economics of information security and privacy*, Springer, Berlin, pp. 265-300.
- Andoh, C, Quaye, D & Akomea-Frimpong, I 2017, 'Impact of fraud on Ghanaian SMEs and coping mechanisms', *Journal of Financial Crime*, vol. 25, no. 2, pp. 400-418. <https://doi.org/10.1108/JFC-05-2017-0050>
- Andrija, B 2017, 'Corporate social responsibility and stakeholders: Review of the last decade 2006-2015', *Business Systems Research: International Journal of the Society for Advancing Innovation and Research in Economy*, vol. 8, no. 1, pp. 133-146. <https://doi.org/10.1515/bsrj-2017-0011>
- Anizoba, EN, Ezugwu, DC & Obumse, A 2005, 'Forensic accounting: Issues and options', MSc Seminar Paper, Department of Accountancy, Nnamdi Azikiwe University, Awka.
- Anthony, R 1965, *Planning and control systems: A framework for analysis*, Harvard University Graduate Business School of Business Administration, Boston.
- Arachchilage, NAG & Love, S 2014, 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behaviour*, vol. 38, pp. 304-312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Aral, KD, Güvenir, HA, Sabuncuoğlu, İ & Akar, AR 2012, 'A prescription fraud detection model', *Computer Methods and Programs in Biomedicine*, vol. 106, no. 1, pp. 37-46. <https://doi.org/10.1016/j.cmpb.2011.09.003>
- Arcuri, MB, Brogi, M & Gandolfi, G 2017, 'How does cybercrime affect firms? The effect of information security breaches on stock returns', in *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, Venice, Italy, January 17-20, pp. 175-193.
- Arens, A & Loebbecke, J 1997, *Auditing: An integrated approach*, Prentice Hall, Englewood Cliffs.
- Ariwala, P 2022, *What is big data analytics and why do I need it for my business?*, viewed 17 December 2022, <<https://www.marutitech.com/big-data-analytics-need-business/>>
- Arjalies, D-L & Mundy, J 2013, 'The use of management control systems to manage CSR strategy: A levers of control perspective', *Management Accounting Research*, vol. 24, pp. 284-300. <https://doi.org/10.1016/j.mar.2013.06.003>
- Arkkelin, D 2014, *Using SPSS to understand research and data analysis: Psychology curricular materials, Book 1*, viewed 22 October 2020, <http://scholar.valpo.edu/psych_oer/1>
- Armash, H, Salarzehi, H & Kord, B 2010, 'Management control system', *Interdisciplinary Journal of Contemporary Research in Business*, vol. 2, no. 6, pp. 193-206.
- Arnaboldi, M, Busco, C & Cuganesan, S 2017, 'Accounting, accountability, social media and big data: Revolution or hype?', *Accounting, Auditing & Accountability Journal*, vol. 30, no. 4, pp. 762-776. <https://doi.org/10.1108/AAAJ-03-2017-2880>
- Artis, M, Ayuso, M & Guillén, M 2002, 'Detection of automobile insurance fraud with discrete choice models and misclassified claims', *The Journal of Risk and Insurance*, vol. 69, no. 3, pp. 325-340. <https://doi.org/10.1111/1539-6975.00022>
- Aseltine, RH, Gore, S & Gordon, J 2000, 'Life stress, anger and anxiety, and delinquency: An empirical test of general strain theory', *Journal of Health and Social Behavior*, vol. 41, no. 3, pp. 256-275. <https://doi.org/10.2307/2676320>
- Association of Certified Fraud Examiners (ACFE) 2012a, *Managing fraud risk: First, second, or third line of defense responsibility?*, viewed 02 February 2020, <https://www.acfe.com/uploadedfiles/acfe_website/content/european/course_materials/2012/11c_risch-cpp.pdf>
- Association of Certified Fraud Examiners (ACFE) 2012b, *Report to the nation on occupational fraud and abuse 2012 global fraud study*, Association of Certified Fraud Examiners, Austin.

- Association of Certified Fraud Examiners (ACFE) 2020, *Report to the nation*, viewed 04 March 2021, <<https://legacy.acfe.com/report-to-the-nations/2020/>>
- Australian Bureau of Statistics 2016, *Personal fraud, 2014-15*, viewed 20 January 2022, <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/>>
- Australian Cybercrime Online Reporting Network (ACORN) 2016, *Australian criminal intelligence commission*, viewed 20 January 2021, <<https://acorn.govspace.gov.au/resources/>>
- Ayatollahi, H, Bath, PA & Goodacre, S 2009, 'Paper-based versus computer based records in emergency department: Staff preferences, expectations and concerns', *Health Informatics Journal*, vol. 15, no. 3, pp. 199-211.
- Ayers, R, Jansen, W, Delaitre, A & Moenner, L 2007, *Cell phone forensic tools: An overview and analysis update*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, viewed 09 September 2020, <<https://csrc.nist.gov/publications/detail/nistir/7387/final>>
- Baader, G & Krcmar, H 2017, 'Reducing false positives in fraud detection: Combining the red flag approach with process mining', *International Journal of Accounting Information Systems*, vol. 31, pp. 1-16. <https://doi.org/10.1016/j.accinf.2018.03.004>
- Bai, B, Yen, J & Yang, X 2007, 'False financial statements: Characteristics of China's listed companies and CART detecting approach', *International Journal of Information Technology & Decision Making*, vol. 7, no. 2, pp. 339-359. <https://doi.org/10.1142/S0219622008002958>
- Balan, S, Otto, J, Minasian, E & Aryal, A 2017, 'Data analysis of cybercrimes in businesses', *Information Technology and Management Science*, vol. 20, pp. 64-68. <https://doi.org/10.1515/itms-2017-0011>
- Balios, D, Kotsilaras, P, Eriotis, N & Vasiliou, D 2020, 'Big data, data analytics and external auditing', *Journal of Modern Accounting and Auditing*, vol. 16, no. 5, pp. 211-219. <https://doi.org/10.17265/1548-6583/2020.05.002>
- Bamrara, A, Singh, G & Bhatt, M 2013, 'Cyber attacks and defense strategies in India: An empirical assessment of banking sector', *International Journal of Cyber Criminology*, vol. 7, no. 1, pp. 49-61. <https://doi.org/10.2139/ssrn.2488413>
- Barclays Africa Group Ltd 2017a, *Integrated report*, viewed 16 November 2020, <<https://www.barclaysafrica.com/content/dam/barclays-africa/bagl/pdf/results/annual/2017-integrated-report.pdf>>
- Barclays Africa Group Ltd 2017b, *GRI report*, viewed 16 November 2020, <<https://www.barclaysafrica.com/content/dam/barclays-africa/bagl/pdf/results/annual/2017-gri-report.pdf>>
- Barrows, E & Neely, A 2012, *Managing performance in turbulent times: Analytics and insight*, John Wiley & Sons, Hoboken.
- Bashir, AH, Zarifah, A & Sheikh, MRH 2013, 'Management control systems: A review of literature and a theoretical framework for future researches', *European Journal of Business and Management*, vol. 5, no. 26, pp. 1-14.
- Basitere, E, Daniyan, I, Mpofo, K & Adeodu, A 2024, 'Performance evaluation of machine learning app approach to modular arrangement of predetermined time standard', in GL Conte & O Sename (eds.), *Proceedings of the 11th International Conference on Mechatronics and Control Engineering: ICMCE 2023*, Springer, Singapore, pp. 117-127. https://doi.org/10.1007/978-981-99-6523-6_9
- Bassey, BE & Ahonkhai, OE 2017, 'Effect of forensic accounting and litigation support on fraud detection of banks in Nigeria', *Journal of Business and Management*, vol. 19, no. 6, pp. 56-60. <https://doi.org/10.9790/487X-1906055660>
- Bell, TB & Carcello, JV 2000, 'A decision aid for assessing the likelihood of fraudulent financial reporting', *Auditing: A Journal of Practice & Theory*, vol. 19, no. 1, pp. 169-174. <https://doi.org/10.2308/aud.2000.19.1.169>

References

- Bengio, Y, Courville, A & Vincent, P 2013, 'Representation learning: A review and new perspectives', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1798–1828. <https://doi.org/10.1109/TPAMI.2013.50>
- Bermúdez, L, Pérez, JM, Ayuso, M, Gómez, E & Vázquez, FJ 2007, 'A Bayesian dichotomous, model with asymmetric link for fraud in insurance', *Insurance: Mathematics and Economics*, vol. 42, no. 2, pp. 779–786. <https://doi.org/10.1016/j.insmatheco.2007.08.002>
- Bhasin ML 2007, 'Forensic accounting: A new paradigm for niche consulting: The chartered accountant', *Country*, n.v., pp. 1000–1010.
- Bhasin, ML 2012, 'Audit committee scenario and trends in a developing country', *European Union Journal*, vol. 4, pp. 53–70. <https://doi.org/10.12816/0001124>
- Bhasin, ML 2013, 'An empirical investigation of the relevant skills of forensic accountants: Experience of a developing economy', *European Journal of Accounting Auditing and Finance Research*, vol. 1, no. 2, pp. 11–52.
- Bhasin, ML 2014, 'Corporate governance and forensic accountants' role: Global regulatory action scenario', *International Journal of Accounting Research*, vol. 1, no. 1, pp. 1–19.
- Bhasin, ML 2016a, 'Corporate governance and forensic accountants' role: Global regulatory action scenario', *International Journal of Accounting Research*, vol. 1, no. 1, pp. 54–86.
- Bhasin, ML 2016b, 'The role of technology in combatting bank frauds: Perspectives and prospects', *EcoForum*, vol. 5, nos. 2/9, pp. 200–212.
- Bhaskar, R & Kapoor, B 2013, *Information technology security management in computer and information security handbook*, JR Vacca (ed.), Morgan Kaufmann Publishers, Burlington, pp. e35–e44. <https://doi.org/10.1016/B978-0-12-803843-7.00027-2>
- Bhusari, V & Patil, S 2011, 'Application of Hidden Markov Model in credit card fraud detection', *International Journal of Distributed and Parallel Systems*, vol. 2, no. 6, pp. 203–211. <https://doi.org/10.5121/ijdps.2011.2618>
- Bigler, M 2001, 'Computer forensics gear', *The Internal Auditor*, August, p. 27.
- Bishop, MC 2006, *Pattern recognition and machine learning*, Springer, New York.
- Biswas, B 2013, *Compensation and benefit design: Applying finance and accounting principles to global HRMs*, Prentice Hall, Upper Saddle River.
- Black, HC, Nolan, JR & Connolly, MJ 1979, *Black's law dictionary: Definition of the terms and phrases of American and English jurisprudence, ancient and modern*, 5th edn., West Publishing Company, Minnesota.
- Boateng, AA, Boateng, GO & Acquah, H 2014, 'A literature review of fraud risk management in micro finance institutions in Ghana', *Research Journal of Finance and Accounting*, vol. 5, no. 11, pp. 42–52.
- Böhme, R & Moore, T 2012, 'How do consumers react to cybercrime?', in *Proceedings of the 7th IEEE APWG eCrime Researchers Summit (eCrime)*, Las Vegas, United States of America, October 23–24, pp. 1–12.
- Bossler, A 2020, 'Contributions of criminological theory to understanding cybercrime offending and victimization', in R Leukfeldt & T Holt (eds.), *The human factor of cybercrime*, Routledge, Oxford, pp. 29–59.
- Bossler, A & Holt, T 2009, 'On-line activities, guardianship, and malware infection: Examining routine activities theory', *International Journal of Cyber Criminology*, vol. 3, no. 1, pp. 400–420.
- Boyd, BK, Bergh, DD & Ketchen, JRDJ 2010, 'Reconsidering the reputation–performance relationship: A resource-based view', *Journal of Management*, vol. 36, no. 3, pp. 588–609.
- Brand, M, Valli, C & Woodward, A 2010, 'Malware forensics: Discovery of the intent of deception', *Journal of Digital Forensics, Security and Law*, vol. 5, no. 4, pp. 31–42. <https://doi.org/10.15394/jdfsl.2010.1082>
- Brennan, NM 2014, 'Forensic accounting in a constitutional parliamentary democracy: The case of Ireland', *Journal of Forensic and Investigative Accounting*, vol. 6, no. 3, pp. 62–97.

- Brickner, DR, Mahoney, LS & Moore, SJ 2010, 'Providing an applied-learning exercise in teaching fraud detection: A case of academic partnering with IRS criminal investigation', *Issues in Accounting Education*, vol. 25, no. 4, pp. 695–708. <https://doi.org/10.2308/iaee.2010.25.4.695>
- Broadhurst, R 2017, 'Cybercrime: Thieves, swindlers, bandits, and privateers in cyberspace', in *The Oxford handbook of cyber security*, Oxford Academic, London, pp. 89–108.
- Broadhurst, R & Grabosky, P 2005, 'Computer-related crime in Asia: Emergent issues', in R Broadhurst & P Grabosky (eds.), *Cyber-crime: The challenge in Asia*, Hong Kong University Press, Hong Kong, pp. 347–360.
- Broadhurst, R, Grabosky, P, Alazab, M & Steve, C 2014, 'Organizations and cybercrime: An analysis of the nature of groups engaged in cyber crime', *International Journal of Cyber Criminology*, vol. 8, no. 1, pp. 1–20.
- Brockett, PL, Derrig, RA & Golden, LL 2002, 'Fraud classification using principal component analysis of RIDITS', *The Journal of Risk and Insurance*, vol. 69, no. 3, pp. 341–371. <https://doi.org/10.1111/1539-6975.00027>
- Brockett, PL, Xia, X & Derrig, RA 1997, 'Using Kononen's self-organizing feature map to uncover automobile bodily injury claims fraud', *The Journal of Risk and Insurance*, vol. 65, no. 2, pp. 245–274. <https://doi.org/10.2307/253535>
- Broidy, LM 2001, 'A test of general strain theory', *Criminology*, vol. 39, pp. 9–36.
- Brown, CSD 2015, 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice', *International Journal of Cyber Criminology*, vol. 9, no. 1, pp. 55–119.
- Buckley, RP & Nixon, J 2009, 'The role of reputation in banking', *Journal of Banking and Finance Law and Practice*, vol. 20, pp. 37–50.
- Budapest Convention, Council of Europe 2022, *Article 10, Offences related to infringements of copyright and related rights*, Cybercrime Programme Office (C-PROC) of the Council of Europe, Johannesburg.
- Burney, SMA & Ali, SM 2019, 'Fuzzy multi-criteria based decision support system for supplier selection in the textile industry', *International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 239–244.
- Burns, N & Kedia, S 2006, 'The impact of performance-based compensation on misreporting', *Journal of Financial Economics*, vol. 79, pp. 35–67. <https://doi.org/10.1016/j.jfineco.2004.12.003>
- BusinessGhana* 2018, 'Bank of Ghana launches cyber security directive for financial institutions', *BusinessGhana*, 25 October, viewed 02 February 2022, <<https://www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions>>
- BusinessTech 2017, 'Major SA banks taken to court over internet fraud', *BusinessTech*, 18 April, viewed 01 August 2020, <<https://businesstech.co.za/news/mobile/170629/major-sa-banks-taken-to-court-over-internet-fraud/>>
- Bzdok, D, Altman, N & Krzywinski, M 2017, 'Statistics vs machine learning', *Nature Methods*, vol. 15, no. 4, pp. 233–234. <https://doi.org/10.1038/nmeth.4642>
- Cao, M, Chychyla, R & Stewart, T 2015, 'Big data analytics in financial statement audits', *Accounting Horizons*, vol. 29, no. 2, pp. 423–429. <https://doi.org/10.2308/acch-51068>
- Capelleveen, GC 2013, *Outlier-based predictors for health insurance fraud detection within US Medicaid*, viewed 16 June 2022, <<http://purl.utwente.nl/essays/64417>>
- Capitec Bank Ltd 2017, *Integrated annual report*, viewed 16 November 2020, <https://commondatastorage.googleapis.com/capitecbank-co-za/integrated_annual_report.pdf>
- Capitec Bank Ltd 2022, *Integrated annual report*, viewed 26 December 2022, <https://www.capitecbank.co.za/globalassets/pages/investor-relations/financial-results/2022/annual-report/integrated_annual_report_2022.pdf>

References

- Carenys, J 2012, 'Management control systems: A historical perspective', *International Journal of Economy, Management and Social Sciences*, vol. 1, no. 1, pp. 1-18.
- Carpenter, TD, Durtschi, C & Gaynor, LM 2011, 'The incremental benefits of a forensic accounting course on skepticism and fraud-related judgments', *Issues in Accounting Education*, vol. 26, no. 1, pp. 1-21. <https://doi.org/10.2308/iace.2011.26.1.1>
- Carrier, B & Spafford, EH 2003, 'Getting physical with the investigative process', *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1-20.
- Carroll, AB 1991, 'The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders', *Business Horizons*, vol. 34, no. 4, pp. 39-48. [https://doi.org/10.1016/0007-6813\(91\)90005-G](https://doi.org/10.1016/0007-6813(91)90005-G)
- Carroll, AB 2016, 'Carroll's pyramid of CSR: Taking another look', *International Journal of Corporate Social Responsibility*, vol. 1, no. 3, pp. 1-8. <https://doi.org/10.1186/s40991-016-0004-6>
- Carvey, H 2009, *Windows forensic analysis DVD toolkit*, Syngress Publishing Inc., Rockland.
- Cassim, F 2011, 'Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players', *Comparative and International Law Journal of Southern Africa*, vol. 44, no. 1, pp. 123-138.
- Caudill, SB, Ayuso, M & Guillén, M 2005, 'Fraud detection using a multinomial logit model with missing information', *The Journal of Risk and Insurance*, vol. 72, no. 4, pp. 539-550. <https://doi.org/10.1111/j.1539-6975.2005.00137.x>
- Centre for Excellence in Financial Service 2017, *The impact of the 4th industrial revolution on the South African financial services*, viewed 16 November 2020, <<https://www.genesisanalytics.com/uploads/downloads/COEFSTheimpactofthefourthindustrialrevolutiononfinancialservicesinSouthAfrica-final-1-FR.pdf>>
- Centre for Forensic Studies 2010, *The role of forensic and investigative accounting: Challenges for the banking industry - roundtable discussion by the Nigerian Institute of Advanced Legal Studies Lagos, Nigeria*, viewed 21 June 2022, <http://www.nials-nigeria.org/round_tables/CommuniqueonForensicandInvestigativeAccount19th_july_10.pdf>
- Centre for Strategic and International Studies (CSIS) 2014, *Net losses: Estimating the global cost of cybercrime*, Technical Report, Centre for Strategic and International Studies, Washington DC, viewed 20 January 2020, <<https://collabra.email/wp-content/uploads/2015/04/rp-economic-impact-cybercrime-2014.pdf>>
- Centre for Strategic and International Studies (CSIS) 2017, *Economic impact of cybercrime-no slowing down*, viewed 15 November 2022, <<https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf>>
- Cerullo, MJ & Cerullo, V 1999, 'Using neural networks to predict financial reporting fraud', *Computer Fraud & Security*, vol. 6, pp. 14-17. [https://doi.org/10.1016/S1361-3723\(99\)80035-9](https://doi.org/10.1016/S1361-3723(99)80035-9)
- Ch, R, Gadekallu, T, Abidi, M & Al-Ahmari, A 2020, 'Computational system to classify cyber crime offenses using machine learning', *Sustainability*, vol. 12, no. 4087, pp. 1-16. <https://doi.org/10.3390/su12104087>
- Chakrabarti, M 2014, 'Problems and prospects of the forensic accounting profession in India', *International Journal of Informative & Futuristic Research*, vol. 2, no. 1, pp. 1-9.
- Chalil, K 2000, *Statistical methods for development research*, Central University of South Bihar, Gayar, pp. 1-21.
- Chan, PK, Fan, W, Prodromidis, AL & Stolfo, SL 1999, 'Distributed data mining in credit card fraud detection', *IEEE Intelligent Systems*, vol. 14, no. 6, pp. 67-74. <https://doi.org/10.1109/5254.809570>
- Chartered Institute of Management Accountants (CIMA) 2007, *Fraud risk management: A guide to good practice*, pp. 1-82, viewed 02 December 2022, <<https://www.cimaglobal.com>>

- com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf>
- Chattopadhyay, P 2014, 'A theoretical construct of forensic accounting and auditing', *The Journal for CMAs*, vol. 49, no. 9, pp. 22-28.
- Chaudhary, GK 2014, 'Development review on phishing: A computer security threat', *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 8, pp. 55-64.
- Chen, H, Chiang, RHL & Storey, VC 2012, 'Business intelligence and analytics: From big data to big impact', *MIS Quarterly*, vol. 36, no. 4, pp. 1165-1188. <https://doi.org/10.2307/41703503>
- Chen, R, Chen, T & Lin, C 2006, 'A new binary support vector system for increasing detection rate of credit card fraud', *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 20, no. 2, pp. 227-239. <https://doi.org/10.1142/S0218001406004624>
- Chigada, J & Madzinga, R 2021, 'Cyberattacks and threats during COVID-19: A systematic literature review', *South African Journal of Information Management*, vol. 23, no. 1, pp. 1-11. <https://doi.org/10.4102/sajim.v23i1.1277>
- Chimuka, TA & Mashumba-Paki, L 2016, 'Understanding cyber scams: An assessment of the challenges of law enforcement in Botswana', *Journal of Sustainable Development in Africa*, vol. 18, no. 2, pp. 111-126. <https://doi.org/10.4324/9781315415499-15>
- China Global Television Network (CGTN) 2020, 'Rights group launches tool to stem cybercrime in Africa', 27 October, viewed July 2022, <<https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmuIPJeM/index.html>>
- Chism, KA & Steinmetz, KF 2017, 'Strain theory and technocrime', in KF Steinmetz & MR Nobles (eds.), *Technocrime and criminological theory*, Routledge, Oxford, pp. 66-84.
- Chiu, T, Wang, Y & Vasarhelyi, MA 2020, 'The automation of financial statement fraud detection: A framework using process mining', *Journal of Forensic and Investigative Accounting*, vol. 12, no. 1, pp. 86-108.
- Choi, J, Peters, M & Mueller, RO 2010, 'Correlational analysis of ordinal data: From Pearson's *r* to Bayesian polychoric correlation', *Asia Pacific Education Review*, vol. 11, pp. 459-466.
- Choobineh, J, Dhillon, G, Grimaila, MR & Rees, J 2007, 'Management of information security: Challenges and research', *Communications of the Association for Information Systems*, vol. 20, pp. 958-971. <https://doi.org/10.17705/1CAIS.02057>
- Chukwunedu, OS & Okoye, EI 2011, *Forensic accounting and audit expectation gap: The perception of accounting academics*, viewed 26 December 2021, <<http://ssrn.com/abstract=1920865>>
- Ciardhuain, SO 2004, 'An extended model of cybercrime investigations', *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1-22.
- Clarke, T & Dela Rama, M 2006, 'The governance of globalization', in T Clarke & M Dela Rama (eds.), *Corporate governance and globalization*, 3 vols., SAGE Publications, Thousand Oaks.
- Clayton, MM 2011, 'Investigative techniques', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 271-281.
- Clayton, MM, Moorman, JC, Wilkinson, J, Shackell, M & Schaffer, G 2006, 'Data mining: Computer-aided forensic accounting investigation technique', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, John Wiley & Sons, Hoboken, pp. 385-422.
- Clementina, K & Isu, IG 2016, 'Security challenge, bank fraud and commercial bank performance in Nigeria: An evaluation', *Journal of Business and Management*, vol. 5, no. 2, pp. 1-21. <https://doi.org/10.12735/jbm.v5n2p01>
- Coetzee, J 2017, 'Strategic implications of Fintech on South African retail banks', *South African Journal of Economic and Management Sciences*, vol. 21, no. 1, a2455. <https://doi.org/10.4102/sajems.v21i1.2455>

References

- Cohen, L & Felson, M 1979, 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, vol. 44, pp. 588-608. <https://doi.org/10.2307/2094589>
- Communication Authority of Kenya 2022, *Cybersecurity overview*, viewed 28 February 2023, <<https://www.ca.go.ke/industry/cyber-security/overview/>>
- Conrad, E, Misener, S & Feldman, J 2012, 'Domain 9: Legal regulation, investigation and compliance', in E Conrad, S Misener & J Feldman (eds.), *10 CISSP study guide*, 2nd edn., Syngress Publisher, Oxford, pp. 389-427.
- Copeland, L, Edberg, D, Panorska, AK & Wendel, J 2012, 'Applying business intelligence concepts to Medicaid claim fraud detection', *Journal of Information Systems Applied Research*, vol. 5, no. 1, p. 51.
- Council of Europe (COE) 2022, *Domestic equivalent to the provisions of the Budapest convention*, August 2022, viewed 26 October 2023, <https://www.coe.int/en/web/octopus/-/south-africa?p_p_col_count=1&p_p_col_id=column-4&p_p_lifecycle=0&p_p_mode=view&p_p_state=normal&redirect=https%3A%2F%2Fwww>
- Council on Foreign Relations 2019, *Last month, over half-a-billion Africans viewed the internet*, viewed 30 July 2022, <<https://www.cfr.org/blog/last-month-over-half-billion-Africans-accessed-internet>>
- CPA 2012, *Study manual on management accounting*, 2nd edn., Deakin University Publisher, Melbourne.
- Cressey, D 1953, *Other people's money: A study in the social psychology of embezzlement*, Free Press, Glencoe.
- Cressey, DR 1973, *Other people's money: A study in the social psychology of embezzlement*, Patterson Smith, Montclair.
- Cross, C & Blackshaw, D 2015, 'Improving the police response to online fraud', *Policing*, vol. 9, no. 2, pp. 119-128. <https://doi.org/10.1093/police/pau044>
- Crumbley, DL 2009, 'So what is forensic accounting?', *The ABO Reporter Fall*, no. 9, pp. 1-6.
- Crumbley, DL, Heitger, LE & Smith, GS 2009, *Forensic and investigative counting*, CCH Group, Chicago, pp. 3-5.
- Curtis, GE 2007, 'Legal and regulatory environments and ethics: Essential fraud and forensic accounting curriculum components', *Issues in Accounting Education*, vol. 23, no. 4, pp. 535-543. <https://doi.org/10.2308/iace.2008.23.4.535>
- Cusack, B & Ahokov, T 2016, 'Improving forensic software tool performance in detecting fraud for financial statements', in C Valli (ed.), *Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016*, Edith Cowan University, Perth, pp. 17-24.
- Cyber Security Ventures 2017, *Cybercrime report*, viewed 17 January 2020, <<https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>>
- Cyber Security Ventures 2022, *Cybercrime to cost the world \$10.5 trillion annually by 2025*, viewed 15 November 2022, <<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/#:~:text=The%20damages%20for%202018%20were,than%20it%20was%20in%202015>>
- Da Vinci Cybersecurity 2023, *Cybercrime investigation in South Africa*, viewed 22 February 2023, <<https://davinciforensics.co.za/cybersecurity/cybercrime-investigations-in-south-africa/>>
- Dada, S, Owolabi, SA & Okwu, AT 2013, 'Forensic accounting a panacea to the alleviation of fraudulent practices in Nigeria', *International Journal of Business Management Economics Research*, vol. 4, no. 5, pp. 787-792.
- Dagada, R 2013, 'Digital banking security, risk and credibility concerns in South Africa', in *Proceedings of the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*, Kuala Lumpur, March 04-06, pp. 148-161.

- Dagilienė, L & Klovienė, L 2019, 'Motivation to use big data and big data analytics in external auditing', *Managerial Auditing Journal*, vol. 34, no. 7, pp. 750-782. <https://doi.org/10.1108/MAJ-01-2018-1773>
- Dalla, EH & Geeta, MS 2013, 'Cybercrime a threat to persons, property, government and societies', *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, pp. 997-1002.
- Dalton, DR, Hitt, MA, Certo, ST & Dalton, CM 2007, 'The fundamental agency problem and its mitigation: Independence, equity, and the market for corporate control', *Academy of Management Annals*, vol. 1, pp. 1-64. <https://doi.org/10.5465/078559806>
- Damilola, D & Olofinsola, J 2007, 'Forensic accountants and the litigation support engagement', *The Nigerian Accountant*, vol. 39, no. 4, pp. 49-52.
- Daniyan, IA, Adeodu, AO, Mpofu, K, Ramatsetse, BI & Muvunzi, R 2022, 'Enhancing the machinability of titanium alloy (Ti6Al4V): A comprehensive review of literature', in IA Daniyan (ed.), *Advances in Manufacturing Technologies*, Benham Science, Singapore, pp. 4-21.
- Daniyan, IA, Mpofu, K, Ramatsetse, BI & Gupta, M 2021, 'Review of life cycle models for enhancing machine tools sustainability: Lessons, trends and future directions', *Heliyon*, vol. 7, no. 4, pp. 1-21. <https://doi.org/10.1016/j.heliyon.2021.e06790>
- Daniyan, IA, Tilhabadira, I, Mpofu, K & Adeodu, AO 2020, 'Development of numerical models for the prediction of temperature and surface roughness during the machining operation of titanium alloy (Ti6Al4V)', *Acta Polytechnica Journal*, vol. 60, no. 5, pp. 369-390. <https://doi.org/10.14311/AP.2020.60.0369>
- Darshan, PP 2020, 'Role of the computers in digital forensics', *International Journal for Science and Advance Research in Technology*, vol. 6, no. 7, pp. 585-588.
- Davia, H, Coggins, P, Wideman, J & Kastanin, J 2001, 'Accountant's guide to fraud detection and control', *EDPACS The EDP Audit, Control and Security Newsletter*, vol. 29, no. 1, pp. 12-13. <https://doi.org/10.1201/1079/43270.29.1.20010701/30409.5>
- Davis, C, Farrell, R & Ogilby, S 2010, *Characteristics and skills of the forensic accountant*, AICPA Publications, New York.
- De Dott, RM 2020, 'The use of big data analytics and artificial intelligence tools to prevent fraud in the audit field: A conceptual frame', *Rivista Italiana Di Ragioneria E Di Economia Aziendale*, 2020 vol., no. 3, pp. 380-389.
- De Haas, M & Kleingeld, A 1999, 'Multilevel design of performance measurement systems: Enhancing strategic dialogue throughout the organization', *Management Accounting Research*, vol. 10, pp. 233-261. <https://doi.org/10.1006/mare.1998.0098>
- Dearden, TE, Parti, K & Hawdon, J 2021, 'Institutional anomie theory and cybercrime - Cybercrime and the American dream', *Journal of Contemporary Criminal Justice*, vol. 37, no. 3, pp. 1-22. <https://doi.org/10.1177/10439862211001590>
- Decker, D, Blanc, A, Loveland, J & Clayton, M 2011, 'Data mining analysis of structured and unstructured information', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 333-362.
- Dedrick, J, Gurbaxani, V & Kraemer, KL 2003, *Information technology and economic performance: A critical review of the empirical evidence*, Centre for Research on Information Technology and Organizations, University of California, Irvine.
- Degboro, D & Olofinsola, J 2007, 'Forensic accountants and the litigation support engagement', *Nigerian Accounting*, vol. 40, no. 2, pp. 49-52.
- Dela Rama, M 2012, 'Corporate governance and corruption: Ethical dilemmas of Asian business groups', *Journal of Business Ethics*, vol. 109, pp. 501-519. <https://doi.org/10.1007/s10551-011-1142-0>
- Delen, D & Demirkan, H 2013, 'Decision support systems, data, information and analytics as services', *Decision Support Systems*, vol. 55, no. 1, pp. 359-363. <https://doi.org/10.1016/j.dss.2012.05.044>

References

- Dellaportas, S 2013, 'Conversations with inmate accountants: Motivation, opportunity and the fraud triangle', *Accounting Forum*, vol. 37, no. 1, pp. 29–39. <https://doi.org/10.1016/j.accfor.2012.09.003>
- Deloitte 2016, *Beneath the surface of a cyberattack*, viewed 11 August 2019, <<https://www2.deloitte.com/us/en/pages/risk/articles/hidden-businessimpact-of-cyberattack.html>>
- Deshmukh, A, Romine, J & Siegel, PH 1997, 'Measurement and combination of red flags to assess the risk of management fraud: A fuzzy set approach', *Managerial Finance*, vol. 23, no. 6, pp. 35–48. <https://doi.org/10.1108/eb018629>
- Deshmukh, A & Talluru, L 1997, 'A rule-based fuzzy reasoning system for assessing the risk of management fraud', *International Journal of Intelligent Systems in Accounting, Finance & Management*, vol. 7, no. 4, pp. 223–241. [https://doi.org/10.1002/\(SICI\)1099-1174\(199812\)7:4%3C223::AID-ISAF158%3E3.3.CO;2-9](https://doi.org/10.1002/(SICI)1099-1174(199812)7:4%3C223::AID-ISAF158%3E3.3.CO;2-9)
- Detica Limited 2011, *The cost of cybercrime*, viewed 15 September 2021, <<https://assets.publishing.service.gov.uk/media/5a78e882e5274a2acd18ab84/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf>>
- Dezfouli, FN, Dehghantanha, A, Mahmoud, R, Binti Mohd Sani, NF & Shamsuddin, SB 2012, 'Volatile memory acquisition using backup for forensic investigation', in *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Kuala Lumpur, June 26–28, pp. 186–189.
- DiGabriele, JA & Lohrey, PL 2016, 'The valuation of economic damages: A case study for the forensic accountant', *Journal of Forensic and Investigative Accounting*, vol. 8, no. 2, pp. 338–348.
- Diksha, J & Hirschi, T 1990, *A general theory of crime*, Stanford University Press, Stanford.
- Dlamini, S & Mbambo, C 2019, 'Understanding policing of cybercrime In South Africa: The phenomena, challenges and effective responses', *Cogent Social Sciences*, vol. 5, a1675404.
- Dlamini, Z & Modise, M 2012, 'Cyber security awareness initiatives in South Africa: A synergy approach', in *7th International Conference on Information Warfare and Security*, Seattle, United States of America, March 22–23, pp. 1–10.
- Donner, CM, Marcum, CD, Jennings, WG, Higgins, GE & Banfield, J 2014, 'Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy', *Computers in Human Behavior*, vol. 34, pp. 165–172. <https://doi.org/10.1016/j.chb.2014.01.040>
- Dorransoro, JR, Ginel, F, Sánchez, C & Cruz, CS 1997, 'Neural fraud detection in credit card operations', *IEEE Transactions on Neural Networks*, vol. 8, no. 4, pp. 827–834. <https://doi.org/10.1109/72.595879>
- Dubey, P 2014, 'Forensic accounting', *International Research Journal of Commerce, Arts and Science*, vol. 5, no. 8, pp. 136–148.
- Dubinina, M, Ksonzhyk, I & Syrtseva, S 2018, 'Forensic accounting: The essence and prospects of development in Ukraine', *Baltic Journal of Economic Studies*, vol. 4, no. 1, pp. 131–138.
- Dutta, A 2007, *Management control system*, Jaico Publishing House, New Delhi.
- Dutta, SK 2013, *Statistical techniques for forensic accounting understanding the theory and application of data analysis*, FT Press, Upper Saddle River, pp. 1–56.
- Dzomira, S 2014, 'Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe', *Risk Governance & Control: Financial Markets & Institutions*, vol. 4, no. 2, pp. 16–26. <https://doi.org/10.22495/rgcv4i2art2>
- Dzomira, S 2015a, 'Cyber-banking fraud risk mitigation conceptual model', *Banks and Bank Systems*, vol. 10, no. 2, pp. 7–14.
- Dzomira, S 2015b, 'Online and electronic fraud prevention and safety tips cognizance in South African banks', *Socioeconomica - The Scientific Journal for Theory and Practice of Socio-Economic Development*, vol. 4, no. 8, pp. 1–14. <https://doi.org/10.12803/SJSECO.48131>
- Dzomira, S 2017, 'Internet banking fraud alertness in the banking sector: South Africa', *Banks and Bank Systems*, vol. 12, no. 1, pp. 143–151. [https://doi.org/10.21511/bbs.12\(1-1\).2017.07](https://doi.org/10.21511/bbs.12(1-1).2017.07)

- Efendi, J, Srivastava, A & Swanson, E 2007, 'Why do corporate managers misstate financial statements? The role of in-the-money options and other incentives', *Journal of Financial Economics*, vol. 85, pp. 667-708. <https://doi.org/10.1016/j.jfineco.2006.05.009>
- Effiok, SO, Ojong, CM & Usang, OUE 2023, 'The implication of occupational fraud and financial abuse on the performance of companies in Nigeria', *Interdisciplinary Journal of Contemporary Research in Business*, vol. 4, no. 7, pp. 516-533.
- Effiong, EJ, Effiong, C, Inyang OI & Ugbajah, DC 2017, 'Opinion and behaviour of Nigerian undergraduate students towards forensic accounting for fraud prevention and detection', *Scholars Journal of Economics, Business and Management*, vol. 4, no. 11, pp. 787-798.
- Efosa, EE & Kingsley, AO 2016, 'Forensic accounting and fraud management: Evidence from Nigeria', *Igbinedion University Journal of Accounting*, vol. 2, no. 8, pp. 245-308.
- E-Governance Academy Report 2022, *National cyber security index*, viewed 17 November 2022, <<https://ncsi.ega.ee/ncsi-index/>>
- Ehioghiren, E & Atu, OOK 2016, 'Forensic accounting and fraud management: Evidence from Nigeria', *Igbinedion University Journal of Accounting*, vol. 2, pp. 245-308.
- Ekeigwe, CC 2011, *Skill sets for forensic accountants*, Institute of Chartered Accountants of Nigeria: Forensic Audit & Investigation Faculty, Lagos.
- Ekina, T, Leva, F, Ruggeri, F & Soyer, R 2013, 'Application of Bayesian methods in detection of healthcare fraud', *Chemical Engineering Transaction*, vol. 33, pp. 151-156.
- Eliezer, O & Emmanuel, B 2015, 'The relevance of forensic accounting in the detection and prevention of fraud in Nigeria', *Historical Research Letter*, vol. 23, pp. 17-20.
- Elkington, J 1997, 'Partnership from cannibals with forks: The triple bottom line of 21st-century business', *Environmental Quality Management*, vol. 8, no. 1, pp. 37-51. <https://doi.org/10.1002/tqem.3310080106>
- Emeh, Y & Obi, JO 2013, 'An empirical analysis of forensic accounting and financial fraud in Nigeria', *African Journal of Social Sciences*, vol. 3, no. 4, pp. 112-121.
- Enofe, AO, Abilogun, TO, Omoolorun, AJ & Elaiho, EM 2017, 'Bank fraud and preventive measures in Nigeria: An empirical review', *International Journal of Academic Research in Business and Social Sciences*, vol. 7, no. 7, pp. 40-51. <https://doi.org/10.6007/IJARBS/v7-i7/3076>
- Enofe, AO, Utomwen, OA & Danjuma, EJ 2015, 'The role of forensic accounting in mitigating financial crimes', *International Journal of Commerce and Management Research*, vol. 1, no. 1, pp. 40-47.
- European Union Report 2002, *Corporate social responsibility main issues*, viewed 24 June 2021. <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_02_153>
- Ezejiofor, RA, Nwakoby, NP & Okoye, JFN 2016, 'Impact of forensic accounting on combating fraud in the Nigerian banking industry', *International Journal of Academic Research in Management and Business*, vol. 1, no. 1, pp. 1-19.
- Fang, LH 2005, 'Investment bank reputation and the price and quality of underwriting services', *The Journal of Finance*, vol. 60, no. 6, pp. 29-61.
- Fanning, KM & Cogger, KO 1997, 'Neural network detection of management fraud using published financial data', *International Journal of Intelligent Systems in Accounting, Finance & Management*, vol. 7, no. 1, pp. 21-41. [https://doi.org/10.1002/\(SICI\)1099-1174\(199803\)7:1%3C21::AID-ISAF138%3E3.3.CO;2-B](https://doi.org/10.1002/(SICI)1099-1174(199803)7:1%3C21::AID-ISAF138%3E3.3.CO;2-B)
- Fassassi, A 2016, 'Cybercrime in Africa: Facts and figures', *Scidenet*, viewed 15 November 2022. <<https://www.scidev.net/subsaharanAfrica/features/cybercrimeAfricafactsfigures/>>
- Federal Bureau of Investigation (FBI) 2019, *Worldwide sweep targets business email compromise*, 10 September 2019, viewed 30 July 2022, <<https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019>>

References

- Feruzza, S & Kim, T 2007, 'IT security review: Privacy, protection, access control, assurance and system security', *International Journal of Multimedia and Ubiquitous Engineering*, vol. 2, no. 2, pp. 17-31.
- Finau, G, Samuwai, J & Prasad, A 2013, 'Cyber crime and its implications to the Pacific', *The Fiji Accountant*, vol. June 2013, pp. 15-16.
- FirstRand Group Ltd 2017, *Annual integrated report*, viewed 16 November 2020, <[https://www.firststrand.co.za/InvestorCentre/Current FSR annual report/FirstRand annual integrated report2017.pdf](https://www.firststrand.co.za/InvestorCentre/Current_FSR_annual_report/FirstRand_annual_integrated_report2017.pdf)>
- FirstRand Group Ltd 2022, *Annual integrated report*, viewed 26 December 2020, <<https://www.firststrand.co.za/media/investors/annual-reporting/firststrand-annual-integrated-report-2022.pdf>>
- Fombrun, CJ 1996, *Reputation: Realizing value from the corporate image*, Harvard Business School Press, Boston.
- Fowler, K 2016, 'Precisely determining the scope of a breach', in *Data breach preparation and response*, Syngress, Rockland, pp. 125-166.
- Fradella, HF, O'Neil, L & Fogarty, A 2004, 'The impact of Daubert on forensic science', *Pepperdine Law*, vol. 31, no. 2, pp. 323-362.
- Franceschetti, BM 2017, *Financial crises and earnings management behavior arguments and evidence against causality*, Contributions to Management Science, Springer, Cham.
- Freeman, E 2010, *Strategic management: A stakeholder approach*, Cambridge University Press, London.
- Freiling, F & Schwittay, B 2007, 'A common process model for incidence response and computer forensics', in *Conference on IT Incident Management and IT Forensics*, IMF, Stuttgart, pp. 1-18.
- Froggio, G 2007, 'Strain and juvenile delinquency: A critical review of Agnew's general strain theory', *Journal of Loss & Trauma*, vol. 12, no. 4, pp. 383-418. <https://doi.org/10.1080/15325020701249363>
- Gady, FS & Austin, G 2010, *Russia, the United States, and cyber diplomacy*, Opening the Doors, EastWest Institute, New York.
- Gai, K, Qiu, M & Zhao, H 2016, 'Security-aware efficient mass distributed storage approach for cloud systems in Big Data Conference session', in M Qiu (ed.), *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data*, IEEE, New York, pp. 140-145.
- Gallet, O 2010, *Halte aux Fraudes: Guide pour Auditeurs et Dirigeants*, 2nd edn., Dunod, Paris.
- Gao, Z & Ye, M 2007, 'A framework for data mining-based anti-money laundering research', *Journal of Money Laundering Control*, vol. 10, no. 2, pp. 170-179. <https://doi.org/10.1108/13685200710746875>
- Gbegi, DO & Adebisi, JF 2014, 'Forensic accounting skills and techniques in fraud investigation in the Nigeria public sector', *Mediterranean Journal of Social Sciences*, vol. 5, no. 3, pp. 243-252. <https://doi.org/10.5901/mjss.2014.v5n3p243>
- Geerts, GL & McCarthy, WE 2022, 'An ontological analysis of the economic primitives of the extended REA enterprise information architecture', *International Journal of Accounting Information Systems*, vol. 3, pp. 1-16. [https://doi.org/10.1016/S1467-0895\(01\)00020-3](https://doi.org/10.1016/S1467-0895(01)00020-3)
- George, G, Haas, MR & Pentland, A 2014, 'Big data and management', *Academy of Management Journal*, vol. 57, no. 2, pp. 321-326. <https://doi.org/10.5465/amj.2014.4002>
- Gerson, JS, Brolly, JP & Skalak, SL 2011, 'The role of auditor and forensic accounting investigator', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 37-61.

- Gherghina, SC & Vintilă, G 2016, 'Exploring the impact of corporate social responsibility policies on firm value: The case of listed companies in Romania', *Economics & Sociology*, vol. 9, no. 1, pp. 23–42. <https://doi.org/10.14254/2071-789X.2016/9-1/2>
- Global Cybersecurity Index (GCI) 2017, *Africa report*, viewed 28 February 2023. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_GCIv2_report.pdf>
- Godfrey, PC, Merrill, CB & Hansen, JM 2009, 'The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis', *Strategic Management Journal*, vol. 30, no. 4, pp. 425–445. <https://doi.org/10.1002/smj.750>
- Goel, S & Shawky, HA 2009, 'Estimating the market impact of security breach announcements on the firm values', *Information and Management*, vol. 46, no. 7, pp. 404–410. <https://doi.org/10.1016/j.im.2009.06.005>
- Golden, TW & Murphy, RD 2011, 'Report of investigation', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 363–387.
- Golden, TW, Skalak, SL & Clayton, MM 2006, *A guide to forensic accounting investigation*, John Wiley and Sons, New York.
- Gond, J-P, Grubnic, S, Herzig, C & Moon, J 2012, 'Configuring management control systems: Theorizing the integration of strategy and sustainability', *Management Accounting Research*, vol. 23, pp. 205–223. <https://doi.org/10.1016/j.mar.2012.06.003>
- Gottschalk, P 2010, 'Categories of financial crime', *Journal of Financial Crime*, vol. 17, no. 4, pp. 441–458. <https://doi.org/10.1108/13590791011082797>
- Grant, C & Osanloo, A 2014, 'Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for "house"', *Administrative Issues Journal: Connecting Education, Practice and Research*, vol. 4, no. 2, pp. 12–22. <https://doi.org/10.5929/2014.4.2.9>
- Green, P & Choi, JH 1997, 'Assessing the risk of management fraud through neural network technology', *Auditing: A Journal of Practice & Theory*, vol. 16, no. 1, pp. 14–28.
- Grippio, FJ & Ibex, JW 2003, *Introduction to forensic accounting*, The National Public Accountant, Washington DC.
- Grobler, T & Louwrens, CP 2009, *High-level integrated view of digital forensics*, University of Johannesburg, Johannesburg, pp. 1–20.
- Grubor, G, Ristić, N & Simeunović, N 2013, 'Integrated forensic accounting investigative process modeling digital environment', *International Journal of Scientific and Research Publications*, vol. 3, no. 12, pp. 1–10.
- Guan, Y 2009, 'Network forensics', in JR Vaca (ed.), *Computer and information security*, 3rd edn., Morgan Kaufmann Publishers, Burlington, pp. 339–347.
- Gumbi, D 2017, 'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom', LLM thesis, University of Cape Town, Cape Town.
- Gurel, E & Tat, M 2017, 'SWOT analysis: A theoretical review', *The Journal of International Social Research*, vol. 10, no. 51, pp. 994–1006. <https://doi.org/10.17719/jisr.2017.1832>
- Hamdan, MW 2017, 'The role of forensic accounting in discovering financial fraud', *International Journal Accounting Research*, vol. 6, no. 2, pp. 1–6.
- Hamilton, DI & Justin, MOG 2012, 'Dimensions of fraud in Nigeria quoted firms', *American Journal of Social Science*, vol. 3, no. 3, pp. 112–120. <https://doi.org/10.5251/ajssms.2012.3.3.112.120>
- Hao, X 2010, 'Analysis of the necessity to develop forensic accounting in China', *International Journal of Business and Management*, vol. 5, no. 5, p. 185. <https://doi.org/10.5539/ijbm.v5n5p185>
- Harris, LC & Dumas, A 2009, 'Online consumer misbehavior: An application of neutralization theory', *Marketing Theory*, vol. 9, no. 4, pp. 379–402. <https://doi.org/10.1177/1470593109346895>

References

- Hasham, S, Joshi, S & Mikkelsen, D 2019, *Financial crime and fraud in the age of cybersecurity*, viewed 07 July 2021, <<https://www.mckinsey.com/-/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf>>
- Hassan, EZ & Morteza, R 2012, 'Accountant's perception of forensic accounting', *Global Journal of Management and Business Research*, vol. 12, no. 6, pp. 1-4.
- Hauser, MD 2006, *Moral minds: How nature designed our universal sense of right and wrong*, Harper Collins, New York.
- Hawdon, J, Bernatzky, C & Costello, M 2019, 'Cyber-routines, political attitudes, and exposure to violence-advocating online extremism', *Social Forces*, vol. 98, no. 1, pp. 329-354. <https://doi.org/10.1093/sf/soy115>
- Hay, C & Meldrum, R 2010, 'Bullying victimization and adolescent self-harm: Testing hypotheses from general strain theory', *Journal of Youth and Adolescence*, vol. 39, pp. 446-459. <https://doi.org/10.1007/s10964-009-9502-0>
- Hay, C, Meldrum, R & Mann, K 2010, 'Traditional bullying, cyberbullying, and deviance: A general strain theory approach', *Journal of Contemporary Criminal Justice*, vol. 26, no. 2, pp. 130-147. <https://doi.org/10.1177/1043986209359557>
- Hayles, A 2020, *Forensic accounting*, viewed 27 January 2022, <<https://www.investopedia.com/terms/f/forensicaccounting.asp#:~:text=What%20is%20Forensic%20Accounting%3F,of%20an%20individual%20or%20business.&text=Forensic%20accounting%20is%20frequently%20used,a%20financial%20crime%20in%20court>>
- He, HW, Graco, JW & Hawkins, S 1997, 'Application of neural networks to detection of medical fraud', *Expert Systems with Applications*, vol. 13, no. 4, pp. 329-336. [https://doi.org/10.1016/S0957-4174\(97\)00045-6](https://doi.org/10.1016/S0957-4174(97)00045-6)
- Hecht, M & Redmond, M 2012, 'Unveiling the mystery of forensic accounting: Oregon society of certified public accountants', *Accounting Today*, viewed 12 November 2019, <www.orcpa.org>
- Hedayati, A 2012, 'An analysis of identity theft: Motives, related frauds, techniques and prevention', *Journal of Law and Conflict Resolution*, vol. 4, no. 1, pp. 1-12.
- Hegazy, S, Sangster, A & Kotb, A 2017, 'Mapping forensic accounting in the UK', *Journal of International Accounting, Auditing and Taxation*, vol. 28, pp. 43-56. <https://doi.org/10.1016/j.intaccudtax.2016.12.004>
- Henri, JF & Journeault, MA 2010, 'Eco-control: The influence of MCS on environmental and economic performance', *Accounting, Organizations and Society*, vol. 35, pp. 63-80. <https://doi.org/10.1016/j.aos.2009.02.001>
- Herselman, M & Warren, M 2004, 'Cyber crime influencing businesses in South Africa', *Issues in Informing Science and Information Technology*, vol. 1, pp. 253-266. <https://doi.org/10.28945/736>
- Hibshi, HA, Vidas, T & Cranor, L 2011, 'Usability of forensics tools: A user study', in H Morgenstern, R Ehlert, S Frings, O Goebel, D Guenther, S Kiltz, J Nedon & D Schadt (eds.), *Sixth International Conference on IT Security Incident Management and IT Forensics*, IEEE Computer Society, Stuttgart, May 10-12, pp. 81-91.
- Hinde, S 2003, 'Computer security: Mapping the future', *Computers and Security*, vol. 22, no. 8, pp. 664-669. [https://doi.org/10.1016/S0167-4048\(03\)00003-8](https://doi.org/10.1016/S0167-4048(03)00003-8)
- Hinders, D 2009, *What is forensic accounting?*, viewed 12 June 2021, <<http://www.wisageek.com>>
- Hinduja, S 2006, *Music piracy and crime theory*, LFB Scholarly, New York.
- Hinduja, S 2012, 'General strain, self-control and music piracy', *International Journal of Cybercriminology*, vol. 6, no. 1, pp. 951-967.
- Hirschi, T & Gottfredson, MR 1993, 'Age and the explanation of crime', *American Journal of Sociology*, vol. 89, no. 3, pp. 552-584. <https://doi.org/10.1086/227905>

- Hitchcock, M 2017, 'The importance and implications of forensic accounting in the financial world', Long Island University Digital Commons Undergraduate Honors College Theses, pp. 1-60.
- Holappa, J, Ahonen, P, Eronen, J, Kajava, J, Kaksonen, T, Karjalainen, K, Koivisto, J-P, Kuusela, E, Ollikainen, V, Rapeli, M, Sademies, A & Savola, R 2005, 'Information security threats and solutions in digital television: The service developer's perspective', *VTT Electronics Research Notes*, vol. 2306, pp. 1-81, viewed 04 May 2021, <<https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2005/T2306.pdf>>
- Hollinger, RC & Clark, JP 1983, *Theft by employees*, Lexington Books, Lexington.
- Holt, TJ & Bossler, AM 2009, 'Examining the applicability of lifestyle-routine activities theory for cybercrime victimization', *Deviant Behavior*, vol. 30, no. 1, pp. 1-25. <https://doi.org/10.1080/01639620701876577>
- Holt, TJ, Burrus, GW & Bossler, AM 2010, 'Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world', *Journal of Crime and Justice*, vol. 33, no. 2, pp. 31-61. <https://doi.org/10.1080/0735648X.2010.9721287>
- Honigsberg, C 2020, 'Forensic accounting', *Annual Review of Law and Social Science*, vol. 16, pp. 147-164. <https://doi.org/10.1146/annurev-lawsocsci-020320-022159>
- Hooper, MJ & Pornelli, CM 2010, *Deterring and detecting financial fraud: A platform for action*, viewed 02 August 2021, <<http://www.thecaq.org/docs/reports-andpublications/deterring-and-detecting-financialreporting-fraud-aplatform-for-action.pdf>>
- Hopkin, P 2010, *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*, Kogan Page Limited, London.
- Houck, MM, Kranacher, M-J, Morris, B & Riley, RA, Jr 2006, 'Forensic accounting as an investigative tool', *The CPA Journal*, vol. 76, no. 8, p. 68.
- Howard, S & Sheetz, M 2006, *Forensic accounting and fraud investigation for non-experts*, John Wiley & Sons, Hoboken.
- Huang, Y 2005, 'The essentials of organisation management', *Management and Organisation Review*, vol. 1, no. 2, pp. 329-333. <https://doi.org/10.1111/j.1740-8784.2005.00017.x>
- Huber, W 2012, 'Is forensic accounting in the United States becoming a profession?', *Journal of Forensic and Investigative Accounting*, vol. 4, no. 1, pp. 255-284.
- Hunton, P 2009, 'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model', *Computer Law & Security Review*, vol. 25, no. 6, pp. 528-535. <https://doi.org/10.1016/j.clsr.2009.09.005>
- Hutchings, A 2013, 'Hacking and fraud: Qualitative analysis of online offending and victimization', in *Global criminology: Crime and victimization in the globalized era*, CRC Press, Boca Raton, pp. 93-114.
- Idolor, EJ 2010, 'Bank frauds in Nigeria: Underlying causes, effects and possible remedies', *African Journal of Accounting, Economics, Finance and Banking Research*, vol. 6, no. 6, pp. 62-80.
- Ijeoma, N & Aronu, CO 2013, 'The impact of fraud management on organisational survival in Nigeria', *American Journal of Economics*, vol. 3, no. 6, pp. 268-272.
- Ikpefan, OA 2007, *Growth of bank frauds and the impact on the Nigerian banking industry*, viewed 19 September 2019, <<http://eprints.covenantuniversity.edu.ng/1316/1/FRAUD.pdf>>
- Imenda, S 2014, 'Is there a conceptual difference between conceptual and theoretical frameworks?', *Journal of Social Science*, vol. 38, no. 2, pp. 185-195. <https://doi.org/10.1080/09718923.2014.11893249>
- Information Security Institute 2013, *Impact of cybercrime*, viewed 16 November 2022, <<https://resources.infosecinstitute.com/topic/2013-impact-cybercrime/>>
- Institute of Internal Auditors 2009, *International professional practices framework, practice guide: Internal auditing and fraud*, viewed 25 March 2021, <https://www.academia.edu/36393289/IPPF_Practice_Guide_Internal_audItInG_and_Fraud>

References

- International Anti-Corruption Resource Centre (IACRC) 2022, *Guide to combating corruption and fraud in development projects*, viewed 10 February 2022, <<https://guide.iacrc.org/the-basics-of-evidence-for-fraud-and-corruption-investigators/>>
- International Finance Corporation 2020, *e-Conomy Africa 2020 – Africa’s \$180 Billion internet economy future*, viewed 28 February 2023, <https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy>
- International Organisation for Standardization (ISO) 2018, *ISO/IEC 27005:2011(en) information technology – Security techniques – Information security risk management*, viewed 16 July 2021, <<https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>>
- INTERPOL 2020, *INTERPOL report shows alarming rate of cyberattacks during COVID-19*, 04 August, viewed 18 November 2022, <<https://www.interpol.int/en/>>
- Ismail, M 2009, 'Corporate social responsibility and its role in community development: An international perspective', *The Journal of International Social Research*, vol. 2, no. 9, pp. 200–209.
- Ivezic, M 2017, *Cybercrime in China – A growing threat for the Chinese economy*, viewed 02 April 2021, <<https://www.linkedin.com/pulse/cybercrime-china-growing-threatchinese-economy-marin-ivezic>>
- Izedonmi, F & Ibadin, PO 2012, 'Forensic accounting and financial crimes: Adopting the inference, relevance and logic solution approach', *African Research Review: An International Multidisciplinary Journal, Ethiopia*, vol. 6, no. 4, pp. 27, 125–139. <https://doi.org/10.4314/afrr.v6i4.9>
- Jadhao, A & Agarwal, A 2016, 'Digital forensics investigation model for social networking site', in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, Udaipur, India, 04–05 March.
- Jain, N & Kalbande, D 2015, 'Digital forensic framework using feedback and case history keeper', in *Proceedings of the 2015 International Conference on Communication, Information, and Computing Technology*, Mumbai, India, 2015. <https://doi.org/10.1109/ICCICT.2015.7045670>
- Jamali, D & Neville, B 2011, 'Convergence versus divergence of CSR in developing countries: An embedded multi-layered institutional lens', *Journal of Business Ethics*, vol. 102, no. 4, pp. 599–621. <https://doi.org/10.1007/s10551-011-0830-0>
- Jans, M, Alles, M & Vasarhelyi, M 2014, 'A field study on the use of process mining of event logs as an analytical procedure in auditing', *The Accounting Review*, vol. 89, no. 5, pp. 1751–1773. <https://doi.org/10.2308/accr-50807>
- Jansen, W & Ayers, R 2007, 'Guidelines on cell phone forensics', *NIST Special Publication*, vol. 800, p. 101. <https://doi.org/10.6028/NIST.SP.800-101>
- Jegade, AE 2014, 'Cyber fraud, global trade and youth crime burden: Nigerian experience', *Afro-Asian Journal of Social Sciences*, vol. V, no. IV, pp. 1–21.
- Jegade, AE, Olowookere, IE & Elegbeleye, AO 2016, 'Youth identity, peer influence and internet crime participation in Nigeria: A reflection', *Ife Psychology*, vol. 24, no. 1, pp. 37–47.
- Jhawar, R & Piuri, V 2017, 'Fault tolerance and resilience in cloud computing environments', in JR Vacca (ed.), *Computer and information security handbook*, Morgan Kaufmann Publishers, Burlington, pp. 165–181.
- Johnson, SA, Ryan, HE & Tian, YS 2003, 'Executive compensation and corporate fraud', Working Paper, Louisiana State University, Baton Rouge.
- Johnson, SA, Ryan, HE, Jr & Tian, YS 2009, 'Managerial incentives and corporate fraud: The sources of incentives matter', *Review of Finance*, vol. 13, pp. 115–145. <https://doi.org/10.1093/rof/rfn014>
- Kadiri, KO 2014, 'The prospects and problems of information technology in the banking sector in Nigeria', *IOSR Journal of Computer Engineering*, vol. 16, no. 5, pp. 28–35. <https://doi.org/10.9790/0661-16562835>

- Kamande, RW, Kiragu, D & Musumba, G 2017, 'Internal controls, staff red flags and computerized financial fraud among commercial banks in Kenya', *International Journal of Economics, Commerce and Management*, vol. VI, no. 5, pp. 95-111.
- Kampen, J & Swyngedouw, M 2000, 'The ordinal controversy revisited', *Quality & Quantity*, vol. 34, pp. 87-102. <https://doi.org/10.1023/A:1004785723554>
- Kanali, N 2022, *Uganda parliament passes new law to curb cyber crime*, viewed 28 February 2023, <<https://africabusinesscommunities.com/tech/tech-news/uganda-parliament-passes-new-law-to-curb-cyber-crime/#:-:text=The%20Ugandan%20Parliament%20has%20passed,strengthen%20the%20growing%20technology%20sector>>
- Kantarcioglu, M & Shaon, F 2019, 'Securing big data in the age of AI conference session', in *Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2019*, Los Angeles, California, United States of America, 12-14 December.
- Kanu, C & Idume, GI 2016, 'Security challenge, bank fraud and commercial bank performance in Nigeria: An evaluation', *Journal of Business and Management*, vol. 5, no. 2, pp. 1-21.
- Kanu, SI & Okorafor, EO 2013, 'The nature, extent and economic impact of fraud on bank deposits in Nigeria', *Interdisciplinary Journal of Contemporary Research in Business*, vol. 4, no. 9, pp. 253-265.
- Kargbo, L 2021, *Parliament of Sierra Leone enact cyber crime bill*, viewed 28 February 2023, <https://www.switsalone.com/39316_parliament-of-sierra-leone-enacts-the-cyber-crime-bill/>
- Karwai, M 2004, *Forensic accounting and fraud investigation for non-experts*, John Wiley & Sons, Hoboken.
- Kasap, M 2013, 'Forensic accountancy profession and conflict with absolute crime', *FEAS Magazine*, vol. 3, no. 1, pp. 121-132.
- Kaur, J 2022, *Data preprocessing and data wrangling in machine learning*, viewed 17 December 2022, <<https://www.xenonstack.com/blog/data-preprocessing-wrangling-ml>>
- Kelly, P & Hartley, CA 2010, 'Casino gambling and triangle, workplace fraud: A cautionary tale for managers', *Management Research Review*, vol. 33, no. 3, pp. 224-239. <https://doi.org/10.1108/01409171011030381>
- Kent, K, Chavallier, S, Grance, T & Dang, H 2006, *Guide to integrating forensics into incidence response*, Technology Administration, US Department of Commerce, Gaithersburg, pp. 1-121.
- Kenton, W 2002, *Sarbanes-Oxley act: What it does to protect investors*, viewed 26 October 2021, <<https://www.investopedia.com/terms/s/sarbanesoxleyact.asp>>
- Kenton, W 2022, *Standard error (SE) definition: Standard deviation in statistics explained*, viewed 21 January 2023, <<https://www.investopedia.com/terms/s/standard-error.asp>>
- Kenyon, W & Tilton, PD 2006, *Potential red flags and fraud detection techniques, a guide to forensic accounting investigation*, 1st edn., TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), John Wiley & Sons, Hoboken.
- Kenyon, W & Tilton, PD 2011, 'Potential red flags and fraud detection technique', in SL Skalak, MM Clayton, JS Pill & TW Golden (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 231-269.
- Khan, H 2011, 'A literature review of corporate governance', *International Conference on E-business, Management and Economics*, vol. 25, pp. 1-5.
- Khan, SA, Kusi-Sarpong, S, Arhin, FK & Kusi-Sarpong, H 2017, 'Supplier sustainability performance evaluation and selection: A framework and methodology', *Journal of Cleaner Production*, vol. 205, pp. 964-979. <https://doi.org/10.1016/j.jclepro.2018.09.144>
- Khatir, M & Hejazi, SM 2007, 'How to find exculpatory and inculpatory evidence using a circular digital forensics process model', in H Jahankhani, K Revett & D Palmer-Brown (eds.), *Global e-security. ICGeS 2008, Communications in computer and information science*, vol. 12, Springer, Berlin, pp. 10-17.

- Khersiat, OM 2017, 'The role of forensic accounting in maintaining public money and combating corruption in the Jordanian public sector', *International Business Research*, vol. 11, no. 3, pp. 66–75. <https://doi.org/10.5539/ibr.v11n3p66>
- Khojastehpour, M & Johns, R 2014, 'The effect of environmental CSR issues on corporate/brand reputation and corporate profitability', *European Business Review*, vol. 26, no. 4, pp. 330–339. <https://doi.org/10.1108/ebr-03-2014-0029>
- Khumalo, K 2017, 'Nedbank opens first digital-only branch', *Personal Finance*, viewed 16 November 2020, <<https://www.iol.co.za/personal-finance/nedbank-opens-first-digital-only-branch-11959803>>
- Kim, HY 2017, *Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test*, Open Lecture on Statistics, The Korean Academy of Conservative Dentistry, Seoul, pp. 152–155. <https://doi.org/10.5395/rde.2017.42.2.152>
- Kimani, J 2011, *Fraud risk assessment plan for Barclays Bank of Kenya*, Tampere University of Applied Sciences, Tampere.
- King, T 2021, *The 8 best data quality tools and software for 2022*, viewed 17 December 2022, <<https://solutionsreview.com/data-management/the-best-data-quality-tools-and-software/>>
- Kirlidog, M & Asuk, C 2012, 'A fraud detection approach with data mining in health insurance', *Procedia-Social and Behavioral Sciences*, vol. 62, pp. 989–994. <https://doi.org/10.1016/j.sbspro.2012.09.168>
- Kitchenham, B, Brereton, OP, Budgen, D, Turner, M, Bailey, J & Linkman, S 2009, 'Systematic literature reviews in software engineering – A systematic literature review', *Information and Software Technology*, vol. 51, no. 1, pp. 7–15. <https://doi.org/10.1016/j.infsof.2008.09.009>
- Kloot, L 1997, 'Organisational learning and management control systems: Responding to environmental change', *Management Accounting Research*, vol. 7, pp. 47–73. <https://doi.org/10.1006/mare.1996.0033>
- Ko, M & Dorantes, C 2006, 'The impact of information security breaches on the financial performance of the breached firms: An empirical investigation', *Information Resources Management Journal*, vol. 2, pp. 17–22.
- Koay, KY 2017, 'Understanding consumers' purchase intention towards counterfeit luxury goods: An integrated model of neutralization techniques and perceived risk theory', *Asia Pacific Journal of Marketing and Logistics*, vol. 30, no. 2, pp. 495–516. <https://doi.org/10.1108/APJML-05-2017-0100>
- Köhn, M, Olivier, MS & Eloff, JH 2006, 'Framework for a digital forensic investigation', in *ISSA*, July, pp. 1–7.
- Kopp, E, Kaffenberger, L & Wilson, C 2017, 'Cyber risk, market failures, and financial stability', IMF Working Paper No. 17/185, IMF, Washington DC, pp. 1–36.
- Kornfeldova, M 2011, 'Equal opportunities in the concept of corporate social responsibility', *Scientific Papers of the University of Pardubice*, vol. 21, no. 3, pp. 102–109.
- Kornfeldová, M & Myšková, R 2012, 'Application of CSR in the construction industry', in *Proceedings of the 1st International Conference on Economics, Political and Law Science (EPLS '122012 [September 20–2][2])*, Zlin.
- Kotabe, HP & Hofmann, W 2015, 'On integrating the components of self-control', *Perspectives on Psychological Science*, vol. 10, no. 5, pp. 618–638. <https://doi.org/10.1177/1745691615593382>
- Kovalerchuk, B, Vityaev, E & Holtfreter, R 2007, 'Correlation of complex evidence in forensic accounting using data mining', *Journal of Forensic Accounting*, vol. VIII, no. 1, pp. 1–36.
- KPMG 2010, *Fraud and misconduct survey, Austria and New Zealand*, pp. 1–48, viewed 16 July 2021, <<https://www.google.com/search?ei>>
- KPMG 2011, *Cyber crime – A growing challenge for governments*, vol. 8, pp. 1–24, viewed 01 August 2022, <[KPMG_INTERNATIONAL_Issues_Monitor_Cyber.pdf](https://www.kpmg.com/au/issuesandinsights/articlespublications/cyber-crime-a-growing-challenge-for-governments)>

- KPMG 2012, *Cybercrimes: A financial sector overview*, viewed 02 February 2022, <www.kpmg.com/in>
- KPMG 2018, *UK Finance: Staying ahead of cybercrime*, viewed 02 February 2020, <www.ukfinance.org.uk>
- KPMG 2019, *The multifaceted threat of fraud: Are banks up to the challenge?*, Global Banking Fraud Survey, viewed 02 February 2021, <<https://kpmg.com/dp/en/home/insights/2020/02/the-multi-faceted-threat-of-fraud.html>>
- Kraemer-Mbula, E, Tang, P & Rush, H 2013, 'The cybercrime ecosystem: Online innovation in the shadows?', *Technological Forecasting and Social Change*, vol. 80, no. 3, pp. 541-555. <https://doi.org/10.1016/j.techfore.2012.07.002>
- Kramer, B, Seda, M & Bobashev, G 2017, 'Current opinions on forensic accounting education', *Accounting Research Journal*, vol. 30, no. 3, pp. 249-264. <https://doi.org/10.1108/ARJ-06-2015-0082>
- Krausert, A 2009, *Performance management for different employee groups: A contribution to the employment systems theory*, Springer-Verlag, Heidelberg.
- Kresse, WJ 2007, 'The Saint Xavier University graduate program in financial fraud examination and management', *Issues in Accounting Education*, vol. 23, no. 4, pp. 601-608. <https://doi.org/10.2308/iace.2008.23.4.601>
- Kritzinger, E & Van Solms, SH 2012, 'A framework for cyber security in Africa', *Journal of Information Assurance and Cyber-security*, 2012 vol., pp. 1-10. <https://doi.org/10.5171/2012.322399>
- Krstic, J 2009, 'The role of forensic accountants in detecting fraud in financial statements', *Economics and Organization*, vol. 6, no. 3, pp. 295-302.
- Kshetri, N 2015, 'Cybercrime and cybersecurity issues in the BRICS economies', *Journal of Global Information Technology Management*, vol. 18, no. 4, pp. 1-5. <https://doi.org/10.1080/1097198X.2015.1108093>
- Kshetri, N 2019, 'Cybercrime and cybersecurity in Africa', *Journal of Global Information Technology Management*, vol. 22, no. 2, pp. 77-81. <https://doi.org/10.1080/1097198X.2019.1603527>
- Kubi, AK, Saleem, S & Popov, O 2011, 'Evaluation of some tools for extracting e-evidence from mobile devices', in *Proceedings of the 2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, IEEE, Baku, October 12-14, pp. 1-6.
- Kumar, M, Ghani, R & Mei, ZS 2010, 'Data mining to predict and prevent errors in health insurance claims processing', in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington DC, United States of America, July 25-28, pp. 65-74.
- Kumudha, S & Rajan, A 2018, 'A critical analysis of cyber phishing and its impact on the banking sector', *International Journal of Pure and Applied Mathematics*, vol. 119, no. 17, pp. 1557-1569.
- Kweyu, M & Ngare, P 2013, 'Factor analysis of customers' perception of mobile banking services in Kenya', *Journal of Emerging Trends in Economics and Management Sciences*, vol. 5, no. 1, pp. 1-8.
- Kwok, BKB 2007, *Forensic accountancy*, 2nd edn., LexisNexis, Hong Kong, pp. 1-364.
- Lagazio, M, Sherif, N & Cushman, M 2014, 'A multi-level approach to understanding the impact of cybercrime on the financial sector', *Computers and Security*, vol. 45, pp. 58-74. <https://doi.org/10.1016/j.cose.2014.05.006>
- Lakshmi, P & Ganesh, M 2016, 'Forensic accounting: A checkmate for corporate fraud', *Journal of Modern Accounting and Auditing*, vol. 12, no. 9, pp. 453-460. <https://doi.org/10.17265/1548-6583/2016.09.002>
- Lalit, W & Virender, P 2012, 'Forensic accounting and fraud examination in India', *International Journal of Applied Engineering Research*, vol. 7, no. 11, pp. 171-177.

References

- Lallie, HS, Shepherd, LA, Nurse, JR, Erola, A, Epiphaniou, G, Maple, C & Bellekens, X 2021, 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Computers & Security*, vol. 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Langfield-Smith, K 1997, 'Management control systems and strategy: A critical review', *Accounting, Organisations and Society*, vol. 22, no. 2, pp. 207-232. [https://doi.org/10.1016/S0361-3682\(95\)00040-2](https://doi.org/10.1016/S0361-3682(95)00040-2)
- Lazarus, S 2017, 'Birds of a feather flock together: The Nigerian cyber fraudsters (yahoo boys) and hip hop artists', *Criminology, Criminal Justice, Law & Society*, vol. 19, no. 2, pp. 63-80. <https://doi.org/10.1177/1748895817741519>
- Lea, D & Bradbery, J 2020, 'Fraud', in D Lea (ed.), *Oxford advanced learner's dictionary*, 10th edn., Oxford University Press, London, pp. 1-1150.
- Lebanidze, E 2011, *Guide to developing a Cyber Security and risk mitigation plan*, National Rural Electric Cooperative Association, Arlington, viewed 28 May 2021, <<https://www.cooperative.com/programs-services/bts/documents/guide-cybersecurity-mitigation-plan.pdf>>
- Leedom, J, Treccagnoli, P & Martston, DL 2011, 'Contract compliance', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., PricewaterhouseCoopers, New York, pp. 571-583.
- Lehrer, C, Wieneke, A, Vom Brocke, J, Jung, R & Seidel, S 2018, 'How big data analytics enables service innovation: Materiality, affordance, and the individualization of service', *Journal of Management Information Systems*, vol. 35, no. 2, pp. 424-460. <https://doi.org/10.1080/07421222.2018.1451953>
- Leo, M, Sharma, S & Maddulety, K 2019, 'Machine learning in banking risk management: A literature review', *Risks*, vol. 7, no. 29, pp. 1-21. <https://doi.org/10.3390/risks7010029>
- Leong, R 2006, 'FORZA - Digital forensics investigation framework that incorporates legal issues', *Digital Investigation*, vol. 3, pp. 29-36. <https://doi.org/10.1016/j.diin.2006.06.004>
- Lessambo, FI 2014, 'Management fraud', in *The international corporate governance system*, Global Financial Market Series, Palgrave Macmillan, London, pp. 326-338.
- Leukfeldt, ER & Yar, M 2016, 'Applying routine activity theory to cybercrime: A theoretical and empirical analysis', *Deviant Behaviour*, vol. 37, no. 3, pp. 263-280. <https://doi.org/10.1080/01639625.2015.1012409>
- LexisNexis Risk Solutions 2020, *True cost of financial crime compliance*, viewed 29 April 2020, <www.riskscreen.com>
- LexisNexis Risk Solutions 2022, *Balancing risks and reward: The new mobile battlefield*, viewed 15 November 2022, <<file:///C:/Users/daniyania/Downloads/Cybercrime%20Report%20Jul-Dec%202021%20%20Infographic%20%20UKI%20pdf.pdf>>
- Li, L, Fan, F, Ma, L & Tang, Z 2016, 'Energy utilization evaluation of carbon performance in public projects by FAHP and cloud model', *Sustainability*, vol. 8, no. 630, pp. 1-18. <https://doi.org/10.3390/su8070630>
- Li, Y & Liu, Q 2021, 'A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments', *Energy Reports*, vol. 7, pp. 8176-8186. <https://doi.org/10.1016/j.egyr.2021.08.126>
- Liberati, A, Altman, DG, Tetzlaff, J, Mulrow, C, Gøtzsche, PC, Ioannidis, JPA, Clarke, M, Devereaux, PJ, Kleijnen, J & Moher, D 2009, 'The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration', *PLoS Medicine*, vol. 6, no. 7, a1000100. <https://doi.org/10.1371/journal.pmed.1000100>
- Little, PL & Little, BL 2000, 'Do perceptions of corporate social responsibility contribute to explaining differences in corporate price-earnings ratios? A research note', *Corporate Reputation Review*, vol. 3, pp. 137-142.

- Lin, JW, Hwang, MI & Becker, JD 2003, 'A fuzzy neural network for assessing the risk of fraudulent financial reporting', *Managerial Auditing Journal*, vol. 18, no. 8, pp. 657-665. <https://doi.org/10.1108/02686900310495151>
- Lister, LM 2007, 'A practical approach to fraud risk: Comprehensive risk assessments can enable auditors to focus antifraud efforts on areas where their organization is most vulnerable', *Internal Auditor*, vol. 64, no. 6, pp. 61-66.
- Liu, H & Cocea, M 2015, *Rule-based systems for big data: A machine learning approach*, Studies in Big Data, Springer, Cham, p. 13.
- Liu, Q & Vasarhelyi, M 2013, 'Healthcare fraud detection: A survey and a clustering model incorporating Geo-location information', in *Proceedings of the 29th World Continuous Auditing and Reporting Symposium (29WCARS)*, Brisbane, Australia, November 21-22, pp. 1-10.
- Lohana, PM 2013, 'Forensic accounting - At nascent stage in India', *Voice of Research*, vol. 2, no. 1, pp. 63-65.
- Lombardi, R, De Villiers, C, Moscariello, N & Pizzo, M 2021, 'The disruption of blockchain in auditing - A systematic literature review and an agenda for future research', *Accounting, Auditing & Accountability Journal*, vol. 35, no. 7, pp. 1534-1565. <https://doi.org/10.1108/AAAJ-10-2020-4992>
- Lombroso, C 1876, *L'Uomo delinquente*, Hoepli, Milano.
- Louwers, TJ 2015, 'The past, present, and future (?) of crime-related forensic accounting methodology', *Accounting Research Journal*, vol. 28, no. 1, pp. 4-9. <https://doi.org/10.1108/ARJ-04-2015-0047>
- Lucian, V 2004, 'A conceptual framework of e-fraud control in an integrated supply chain', *European Conference on Information System (ECIS) Proceedings*, vol. 161, pp. 1-9.
- Luka, MK & Frank, IA 2012, 'The impacts of ICTs on banks: A case study of the Nigerian banking industry', *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 9, pp. 145-149. <https://doi.org/10.14569/IJACSA.2012.030921>
- Mac, F 2015, *Fraud mitigation best practices*, viewed 07 July 2022, <www.freddiemac.com>
- Madumere, I & Onumah, J 2013, 'Forensic accounting: A relief to corporate fraud', *Research Journal of Finance and Accounting*, vol. 4, no. 14, pp. 43-50.
- Magrath, L & Weld, L 2002, 'Abusive earnings management and early warning signs', *The CPA Journal*, vol. 72, no. 8, pp. 50-55.
- Makgatho, KE 2013, 'Effectiveness of internal control mechanisms in monitoring financial resources at the Gauteng Department of Education', Master's degree thesis, Vaal Triangle Campus of North-West University.
- Malik, MS & Islam, U 2019, 'Cybercrime: An emerging threat to the banking sector of Pakistan', *Journal of Financial Crime*, vol. 26, no. 1, pp. 50-60. <https://doi.org/10.1108/JFC-11-2017-0118>
- Malik, S, Noreen, S & Awan, AG 2017, 'The impact of cybercrimes on the efficiency of the banking sector of Pakistan', *Global Journal of Management, Social Sciences and Humanities*, vol. 4, no. 4, pp. 821-842.
- Manurung, D & Hadian, N 2013, 'Detection fraud of financial statement with fraud triangle', in *Proceedings of 23rd International Business Research Conference*, Marriott Hotel, Melbourne, April 09-10, pp. 18-20.
- Markman, MS, Levko, A, Haller, MW, Dennis, RW, Clayton, MM, Dineen, JC, Decker, D & Sims, S 2011, 'Other dimensions of forensic accounting', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 585-591.
- Martin, N & Rice, J 2011, 'Cybercrime: Understanding and addressing the concerns of stakeholders', *Computers and Security*, vol. 30, no. 8, pp. 803-814. <https://doi.org/10.1016/j.cose.2011.07.003>

References

- Mbelli, TM & Dwolatzky, B 2016, 'Cyber security, a threat to cyber banking in South Africa: An approach to network and application security', in *Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing*, Beijing, China, 25-27 June.
- McAfee, A & Brynjolfsson, E 2012, 'Big data: The management revolution', *Harvard Business Review*, October, pp. 60-66.
- McGuire, M & Dowling, S 2013, *Cybercrime: A review of the evidence*, viewed 05 April 2022, <<https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf>>
- Mcintyre, J-L, Van Graan, C, Van Romburgh, J & Van Zyl, A 2014, 'Contextualizing the South African forensic accountant', *Journal of Forensic & Investigative Accounting*, vol. 6, no. 3, pp. 98-153.
- Mckinsey Global Institute 2011, *Big data: The next frontier for innovation, competition, and productivity*, viewed 06 December 2022, <<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation>>
- McMullan, JL & Rege, A 2010, 'Online crime and internet gambling', *Journal of Gambling Issues*, vol. 24, pp. 54-85. <https://doi.org/10.4309/jgi.2010.24.5>
- Meeplam, P 2017, 'Challenges in internet fraud prosecution and investigation in Thailand: The perspective of Thai Police officers', MSc thesis, Durham University, Durham.
- Meesters, ME & Behagel, JH 2017, 'The social license to operate: Ambiguities and the neutralization of harm in Mongolia', *Resources Policy*, vol. 53, pp. 274-282. <https://doi.org/10.1016/j.resourpol.2017.07.006>
- Mehta, A & Bhavani, G 2017, 'Application of forensic tools to detect fraud: The case of Toshiba', *Journal of Forensic and Investigative Accounting*, vol. 9, no. 1, pp. 692-710.
- Mekonnen, S, Padayachee, K & Meshesha, M 2015, 'A privacy-preserving context-aware insider threat prediction and prevention model predicated on the components of the fraud diamond', in *Proceedings of the 2015 Annual Global Online Conference on Information and Computer Technology (GOCICT)*, Louisville, Kentucky, United States of America, 04-06 November, pp. 60-65.
- Messina, G 2019, *What is memory forensics?*, viewed 03 March 2023, <<https://resources.infosecstitute.com/topic/computer-forensics-memory-forensics/#:-:text=Memory%20forensics%20is%20a%20vital,known%20as%20a%20memory%20dump>>
- Miller, FR & Martson, DL 2011, 'Building a case: Gathering and documenting evidence', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., John Wiley & Sons, Hoboken, pp. 175-189.
- Mitchell, T 1997, *Machine learning*, McGraw Hill, New York.
- Mittal, P, Kaur, A & Gupta, PK 2021, 'The mediating role of big data to influence practitioners to use forensic accounting for fraud detection', *European Journal of Business Science and Technology*, vol. 7, no. 1, pp. 47-58. <https://doi.org/10.11118/ejobsat.2021.009>
- Modugu, KP & Anyaduba, JO 2013, 'Forensic accounting and financial fraud in Nigeria: An empirical approach', *International Journal of Business and Social Science*, vol. 4, no. 7, pp. 281-289.
- Moffitt, KC & Vasarhelyi, MA 2013, 'AIS in an age of big data', *Journal of Information Systems*, vol. 27, no. 2, pp. 1-19. <https://doi.org/10.2308/isys-10372>
- Mohammed, HK & Knapkova, A 2016, 'The impact of total risk management on company's performance', *Procedia-Social and Behavioral Sciences*, vol. 220, pp. 271-277. <https://doi.org/10.1016/j.sbspro.2016.05.499>
- Mohd, KAA, Rayvieana, VR, Leau, YB & Tan, SF 2010, 'Security issues on banking systems', *International Journal of Computer Science and Information Technologies*, vol. 1, no. 4, pp. 268-272.

- Mohd-Sanusi, Z, Mohamed, N, Omar, N & Mohd-Nassir, MD 2015, 'Effects of internal controls, fraud motives and experience in assessing the likelihood of fraud risk', *Journal of Economics, Business and Management*, vol. 3, no. 2, pp. 194–200. <https://doi.org/10.7763/JOEBM.2015.V3.179>
- Mohtasebi, S & Dehghantanha, A 2013, 'Towards a unified forensic investigation framework of smartphones', *International Journal of Computer Theory and Engineering*, vol. 5, no. 2, pp. 351–355. <https://doi.org/10.7763/IJCTE.2013.V5.708>
- Monks, RAG & Minow, W 2011, *Corporate governance*, 5th edn., John Wiley & Sons, Hoboken.
- Monni, SS & Sultana, A 2016, 'Investigating cyber bullying: Pervasiveness, causes and sociopsychological impact on adolescent girls', *Journal of Public Administration and Governance*, vol. 6, no. 4, pp. 1–26. <https://doi.org/10.5296/jpag.v6i4.10132>
- Moon, B & Hays, K 2009, 'General strain theory, key strains and deviance', *Journal of Criminal Justice*, vol. 40, pp. 117–127.
- Moon, B & Morash, M 2017, 'Gender and general strain theory: A comparison of strains, mediating, and moderating effects explaining three types of delinquency', *Youth & Society*, vol. 49, no. 4, pp. 1–10. <https://doi.org/10.1177/0044118X14541877>
- Mugari, I, Gona, S, Maunga, M & Chiyambiro, R 2016, 'Cybercrime: The emerging threat to the financial services sector in Zimbabwe', *Mediterranean Journal of Social Sciences*, vol. 7, no. 3, pp. 135–143. <https://doi.org/10.5901/mjss.2016.v7n3s1p135>
- Murphy, PR & Free, C 2016, 'Broadening the fraud triangle: Instrumental climate and fraud', *Behavioural Research in Accounting*, vol. 28, no. 1, pp. 41–56. <https://doi.org/10.2308/bria-51083>
- Musal, RM 2010, 'Two models to investigate Medicare fraud within unsupervised databases', *Expert Systems with Applications*, vol. 37, no. 12, pp. 8628–8633. <https://doi.org/10.1016/j.eswa.2010.06.095>
- Mushtaque, K, Ahsan, K & Umer, A 2015, 'Digital forensic investigation models: An evolution study', *Journal of Information Systems and Technology Management*, vol. 12, no. 2, pp. 233–244. <https://doi.org/10.4301/S1807-17752015000200003>
- Nasser, K & AlDosari, KA 2020, 'Cybercrime: Theoretical determinants, criminal policies, prevention & control mechanisms', *International Journal of Technology and Systems*, vol. 5, no. 3, pp. 34–63. <https://doi.org/10.47604/ijts.1133>
- Natalie, B n.d., *Sociological and psychological theories of crime: Overview and features*, viewed 24 November 2021, <<http://study.com/academy/lesson>>
- National Cyber Security Authority 2022, *About NSCA*, viewed 28 February 2023, <<https://cyber.gov.rw/about/>>
- National Fraud Authority 2012, *Annual fraud indicator*, viewed 02 February 2022, <www.homeoffice.gov.uk>
- Nedbank Group Ltd 2015, *Integrated Annual Report*, viewed 16 November 2020, <[https://www.nedbank.co.za/content/dam/nedbank/site-assets/AboutUs/Information%20Hub/Integrated%20Report/2015/2015\(A\)_Nedbank_Group_Integrated_Report.pdf](https://www.nedbank.co.za/content/dam/nedbank/site-assets/AboutUs/Information%20Hub/Integrated%20Report/2015/2015(A)_Nedbank_Group_Integrated_Report.pdf)>
- Nedbank Group Ltd 2017, *Integrated annual report*, viewed 16 November 2020, <<https://www.nedbank.co.za/content/dam/nedbank/siteassets/AboutUs/Information%20Hub/Integrated%20Report/2017/2017%20Nedbank%20Group%20Integrated%20Report.pdf>>
- Nedbank Group Ltd 2021, *Integrated annual report*, viewed 26 December 2022, <[https://www.nedbank.co.za/content/dam/nedbank/siteassets/AboutUs/Information%20Hub/Integrated%20Report/2022/2021%20Nedbank%20Group%20Integrated%20Report%20\(1A\).pdf](https://www.nedbank.co.za/content/dam/nedbank/siteassets/AboutUs/Information%20Hub/Integrated%20Report/2022/2021%20Nedbank%20Group%20Integrated%20Report%20(1A).pdf)>
- Ngai, EWT, Hu, Y, Wong, YH, Chen, Y & Sun, X 2011, 'The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature', *Decision Support Systems*, vol. 50, no. 3, pp. 559–569. <https://doi.org/10.1016/j.dss.2010.08.006>

References

- Ngufor, C & Wojtusiak, J 2013, 'Unsupervised labeling of data for supervised learning and its application to medical claims prediction', *Computer Science*, vol. 14, no. 2, p. 191. <https://doi.org/10.7494/csci.2012.14.2.191>
- Nigrini, M 2011, *Forensic analytics: Methods and techniques for forensic accounting investigations*, John Wiley & Sons, Hoboken.
- Nissan, E 2012, 'The forensic disciplines: Some areas of actual or potential application', in *Computer applications for handling legal evidence, police investigation and case argumentation*, vol. 5, Law, Governance and Technology Series, Springer, Dordrecht, pp. 841-989.
- National Institute of Standards and Technology (NIST) 2013, *Test results for mobile device acquisition tool: Device seizure v5.0 build 4582.15907*, viewed 09 September 2016, <<https://www.ncjrs.gov/pdffiles1/nij/241153.pdf>>
- Njanike, K, Dube, T & Mashayanye, E 2009, 'The effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds', *Journal of Sustainable Development in Africa*, vol. 10, no. 4, pp. 405-425.
- Njenga, NM & Osiemo, O 2013, 'Effect of fraud risk management on organisation performance: A case of deposit-taking microfinance institutions in Kenya', *International Journal of Social Sciences and Entrepreneurship*, vol. 1, no. 7, pp. 1-17.
- Njeru, PW & Gaitho, V 2019, 'Investigating the extent to which cybercrime influences the performance of commercial banks in Kenya', *International Journal of Economics, Commerce and Management*, vol. VII, no. 8, pp. 489-514.
- Nonye, A & Okoli, BE 2015, 'Forensic accounting veritable tool for efficient management of state-owned public sectors in Ebonyi State: The accounting perspective', *British Journal of Education*, vol. 3, no. 8, pp. 55-62.
- Noorein, SI 2012, 'Alignment of strategy with structure using management control systems', *Strategic Management Review*, vol. 6, no. 1, pp. 1-26.
- National Television System Committee (NTSC) 2020, *Cyber security report 2020*, viewed 15 November 2022, <<https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf>>
- Nunn, L, McGuire, BL, Whitcomb, C & Jost, E 2006, 'Forensic accountants: Financial investigations', *Journal of Business & Economic Research*, vol. 4, no. 2, pp. 1-6. <https://doi.org/10.19030/jber.v4i2.2631>
- Nwankwo, O 2013, 'Implications of fraud on commercial banks' performance in Nigeria', *International Journal of Business and Management*, vol. 8, no. 15, pp. 144-150. <https://doi.org/10.5539/ijbm.v8n15p144>
- Obalola, M, Omoteso, K & Adelopo, I 2009, *Corporate governance and corporate social responsibility practices in Africa*, 1st edn., Routledge, Oxford.
- Obeng-Adjei, A 2017, 'Analysis of cybercrime activity: Perceptions from a South African financial bank - a research report', MSc thesis, University of Witwatersrand, pp. 1-87.
- Ocansey, EOND 2017, 'Forensic accounting and the combating of economic and financial crimes in Ghana', *European Scientific Journal*, vol. 13, no. 31, pp. 379-393. <https://doi.org/10.19044/esj.2017.v13n31p379>
- Odelabu, AT 2014, 'Effect of forensic accounting on the financial performance of commercial banks in Nigeria', *Research Journal of Finance and Accounting*, vol. 5, no. 8, pp. 103-109.
- Offei, M, Andoh-Baidoo, FK & Asamoah, D 2021, 'How do individuals justify and rationalize their criminal behaviours in online romance fraud?', *Information System Frontiers*, vol. 24, pp. 475-491.
- Offei, M, Kofi Andoh-Baidoo, F, Ayaburi, E & Asamoah, D 2019, 'Understanding internet fraud: Denial of risk theory perspective', in *International Working Conference on Transfer and Diffusion of IT (TDIT)*, Accra, Ghana, June, pp. 415-424.
- Ogbi, FE 2013, 'Corruption in the matrix of development in Nigeria', *European Scientific Journal*, vol. 9, no. 7, pp. 78-87.

- Oguda, NJ, Odhiambo, A & Byaruhanga, J 2015, 'Effect of internal control on fraud detection and prevention in district treasuries of Kakamega County', *International Journal of Business and Management Invention*, vol. 4, no. 1, pp. 47-57.
- Ogunleye, GA 2010, *Perspectives on the Nigerian Financial Safety-Net Nigeria Deposit Insurance Corporation*, Abuja, viewed 20 February 2022, <<https://ndic.gov.ng/wpcontent/uploads/2015/01/PerspectivesOntheNigerianFinancialSafetyNetNDIC2.pdf>>
- Okeshola, FB & Adeta, AK 2013, 'The nature of causes and consequences of Cyber Crime in tertiary institutions in Zaria Kaduna State, Nigeria', *American International Journal of Contemporary Research*, vol. 3, no. 9, pp. 98-114.
- Okoye, E & Alamobi, N 2009, 'The role of forensic accounting in fraud investigation and litigation support', *The Nigerian Academic Forum*, vol. 17, pp. 39-44.
- Okoye, EI & Akenbor, CO 2009, 'Forensic accounting in developing economies: Problems and prospects', *The University Advanced Research Journal*, vol. 1, pp. 1-13.
- Okoye, EI & Gbegi, DO 2013, 'Forensic accounting: A tool for fraud detection and prevention in the public sector (A study of selected ministries in Kogi State)', *International Journal of Academic Research in Business and Social Sciences*, vol. 3, no. 3, pp. 1-19.
- Okunbor, JA & Obaretin, O 2010, 'Effectiveness of the application of forensic accounting services in Nigerian organisations', *AAU Journal of Management Science*, vol. 1, no. 1, pp. 171-184.
- Okutan, A & Çebi, Y 2019, 'A framework for cyber crime investigation', *Procedia Computer Science*, vol. 158, pp. 287-294.
- Okwoli, AA 2004, 'Towards probity, accountability and transparency in revenue generation in the Nigerian public sector', *Nigerian Journal of Accounting Research*, vol. 1, no. 1, pp. 1-9.
- Olaoye, CO & Olanipekun, CT 2018, 'Impact of forensic accounting and investigation on corporate governance in Ekiti State', *Journal of Accounting, Business and Finance Research*, vol. 4, no. 1, pp. 28-36. <https://doi.org/10.20448/2002.41.28.36>
- Olukowade, E & Balogun, E 2015, 'Relevance of forensic accounting in the detection and prevention of fraud in Nigeria', *International Journal of Accounting Research*, vol. 2, no. 7, pp. 67-77. <https://doi.org/10.12816/0017351>
- Oluwadare, DA 1993, 'Precipitating factors in fraud and criminal motivation', *A paper presented at the Effective Bank Inspection Course organised by the Financial Institutions Training Centre*, Yaba, Lagos.
- Oluwatoyin, EA, Mashigo, P & Zerihun, MF 2023. 'The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry', *Cogent Business & Management*, vol. 10, p. 1. <https://doi.org/10.1080/23311975.2022.2163560>
- Omar, N, Johari, ZA & Hasnan, S 2015, 'Corporate culture and the occurrence of financial statement fraud: A review of literature', *Procedia Economics and Finance*, vol. 31, pp. 367-372. [https://doi.org/10.1016/S2212-5671\(15\)01211-3](https://doi.org/10.1016/S2212-5671(15)01211-3)
- Omar, NB, Mohamed, N & Jomitin, B 2013, 'The relevance of forensic accounting in the public sector (A study of selected government agencies in Klang Valley)', in *Proceedings of the 5 International Conference on Financial Criminology (ICFC), Malaysia*, pp. 225-232.
- Omodunbi, BA, Odiase, PO, Olaniyan, OM & Esan, AO 2016, 'Cybercrimes in Nigeria: Analysis, detection and prevention', *FUOYE Journal of Engineering and Technology*, vol. 1, no. 1, pp. 37-42. <https://doi.org/10.46792/fuoyejet.v1i1.16>
- Onodi, BE, Okoye, EI & Egbunike, PA 2017, 'Application of fraud box-key model in the determination of fraud risk factors: Evidence from banks in Nigeria', *Journal of Global Accounting*, vol. 5, no. 1, pp. 99-112.
- Onuorah, A & Appah, E 2012, 'Fraudulent activities and forensic accounting services of banks in Port Harcourt, Nigeria', *Asian Journal of Business Management*, vol. 4, no. 2, pp. 124-129.

References

- Onyekwelu, UL, Ugwu, KO & Nnamani, JN 2016, 'Does forensic accounting enhance the quality of financial reporting in Nigeria? An empirical investigation', *European Journal of Accounting, Auditing and Finance Research*, vol. 4, no. 8, pp. 62-84.
- Organization for Economic Co-operation and Development (OECD) 2007, *Malicious software malware: A security threat to the internet economy*, viewed 15 May 2019, <<http://www.oecd.org/sti/40724457.pdf>>
- Oseni, AI 2017, 'Forensic accounting and financial fraud in Nigeria: Problems and prospect', *Journal of Accounting and Financial Management*, vol. 3, no. 1, pp. 23-33.
- Osioma, B 2012, 'Fraud prevention in Nigeria: Applying the forensic accounting tool', in *2nd Annual Fraud & Corruption Africa Summit, Held at Zanzibar Beach Resort, Zanzibar Republic of Tanzania*, s.l., 13-15 July.
- Otley, DT 2016, 'The contingency theory of management accounting and control: 1980-2014', *Management Accounting Research*, vol. 31, pp. 45-62. <https://doi.org/10.1016/j.mar.2016.02.001>
- Özcan, OUA 2019, 'Analyzing the impact of forensic accounting on the detection of financial information manipulation', *Manas Journal of Social Studies*, vol. 8, no. 2, pp. 1744-1758. <https://doi.org/10.33206/mjss.486662>
- Ozili, P 2015, 'Forensic accounting and fraud: A review of literature and policy implications', *International Journal of Accounting and Economics Studies*, vol. 3, no. 1, pp. 63-68. <https://doi.org/10.14419/ijaes.v3i1.4541>
- Ozili, PK 2020, 'Forensic accounting theory', in E Özen & S Grima (ed.), *Uncertainty and challenges in contemporary economic behavior (Emerald Studies in Finance, Insurance, and Risk Management)*, Emerald, Bingley, pp. 49-60.
- Özkul, FU & Pamukcu, A 2012, 'Fraud detection and forensic accounting', in K Caliyurt & SO Idowu (eds.), *Emerging fraud: Fraud cases from emerging economies*, Springer-Verlag, Berlin, pp. 19-41.
- Pandya, P 2013, 'The enemy (The intruder's genesis)', in JR Vacca (ed.), *Computer and information security handbook*, Morgan Kaufmann Publishers, Burlington, pp. e35-e44.
- Pandya, P & Frazin, Z 2004, 'Information security management: A research project', in *Issues in informing science and information technology*, vol. 1, pp. 1065-1072.
- Panhalkar, T 2023, *What is email forensic investigation?*, viewed 03 March 2023, <<https://infosavvy.com/whatisemailforensicinvestigation/>>
- Patchin, JW & Hinduja, S 2011, 'Traditional and nontraditional bullying among youth: A test of general strain theory', *Youth & Society*, vol. 43, no. 2, pp. 727-751. <https://doi.org/10.1177/0044118X10366951>
- Paternoster, R & Mazerolle, P 1994, 'General strain theory and delinquency: A replication and extension', *Journal of Research in Crime and Delinquency*, vol. 31, no. 3, pp. 235-263. <https://doi.org/10.1177/0022427894031003001>
- Pathak, J, Vidyarthi, N & Summers, SL 2005, 'A fuzzy-based algorithm for auditors to detect elements of fraud in settled insurance claims', *Managerial Auditing Journal*, vol. 20, no. 6, 632-644. <https://doi.org/10.1108/02686900510606119>
- Paura, L & Arhipova, I 2012, 'Advantages and disadvantages of professional and free software for teaching statistics', *Information Technology and Management Science*, vol. 15, pp. 1-14. <https://doi.org/10.2478/v10313-012-0001-z>
- Pearson, TA & Singleton, TW 2008, 'Fraud and forensic accounting in the digital environment', *Issues in accounting education*, vol. 23, no. 4, pp. 545-559. <https://doi.org/10.2308/iace.2008.23.4.545>
- Pedneault, S, Rudewicz, F, Silverstone, H & Sheetz, M 2012, *Forensic accounting and fraud investigation for non-experts*, 3rd edn., John Wiley & Sons, Hoboken, pp. 1-336.
- Peretti-Watel, P 2003, 'Neutralization theory and the denial of risk: Some evidence from cannabis use among French adolescents', *The British Journal of Sociology*, vol. 54, pp. 21-42. <https://doi.org/10.1080/0007131032000045888>

- Pfister, J 2014, 'Controlling creativity and innovation: Paradox or necessity?', in D Otley & K Soim (eds.), *Management control and uncertainty*, Palgrave Macmillan, London, pp. 134-148.
- Pilli, E, Joshi, R & Niyogi, R 2010, 'A generic framework for network forensics', *International Journal of Computers and Applications*, vol. 1, no. 11, pp. 1-6. <https://doi.org/10.5120/251-408>
- Plier, K 2020, *Effective communication mitigates risk in a cybersecurity world*, viewed 27 May 2021, <<https://www.forbes.com/sites/forbesagencycouncil/2020/01/21/effectivecommunicationmitigatesriskinacybersecurityworld/?sh=24e9a2483afb>>
- Pooley, J 2013, *Computer and information security handbook*, 3rd edn., Morgan Kaufmann Publishers, Burlington.
- Popoola, OMJ, Ahmad, AC & Samsudin, RS 2015a, 'Task performance fraud risk assessment on forensic accountant and auditor knowledge and mindset in Nigerian public sector', *Risk Governance & Control: Financial Markets & Institutions*, vol. 4, no. 3, pp. 84-90. <https://doi.org/10.22495/rgcv4i3c1art2>
- Popoola, OMJ, Ahmad, AC & Samsudin, RS 2015b, 'An empirical investigation of fraud risk assessment and knowledge requirement on fraud-related problem representation in Nigeria', *Accounting Research Journal*, vol. 28, no. 1, pp. 78-97. <https://doi.org/10.1108/ARJ-08-2014-0067>
- Porter, ME & Heppelmann, JE 2015, 'How smart, connected products are transforming companies', *Harvard Business Review*, vol. October 2015, pp. 97-114.
- Prabowo, HY 2011, 'Building our defence against credit card fraud: A strategic view', *Journal of Money Laundering Control*, vol. 14, no. 4, pp. 371-386. <https://doi.org/10.1108/13685201111173848>
- Prayudi, Y, Ashari, A & Priyambodo, T 2015, 'A proposed digital forensic business model to support cybercrime investigation in Indonesia', *International Journal of Computer Network and Information Security*, vol. 7, no. 11, pp. 1-8. <https://doi.org/10.5815/ijcnis.2015.11.01>
- Primer, A 2016, 'Cybersecurity plans and strategies, establishing priorities, organizing roles and responsibilities', in *Protection of transportation infrastructure from cyber attacks*, The National Academies Press, Washington DC, pp. 1-170.
- Punitha, A, Umasri, V, Nizamuddin, SM, Shanmugam, K & Radjamanogary, R n.d., *Management control systems*, Pondicherry University, Directorate of Distance Education, Kalapet.
- PricewaterhouseCoopers (PwC) 2007, *The 4th Biennial Global Economic Crime Survey: India*, viewed 02 February 2020, <<https://www.pwc.in/assets/pdfs/global-economic-crime-survey.pdf>>
- PricewaterhouseCoopers (PwC) 2011, *Fraud: A guide to its prevention, detection and investigation*, pp. 1-46, viewed 15 August 2019, <<https://www.pwc.com.au/consulting/assets/riskcontrols/fraudcontroljul08.pdf>>
- PricewaterhouseCoopers (PwC) 2014, *Confronting the changing Face of economic crime*, pp. 1-60, viewed 17 July 2022, <www.pwc.org>
- PricewaterhouseCoopers (PwC) 2016, *Banking in Africa matters - African banking survey*, Global Fintech Report, pp. 1-100, viewed 16 October 2021, <www.pwc.org>
- PricewaterhouseCoopers (PwC) 2018, *Global economic crime survey: Pulling fraud out of the shadows*, pp. 1-30, viewed 05 January 2019, <www.pwc.org>
- PricewaterhouseCoopers (PwC) 2020, *Global economic crime and fraud survey*, 7th edn., viewed 17 January 2021, <<https://www.corruptionwatch.org.za/wpcontent/uploads/2020/06/globaleconomiccrimesurvey20201.pdf>>
- PricewaterhouseCoopers (PwC) 2022a, *Protecting the perimeter: The rise of external fraud*, viewed 15 November 2022, <<https://www.pwc.com/gx/en/forensics/gecsm2022/pdf/PwC%E2%80%99sGlobalEconomicCrimeandFraudSurvey2022.pdf>>
- PricewaterhouseCoopers (PwC) 2022b, *US highlights*, viewed 15 November 2022, <<https://www.pwc.com/us/en/services/consulting/cybersecurityriskregulatory/library/globaleconomicfraudsurvey.html>>

References

- Quah, JTS & Sriganesh, M 2008, 'Realtime credit card fraud detection using computational intelligence', *Expert Systems with Applications*, vol. 35, no. 4, pp. 1721-1732. <https://doi.org/10.1016/j.eswa.2007.08.093>
- Rae, K & Subramaniam, N 2008, 'Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud', *Managerial Auditing Journal*, vol. 23, no. 2, pp. 104-124. <https://doi.org/10.1108/O2686900810839820>
- Raghavan, AR & Parthiban, L 2014, 'The effect of cybercrime on a bank's finances', *International Journal of Current Research & Academic Review*, vol. 2, no. 2, pp. 173-178.
- Rahmawati, D, Yaqin, MA & Sarno, R 2016, 'Fraud detection on event logs of goods and services procurement business process using heuristics miner algorithm', in *Proceedings of 2016 International Conference on Information & Communication Technology and Systems*, Surabaya, Indonesia, October 12, pp. 249-254.
- Ramamoorti, S, Morrison, D & Koletar, JW 2014, 'Bringing Freud to fraud', *Journal of Forensic & Investigative Accounting*, vol. 6, no. 1, pp. 47-81.
- Ramaswamy, V 2005, 'Corporate governance and the forensic accountant', *CPA Journal*, vol. 75, no. 3, pp. 68-70.
- Ramy, F, Evan, S & Daniel, H 2017, *The hidden cost of reputation risk: An approach to quantifying reputation risk losses*, viewed 21 September 2022, <www.oliverwyman.com>
- Rana, R & Singhal, R 2015, 'Chi-square test and its application in hypothesis testing', *Journal of the Practice of Cardiovascular Sciences*, vol. 1, no. 1, pp. 68-71. <https://doi.org/10.4103/2395-5414.157577>
- Rao, HS 2019, 'Cyber crime in the banking sector', *International Journal of Research*, vol. 7, no. 1, pp. 148-161. <https://doi.org/10.29121/granthaalayah.v7.i1.2019.1043>
- Rasha, K & Andrew, H 2012, 'The new fraud triangle', *Journal of Emerging Trends in Economics and Management Sciences*, vol. 3, no. 3, pp. 87-94.
- Rashid, YF 2013, *Cyber-criminals stole \$500 million in Internet crime in 2012*, viewed n.d., <<https://www.pcmag.com/nws/cyber-criminals-stole-500-million-in-internet-crime-in-2012>>
- Ravi, S 2012, 'Study of latest emerging trend and its challenges to society', *International Journal of Scientific and Engineering Research*, vol. 3, no. 6, pp. 1-4.
- Redy, A 2018, *NoSQL databases and big data*, viewed 17 December 2022, <<https://medium.com/@arunbollam/nosqldatabasesandbigdata57562e93f302>>
- Reddy, ML & Bhargavi, V 2018, 'Cyber security attacks in banking sector: Emerging security challenges and threats', *American International Journal of Research in Humanities, Arts and Social Sciences*, vol. 21, no. 1, pp. 65-71.
- Reith, M, Carr, C & Gunsch, G 2002, 'An examination of digital forensic models', *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 42-53.
- Reyns, BW 2013, 'Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses', *Journal of Research in Crime and Delinquency*, vol. 50, no. 2, pp. 216-238. <https://doi.org/10.1177/0022427811425539>
- Rezaee, Z 2005, 'Causes, consequences, and deterrence of financial statement fraud', *Critical Perspectives on Accounting*, vol. 16, no. 3, pp. 277-298. [https://doi.org/10.1016/S1045-2354\(03\)00072-8](https://doi.org/10.1016/S1045-2354(03)00072-8)
- Rezaee, Z, Lo, D, Ha, M & Suen, A 2016, 'Forensic accounting education and practice: Insights from China', *Journal of Forensic & Investigative Accounting*, vol. 8, no. 1, pp. 106-119.
- Rezk, A, Barakat, S & Saleh, H 2017, 'The impact of cyber crime on e-commerce', *International Journal of Intelligent Computing and Information Sciences*, vol. 17, no. 3, pp. 85-96.
- Riahi-Belkaoui, AR & Picur, R 2000, 'Understanding fraud in accounting environment', *Managerial Finance*, vol. 26, no. 1, pp. 33-41. <https://doi.org/10.1108/O3074350010766972>
- Rice, KJ & Csmith, WR 2002, 'Socioecological models of automotive theft: Integrating routine activity and social disorganization approaches', *Journal of Research in Crime and Delinquency*, vol. 39, no. 3, pp. 304-336. <https://doi.org/10.1177/002242780203900303>

- Richards, DA, Melancon, BC & Ratley, JD 2019, *Managing the business risk of fraud: A practical guide*, The Institute of Internal Auditors, The American Institute of Certified Public Accountants Association of Certified Fraud Examiners, Austin.
- Roberts, PW & Dowling, GR 2002, 'Corporate reputation and sustained superior financial performance', *Strategic Management Journal*, vol. 23, pp. 1077-1093.
- Rodgers, W, Söderbom, A & Guiral, A 2014, 'Corporate social responsibility enhanced control systems reducing the likelihood of fraud', *Journal of Business Ethics*, vol. 131, pp. 871-882. <https://doi.org/10.1007/s10551-014-2152-5>
- Rogers, K, Goldman, J, Mislán, R, Wedge, T & Debrota, S 2006, 'Computer forensic field triage process model', *Journal of Digital Forensics Security and Law*, vol. 1, no. 2, pp. 19-38. <https://doi.org/10.15394/jdfsl.2006.1004>
- Rowlingson, R 2004, 'A ten-step process for forensic readiness', *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1-28.
- Saaty, TL 1980, *The analytic hierarchy process: Planning, priority setting, resource allocation*, McGraw Hill, New York.
- Saaty, TL 2008, 'Decision making with the analytic hierarchy process', *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83-98.
- Saini, H, Rao, YS & Panda, TC 2012, 'Cybercrimes and their impacts: A review', *International Journal of Engineering Research and Applications*, vol. 2, no. 2, pp. 202-209.
- Santos Filho, CR, Carlos, FA & Costa, FM 2017, 'Relevant skills for criminal accounting expertise: The perception of federal police experts and delegates', *Journal of Education and Research in Accounting*, vol. 11, no. 1, pp. 69-88. <https://doi.org/10.17524/repec.v11i1.1446>
- Sanusi, MZ, Mohamed, N, Omar, N & Mohd-Nassir, MD 2015, 'Effects of internal controls, fraud motives and experience in assessing the likelihood of fraud risk', *Journal of Economics, Business and Management*, vol. 3, no. 2, pp. 194-200. <https://doi.org/10.7763/JOEBM.2015.V3.179>
- Schuchter, A & Levi, M 2013, 'The fraud triangle revisited', *Security Journal*, vol. 29, no. 2, pp. 107-121. <https://doi.org/10.1057/sj.2013.1>
- Security and Forensic Studies in Nigeria 2010, *Institute for Security and Forensic Studies Report*, viewed 20 November 2022, <<https://www.sfsnigeria.com.ng/>>
- Security and Forensic Studies in Nigeria 2018, *Security and forensic (sic) studies Nigeria*, viewed 26 February 2022, <<https://www.sfsnigeria.com.ng/>>
- Security Scorecard 2022, What is mobile forensics? Definition, processes and examples, viewed 02 February 2023, <<https://securityscorecard.com/blog/whatismobileforensicsarealexamplefromthesecurityscorecardforensicslab/#:-:text=Mobile%20forensics%20is%20e%20process,smartphones%2C%20androids%2C%20and%20tablets>>
- Seda, MA, Bonita, PK & Larry, CD 2019, 'An examination of computer forensics and related certifications in the accounting curriculum', *Journal of Digital Forensics, Security and Law*, vol. 14, no. 1, pp. 1-24, Article 4. <https://doi.org/10.15394/jdfsl.2019.1578>
- Sedgwick, P 2014, 'Spearman's rank correlation coefficient', *British Medical Journal*, vol. 349, pp. 1-3. <https://doi.org/10.1136/bmj.g7528>
- Selamat, SR, Yusof, R & Sahib, S 2008, 'Mapping process of digital forensic investigation framework', *International Journal of Computer Science Network Security*, vol. 8, no. 10, pp. 163-169.
- Serhii, K, Vadym, P, Oleg, K, Oleksandr, M & Strilets, O 2019, 'Forensic economic examination as a means of investigation and counteraction of economic crimes in East Europe (example of Ukraine)', *Journal of Legal, Ethical and Regulatory Issues*, vol. 22, no. 3, pp. 1-8.
- Serianu 2016, *Africa cyber security report*, viewed 18 November 2022, <<https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>>
- Serianu 2021, *Africa cyber security report*, viewed July 2022, <<https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf>>
- Shahabuddin, AM, Alam, A & Azad, MM 2011, 'Internal controls in management information system', *International Journal of Computer Information Systems*, vol. 2, no. 6, pp. 58-78.

References

- Shaheen, I, Pranathi, Sultana, A & Noor, A 2014, 'Forensic accounting and fraud examination in India', *International Journal of Innovative Research and Development*, vol. 3, no. 12, pp. 171-177.
- Shim, DC & Eom, TH 2008, 'eGovernment and anticorruption: Empirical analysis of international data', *International Journal of Public Administration*, vol. 31, no. 3, pp. 298-316. <https://doi.org/10.1080/01900690701590553>
- Shimoli, D 2015, 'Forensic accounting: Signaling practicing accountants to improve skillset and forming regulatory body for forensic accountants in India', *Global Journal for Research Analysis*, vol. 4, no. 5, pp. 63-66.
- Shin, H, Park, H, Lee, J & Jhee, WC 2012, 'A scoring model to detect abusive billing patterns in health insurance claims', *Expert Systems with Applications*, vol. 39, no. 8, pp. 7441-7450. <https://doi.org/10.1016/j.eswa.2012.01.105>
- Shurafa, R & Mohamed, RB 2016, 'Management control system, organisational learning, and firm's performance: An empirical study from developing economy', *International Journal of Advanced and Applied Sciences*, vol. 3, no. 10, pp. 79-88. <https://doi.org/10.21833/ijaas.2016.10.013>
- Sidharta, E & Fitriyah, F 2015, 'Forensic accounting and fraud prevention Indonesia public sector', *International Journal of Business and Management Studies*, vol. 4, no. 1, pp. 123-131.
- Sigala, M 2017, 'How "bad" are you? Justification and normalization of online deviant customer behavior', in R Schegg & B Stangl (eds.), *Information and Communication Technologies in Tourism 2017*, Springer, Cham, pp. 607-622.
- Singleton, TW & Singleton, AJ 2006, *Fraud auditing and forensic accounting*, 3rd edn., John Wiley & Sons, Hoboken.
- Singleton, TW & Singleton, AJ 2010, *Fraud auditing and forensic accounting*, vol. 11, 4th edn., John Wiley & Sons, Hoboken.
- Skalak, SL, Alas, MA & Sellito, G 2011, *Fraud: An introduction. In a guide to forensic accounting investigation*, TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), John Wiley & Sons, Hoboken, pp. 1-23.
- Slavoljub, S, Srdjan, S & Predrag, V 2015, 'Management control in modern organisations faculty of business economics and entrepreneurship', *International Review*, vol. 3, no. 4, pp. 39-49. <https://doi.org/10.5937/intrev1504039S>
- Smith, GS 2005, 'Computer forensics: Helping to achieve the auditor's fraud mission', *Journal of Forensic Accounting, Auditing, Fraud & Taxation*, vol. 4, no. 1, pp. 119-134.
- Smith, GS & Crumbley, DL 2009, 'Defining a forensic audit', *Journal of Digital Forensics, Security and Law*, vol. 4, no. 1, pp. 61-80. <https://doi.org/10.15394/jdfsl.2009.1054>
- Smith, M, Sagafi-Nejad, T & Wang, K 2008, 'Going international: Accounting and auditing standards', *Internal Auditing*, vol. 23, no. 4, pp. 3-12.
- Sonepat, R & Sonepat, S 2014, 'Analysis on credit card fraud detection methods', *International Journal of Computer Trends and Technology*, vol. 8, no. 1, p. 45. <https://doi.org/10.14445/22312803/IJCTT-V8P109>
- South African Banking Risk Information Centre (SABRIC), 2018, *Digital banking crime statistics*, viewed 05 June 2020, <<https://www.sabric.co.za/mediaandnews/pressreleases/digitalbankingcrimestatistics/>>
- South African Banking Risk Information Centre (SABRIC) 2020, *Annual crime statistics 2020*, viewed 20 June 2022, <<https://www.sabric.co.za/media/20oouwbg/sabricannualcrimestats2020.pdf>>
- South African Banking Risk Information Centre (SABRIC) 2021, *Annual crime statistics 2021*, viewed 15 November 2022, <https://www.sabric.co.za/media/5dlnhnyj/sabriccrimestats2021_fa.pdf>
- Srivastava, A, Kundu, A, Sural, S & Majumdar, AK 2008, 'Credit card fraud detection using hidden Markov model', *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37-48. <https://doi.org/10.1109/TDSC.2007.70228>

- Stanbury, J & Paley-Menzies, C 2010, 'Forensic Futurama: Why forensic', in *Accounting is evolving*, viewed 05 June 2020, <<http://www.aicpa.org/Publications/Newsletters/AICPACPAInsider/2010/jun28/Pages/ForensicFuturamaWhyForensicAccountingIsEvolving.aspx>>
- Standard Bank Group Ltd 2016a, *Annual integrated report*, viewed 16 November 2020, <http://annualreport2016.standardbank.com/downloads/Standard_Bank_AIR_2016_Full_annual_integrated_report.pdf>
- Standard Bank Group Ltd 2016b, *Report to society*, viewed 16 November 2020, <http://sustainability.standardbank.com/pdfs/Standard_Bank_Report_to_society_2016.pdf>
- Standard Bank Group Ltd 2021, *Annual integrated report*, viewed 26 December 2022, <<https://www.standardbank.com/sbg/standardbankgroup/whats happening/financials/annualintegratedreport>>
- Statista 2022, *Average cost of a data breach worldwide as of 2022, by country or region*, viewed 30 July 2022, <<https://www.statista.com/statistics/463714/costdatabreachbycountryorregion/>>
- StatisticsSolution 2020, *Cronbach's alpha*, viewed 09 September 2020, <<https://www.statisticssolutions.com/cronbachsalph/>>
- Stein, A 2012, *Big data and analytics the analytics value chain*, viewed 17 December 2022, <<http://steinbox.com/blog/bigdataandanalyticstheanalyticsvaluechain/>>
- Stoneburner, G, Goguen, A & Feringa, A 2002, *Risk management guide for information technology systems*, National Institute of Standards and Technology Special Publication, Gaithersburg, vol. 800, no. 30, pp. 1-53. <https://doi.org/10.6028/NIST.SP.800-30>
- Sugiura, L 2018, 'Challenging the risks in online medicine purchasing: Respectable deviance', in TJ Holt & C Cross (eds.), *Respectable deviance and purchasing medicine online*, Palgrave Macmillan, Cham. pp. 101-138.
- Sule, S, Ibrahim, SS & Sani, AA 2019, 'The effect of forensic accounting investigation in detecting financial fraud: A study in Nigeria', *International Journal of Academic Research in Business and Social Sciences*, vol. 9, no. 2, pp. 545-553. <https://doi.org/10.6007/IJARBS/v9-i2/5590>
- Sutanapong, C & Louangrath, PI 2015, 'Descriptive and inferential statistics', *International Journal of Research & Methodology in Social Science*, vol. 1, no. 1, pp. 22-25.
- Sutherland, E 2017, 'Governance of cybersecurity - The case of South Africa', *The African Journal of Information and Communication*, vol. 20, pp. 83-112.
- Sutherland, EH 1940, 'White-collar criminality', *American Sociological Review*, vol. 5, no. 1, pp. 1-12. <https://doi.org/10.2307/2083937>
- Symantec Report, 2016, *Cybercrime and cyber security: Trends in Africa*, viewed 02 February 2020, <<http://www.symantec.com/>>
- Talib, A & Alomary, F 2015, 'Towards a comprehensive ontology based investigation for digital forensics cybercrime', *International Journal of Communications Antenna and Propagation*, vol. 5, no. 5, pp. 263-268. <https://doi.org/10.15866/irecap.v5i5.6112>
- Tan Harry, SK 2002, 'E-fraud; current trends and international developments', *Journal of Financial Crime*, vol. 9, no. 4, pp. 347-354. <https://doi.org/10.1108/eb026034>
- Tang, J & Karim, KE 2019, 'Financial fraud detection and big data analytics: Implications on auditors' use of fraud brainstorming session', *Managerial Auditing Journal*, vol. 34, no. 3, pp. 324-337. <https://doi.org/10.1108/MAJ-01-2018-1767>
- Tang, M, Mendis, BSU, Murray, DW, Hu, Y & Sutinen, A 2011, 'Unsupervised fraud detection in Medicare Australia', in *Proceedings of the Ninth Australasian Data Mining Conference*, Ballarat, Australia, December 01-02, pp. 103-110.
- Tapp, DJ & Henderson, WM 2011, 'When and Why to Call in Forensic Accounting Investigators', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, John Wiley & Sons, Hoboken, pp. 79-94.

References

- Tarde, G 1886, *La Criminalité Comparée*, transl. JR Baker, F Alcan, Paris.
- Tariq, M, Ahmed, A, Rafi, S & Ahmed, S 2014, 'Investigating the impact of balanced scorecard on performance of business: A study based on the banking sector of Pakistan', *IBT Journal of Business Studies*, vol. 9, no. 1, pp. 125–136. <https://doi.org/10.46745/ilma.jbs.2014.10.01.09>
- Tariq, N 2018, 'Impact of cyberattacks on financial institutions', *Journal of Internet Banking and Commerce*, vol. 23, no. 2, pp. 1–11.
- Tarr, JA, Van Akkeren, J & Buckby, S 2016, 'Forensic accounting: Professional regulation of a multidisciplinary field', *Australian Business Law Review*, vol. 44, no. 3, pp. 204–215.
- Tassev, S 2022, 'The growing costs of cybercrime – A data breach can impact a business for many years to come', 19 July, viewed 15 November 2022, <<https://www.engineeringnews.co.za/article/thegrowingcostsofcybercrimeadatabreachcanimpactabusinessformanyyears tocome20220719>>
- Tawfeeq, T, Alabdullah, Y, Mohammad, M, Alfadhli, A, Yahya, S & Rabi, AMA 2014, 'The role of forensic accounting in reducing financial corruption: A study in Iraq', *International Journal of Business Management*, vol. 9, no. 1, pp. 26–34. <https://doi.org/10.5539/ijbm.v9n1p26>
- Tekavčič, M & Peljhan, D 2003, 'Insights into managerial tools related to cost management in Slovenia companies', *Journal of Economics and Business*, vol. 21, no. 1, pp. 83–99.
- Teufel, H, Subramanian, S & Pedro, S 2011, 'Personal privacy and public disclosure', in TW Golden, SL Skalak, MM Clayton & JS Pill (eds.), *A guide to forensic accounting investigation*, 2nd edn., PricewaterhouseCoopers, New York, pp. 151–174.
- Thomas, D 2022, 'Growing cybercrime demands firm African response', *African Business*, viewed 26 October 2023, <<https://african.business/2022/08/technology-information/growing-cybercrime-demands-firm-african-response>>
- Thomas, WG, Steven, LS & Mona, MC 2006, *A guide to forensic accounting investigation*, John Wiley & Sons, Hoboken, pp. 1–565.
- Thomson, D & Jain, A 2006, 'Corporate governance failure and its impact on National Australia Bank's performance', *Journal of Business Case Studies*, vol. 2, no. 1, pp. 41–50.
- Tiwari, RK & Debnath, J 2017, 'Forensic accounting: A blend of knowledge', *Journal of Financial Regulation and Compliance*, vol. 25, no. 1, pp. 73–85. <https://doi.org/10.1108/JFRC-05-2016-0043>
- Tiwari, S, Bhalla, A & Rawat, R 2016, 'Cybercrime and security', *International of Advanced Research on Computer Science and Software Engineering*, vol. 6, no. 4, pp. 46–52.
- TransparenIT 2022, *EFCC Convictions from 2010 to 2021*, viewed 17 November 2022, <<https://transparenit.com/efccconvictionsfrom2010to2021/>>
- Turban, E, Leidner, D, Mclean, E & Wetherbe, J 2004, *Information technology for management: Transforming organizations in the digital economy*, 4th edn., John Wiley & Sons, Hoboken.
- Turbey, BE 2012, *Forensic fraud: Evaluating law enforcement and forensic science cultures in the context of examiner misconduct*, 1st edn., Academic Press, Cambridge.
- UK Finance 2018, *Staying ahead of cybercrime*, viewed 20 January 2020, <<https://www.ukfinance.org.uk/system/files/Staying-ahead-of-cyber-crime.pdf>>
- UK Finance 2020, *Overview of payment industry fraud*, viewed 05 September 2022, <www.ukfinance.org.uk>
- UK Finance 2022, *Annual fraud report: The definitive overview of payment industry fraud in 2021*, viewed 15 November 2022, <https://www.ukfinance.org.uk/system/files/202206/Annual%20Fraud%20Report%202022_FINAL_pdf>
- Uket, EE & Udoayang, JO 2012, 'The impact of internal control design on banks' ability to investigate staff fraud detection in Nigeria', *International Journal of Research in Economics & Social Sciences*, vol. 2, no. 2, pp. 32–43.
- Uma, M & Padmavathi, G 2013, 'A survey on various cyberattacks and their classification', *International Journal of Network Security*, vol. 15, no. 1, pp. 390–396.

- United Nations Office on Drug Crime 2013, *Comprehensive study on cybercrime*, viewed 15 August 2020, <https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>
- United States Department of Justice 2014, *Cyber-Investigative Issues II*, US Department of Justice, Washington DC.
- Uppal, D, Mehra, V & Verma, V 2014, 'Basic survey on malware analysis, tools and techniques', *International Journal on Computational Sciences & Applications*, vol. 4, no. 1, pp. 103-112. <https://doi.org/10.5121/ijcsa.2014.4110>
- Ur Rehman, MH, Liew, CS, Abbas, A, Jayaraman, PP, Wah, TY & Khan, SU 2016, 'Big data reduction methods: A survey', *Data Science and Engineering*, vol. 1, no. 4, pp. 265-284. <https://doi.org/10.1007/s41019-016-0022-0>
- US Department of Justice 2007, *Education and training in fraud and forensic accounting: A guide for educational institutions, stakeholder organizations, faculty, and students*, viewed 02 February 2022, <<https://www.ojp.gov/pdffiles1/nij/grants/217589.pdf>>
- US National Institute of Justice 2007, *Investigative uses of technology: Devices, tools and techniques*, viewed 26 October 2021, <<https://www.ojp.gov/pdffiles1/nij/213030.pdf>>
- Usher, A 2006, *Essential strategies for protecting against the new wave of information security threats*, Sharp Ideas LLC, viewed 19 June 2021, <<https://slideplayer.com/slide/4785106/>>
- Uvaneswaran, SM, Zemen, T & Ahmed, SD 2019, 'Corporate social responsibility (CSR) practices of business organizations in South Wollo Region - Ethiopia', *Studies and Scientific Researches. Economics Edition*, vol. 30, pp. 65-76. <https://doi.org/10.29358/sceco.v0i30.427>
- Vacca, JR 2005, *Computer forensic: Computer crime scene investigation*, Cengage Learning, Boston.
- Valjarevic, A & Venter, HS 2012, 'Harmonised digital forensic investigation process model', in *2012 Information Security for South Africa*, Johannesburg, South Africa, August 15-17, pp. 1-10.
- Van Niekerk, B 2017, 'An analysis of cyber-incidents in South Africa', *The African Journal of Information and Communication*, vol. 20, pp. 113-132.
- Van Otterlo, M & Wiering, M 2012, 'Reinforcement learning and Markov decision processes', *Adaptation, Learning, and Optimization*, vol. 12, pp. 3-42. https://doi.org/10.1007/978-3-642-27645-3_1
- Vasarhelyi, MA, Kogan, A & Tuttle, BM 2015, 'Big data in accounting: An overview', *Accounting Horizons*, vol. 29, no. 2, pp. 381-396. <https://doi.org/10.2308/acch-51071>
- Venegas, JC 2012, *Fiscal accounts*, s.n., s.l., pp. 1-86.
- VeraMunoz, SC, Hov, JL & Chow, CW 2006, 'Enhancing knowledge sharing in public accounting firms', *Accounting Horizons*, vol. 20, no. 2, pp. 133-155. <https://doi.org/10.2308/acch.2006.20.2.133>
- Verizon 2012, *Data breach investigation report 2012*, viewed 01 August 2020, <http://www.verizonenterprise.com/resources/reports/rp_databreachinvestigationsreport2012_en_xg.pdf>
- Viaene, S, Dedene, G & Derrig, RA 2004, 'A case study of applying boosting naive Bayes to claim fraud diagnosis', *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 5, pp. 612-620. <https://doi.org/10.1109/TKDE.2004.1277822>
- Viaene, S, Dedene, G & Derrig, RA 2005, 'Auto claim fraud detection using Bayesian learning neural networks', *Expert Systems with Applications*, vol. 29, no. 3, pp. 653-666. <https://doi.org/10.1016/j.eswa.2005.04.030>
- Visser, W 2012, 'The future of CSR: Towards transformative CSR, or CSR 2.0', *Kaleidoscope Futures Paper Series*, vol. 1, pp. 1-17. <https://doi.org/10.2139/ssrn.2208101>
- Volonino, L, Anzaldúa, R & Godwin, J 2006, *Computer forensics principles and practices*, 1st edn., Pearson, New York.

References

- Vona, IW 2008, *Fraud risk assessment: Building a fraud audit programme*, John Wiley & Sons, Hoboken.
- Wada, F & Odulaja, GO 2012, 'Electronic banking and cyber crime in Nigeria: A theoretical policy perspective on causation', *African Journal of Computing & ICT*, vol. 4, no. 2, pp. 69–82.
- Walden, I 2007, *Computer crimes and digital investigations*, Oxford University Press, Oxford.
- Wanemba, MA 2010, 'Strategies applied by Commercial Banks in Kenya to Combat Fraud', A Management Research Project Submitted in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Business Administration, Department of Business Administration, School of Business, University of Nairobi, Nairobi.
- Wang, CH, Gopal, RD & Zionts, S 1997, 'Use of data environment analysis in assessing information technology impact on firm performance', *Annals of Operations Research*, vol. 73, pp. 191–213. <https://doi.org/10.1023/A:1018977111455>
- Wang, J, Lee, G & Crumbley, DL 2016, 'Current availability of forensic accounting education and state of forensic accounting services in Hong Kong and Mainland China', *Journal of Forensic and Investigative Accounting*, vol. 8, no. 3, pp. 515–534.
- Wanyama, E 2013, 'The upsurge of Cyber Crime in Uganda: Where the gaps and loops lie; analysis of the need for legislative and policy framework', *Makerere Law Journal*, 2013 vol., pp. 1–26.
- Warren, JD, Jr, Moffitt, KC & Byrnes, P 2015, 'How big data will change accounting', *Accounting Horizons*, vol. 29, no. 2, pp. 397–407. <https://doi.org/10.2308/acch-51069>
- Watson, HJ 2014, 'Tutorial: Big data analytics: Concepts, technologies, and applications', *Communications of the Association for Information Systems*, vol. 34, no. 65, pp. 1247–1268. <https://doi.org/10.17705/1CAIS.03465>
- Wekesa, MM, Namusonge, GS & Makokha, EN 2016, 'Determinants of effective fraud management: A survey of domestic tier one commercial banks in Trans Nzoia County, Kenya', *International Journal of Scientific and Research Publications*, vol. 6, no. 10, pp. 375–384.
- Wells, JT 2003, 'The fraud examiners', *Journal of Accountancy*, vol. 196, no. 4, p. 76.
- Werner, M 2016, 'Process model representation layers for financial audits', in *49 Hawaii International Conference on System Sciences 2016*, Koloa, Hawaii, United States of America, January 05–08, pp. 5338–5347.
- White, DR 2004, 'A student's guide to statistics for analysis of cross tabulations', *World Cultures*, vol. 14, no. 2, pp. 179–193.
- Wilhelm, WK 2004, 'The fraud management lifecycle theory: A holistic approach to fraud management', *Journal of Economic Crime Management*, vol. 2, no. 2, pp. 1–38.
- Williams, JW 2006, 'Private legal orders: Professional markets and the commodification of financial governance', *Social and Legal Studies*, vol. 15, no. 2, pp. 209–235. <https://doi.org/10.1177/0964663906063575>
- Williams, L 2023, *What is digital forensics? History, process, types, challenges*, viewed 02 February 2023, <<https://www.guru99.com/digitalforensics.html>>
- Wilson, TP 1971, 'Critique of ordinal variables', *Social Forces*, vol. 49, pp. 432–444. <https://doi.org/10.1093/sf/49.3.432>
- Winter, BI 2004, 'Choosing the right tools for internal control reporting', *Journal of Accountancy*, 2004 vol., pp. 32–41.
- Wolfe, DT & Hermanson, DR 2004, 'The fraud diamond: Considering the four elements of fraud', *The CPA Journal*, vol. 74, no. 12, pp. 38–42.
- World Economy Forum (WEF) 2022, *Global cybersecurity outlook*, viewed 17 November 2022, <https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf>
- Wright, MF & Li, Y 2012, 'Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression', *Cyberpsychology, Behavior and Social Networking*, vol. 15, no. 9, pp. 448–454. <https://doi.org/10.1089/cyber.2012.0061>

- Wu, C, Lin, C & Tsai, P 2009, 'Financial service sector performance measurement model: AHP sensitivity analysis and balanced scorecard approach', *The Service Industries Journal*, vol. 31, no. 5, pp. 695-711. <https://doi.org/10.1080/02642060902852908>
- Yadav, S & Yadav, S 2013, 'Forensic accounting: A new dynamic approach to investigate fraud cases', *Excel International Journal of Multidisciplinary Management Studies*, vol. 3, no. 7, pp. 1-9.
- Yang, L & Wu, D 2017, 'Digital forensic analysis of cybercrime', *International Journal of Information Security and Privacy*, vol. 11, no. 2, pp. 25-37. <https://doi.org/10.4018/IJISP.2017040103>
- Yar, M 2005, 'Computer hacking: Just another case of juvenile delinquency?', *The Howard Journal of Criminal Justice*, vol. 44, no. 4, pp. 387-399. <https://doi.org/10.1111/j.1468-2311.2005.00383.x>
- Yau, FS 2000, 'Alignment of management control system to corporate competitive orientation: Some empirical evidence in Malaysia', *Pertanika Journal of Social Science and Humanities*, vol. 8, no. 2, pp. 91-102.
- Yeh, I & Lien, C 2008, 'The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients', *Expert Systems with Applications*, vol. 36, no. 2, pp. 2473-2480. <https://doi.org/10.1016/j.eswa.2007.12.020>
- Yoo, Y, Boland, RJ, Jr, Lyytinen, K & Majchrzak, A 2012, 'Organizing for innovation in the digitized world', *Organization Science*, vol. 23, no. 5, pp. 1398-1408. <https://doi.org/10.1287/orsc.1120.0771>
- Yoon, K, Hoogduin, L & Zhang, L 2015, 'Big data as complementary audit evidence', *Accounting Horizons*, vol. 29, no. 2, pp. 431-438. <https://doi.org/10.2308/acch-51076>
- Zaby, S & Pohl, M 2019, 'The management of reputational risks in banks: Findings from Germany and Switzerland', *Sage Open*, vol. 6, no. 3, pp. 1-15.
- Zakaria, KM, Nawawi, A & Salin, ASA 2016, 'Internal controls and fraud - Empirical evidence from oil and gas company', *Journal of Financial Crime*, vol. 23, no. 4, pp. 1154-1168. <https://doi.org/10.1108/JFC-04-2016-0021>
- Zaslavsky, V & Strizhak, A 2006, 'Credit card fraud detection using self-organizing maps', *Information & Security*, vol. 18, pp. 48-63. <https://doi.org/10.11610/isij.1803>
- Zhang, J, Zhan, Z-H, Lin, Y, Chen, N, Gong, Y-J, Zhong, J, Chung, HSH, Li, Y & Shi, YH 2011, 'Evolutionary computation meets machine learning: A survey', *Computational Intelligence Magazine*, vol. 6, no. 4, pp. 68-75. <https://doi.org/10.1109/MCI.2011.942584>

APPENDIX

Appendix

■ Operational Definition of Terms

- **Accounting** is the process by which economic information is identified, measured and communicated to allow an informed decision or judgement by the users of such information.
- **Bank reputation** refers to public opinion about the bank in terms of proficiency, integrity and fidelity, which often results from the view of the customers and other stakeholders (Zaby & Pohl 2019, p. 1). The reputation of an organisation is referred to as a strategic intangible asset through which tangible profits and an increased value in terms of increase in turnover and revenue, lower operating expenses and employee satisfaction can be achieved. It represents an organisation's past activities and prospects, which defines its overall appeal to all its critical shareholders compared to rival organisations (Fombrun 1996, p. 72; Little & Little 2020, p. 137; Roberts & Dowling 2002, p. 1078). The variables of forensic accounting and management control systems (MCSs) were formulated into bank reputation and other sub-variables. This is because adequately implementing forensic accounting techniques and an effective MCS can promote a bank's reputation. It is an intangible asset that defines the value or worth of an organisation to its stakeholders (both internal and external). This study considered four primary factors capable of influencing a bank's reputation. These factors are bank size, corporate governance, corporate social responsibility, regulatory compliance, revenue and business ethics. Reputation is an asset that is termed more emotive than financial. It is a perception of past actions and future behaviour viewed not in isolation but in the context of what others are doing in the marketplace (CIMA 2007, p. 6). Reputation risk is defined as the risk incurred by an organisation because of changes in opinions by the major shareholders (customers, investors and regulators). The change of opinion can result from many factors: significant financial underperformance, internal fraud, customer dissatisfaction and weak internal controls. It is motivated by the conviction that the organisation's viability in achieving the objectives and targets will diminish over time (Ramy et al. 2017, p. 4). This agrees with the existing literature, which postulated that the main factors that affect the bank's reputation (reputation risk) are the size of the bank, market competition, level of involvement in corporate social responsibility, security level, issues of ethics and integrity, as well as the quality of products and services provided, among others (Buckley & Nixon 2009, p. 32; Dinc 2000, p. 798; Fang 2005, p. 27). Supporting this view, Thomas and Jain (2006, p. 48)

argued that a successful attraction of depositors and investors to the banking sector requires proper maintenance of share price, reputation for good corporate governance and regulatory compliance.

- **Computer forensics (sometimes known as computer forensic science)** involves acquiring evidence found in computers and digital storage media. Computer forensics examines digital media forensically soundly to identify, preserve, recover, analyse and present facts and opinions about digital information.
- **Computer** denotes an electronic device that accepts data through input devices (keyboard and magnetic tape) and gives out information at the output unit (visual display unit [VDU]).
- **Corporate governance** deals with how organisations are governed, and the fundamental forces governing any corporation are the management, shareholders and board of directors, which are internal and structural (Monks & Minow 2011, p. 415). Corporate governance encompasses ownership and control, mission or objectives, rights and responsibilities, and the distribution of value created (Clarke & dela Rama 2006, p. xix). Corporate governance describes the processes, customs, policies, laws and institutions that direct organisations and corporations in acting, administering and controlling their operations. This concept works towards achieving the organisation's goal and managing its relationship with the stakeholders, including the board of directors and the shareholders. It also takes into cognisance the accountability of the individuals through a mechanism that reduces the principal-agent problem in the organisation (Khan 2011, p. 1).
- **Cybersecurity** protects the organisational or personal computers, electronic systems, mobile or smart devices, network, database and other internet-connected devices from cyberattacks. The loopholes in the organisation's cyber security give rise to cyber fraud.
- **Cyber fraud** is a digital and organised form of crime in which a perpetrator employs computers, Internet connection and other IT-enabled devices to obtain money or other sensitive information from a victim illegally (Dalla & Geeta 2013; Okeshola & Adeta 2013; Walden 2007). It involves a range of crimes, such as unauthorised intrusion into the computer systems, customers' data or organisation's information (KPMG 2011). Cyberfraud is the product of modernisation traced to technological advancement. It is defined according to the US Department of Justice as any fraudulent activity that employs the internet for fraudulent solicitations, deception of victims, illegal and fraudulent transactions, or to transfer the fraud proceeds to financial institutions or others linked with the fraud (United States Department of Justice 2014, p. 1). The motivation of fraud varies by the nature of fraud as well as identified individual cases, just as the risk of cyber fraud also varies from one organisation and department to the next depending solely on the nature

of business activities carried out, organisational structure and the strategies employed to achieve set goals. However, for effective fraud control, there is a need for those in charge of cyber fraud control (forensic accountants) to work with information system users to understand the rudiments of the organisation's system operation and the business environment.

- **Financial crime** encompasses a broad range of crimes ranging from theft or fraud perpetrated by an individual to corporate or organised fraud by a group of individuals. It covers a range of crimes, such as cybercrime, tax evasion, bribery and corruption, fraud, money laundering, asset misappropriation and embezzlement.
- **Forensic accounting** integrates accounting principles, auditing, criminology and law to uncover fraud perpetration. It is understood as an independent investigation performed on behalf of an organisation to resolve disputes or fraud cases (Dubinina et al. 2018, p. 132). Forensic accounting integrates the conventional accounting system into the legal framework for fraud mitigation and provides litigation support for the prosecution of the threat actors (Clayton 2011, p. 271; Karwai 2004). Therefore, it is widely believed that forensic accounting can assist in fraud mitigation, especially financial crime, by identifying and investigating suspected fraud cases (Grubor, Ristić & Simeunović 2013, p. 1; Hibshi, Vidas & Cranor 2011, p. 81).
- **Forensic science** is the term given to investigating a crime using scientific means. It is also used as the term for applying scientific knowledge to legal matters.
- **Fraud** means deliberate misinformation or misrepresentation of the truth to manipulate or deceive an individual or an organisation for personal gain.
- **Information security** involves the protection of data or information and its properties from theft, natural disaster, and unauthorised access and activities such as modification, inspection, destruction, copying or recording and corruption while ensuring that the protected data or information is only accessible to its authorised users on demand (Aggarwal et al. 2014, p. 48). Effective protection of vital information infrastructures is critical to the security and economic well-being of any nation (Ravi 2012, p. 1). Information security can also be defined as the processes and technologies developed for the protection of networks and data from illicit access by threat actors (Tiwari, Bhalla & Rawat 2016, p. 51).
- **Information Technology** is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in a business or other enterprise.
- **Keylogging** is often referred to as keyboard capturing, which is the action of recording (or *logging*) the *keys* struck on a keyboard, typically

to secretly monitor the authorised user of the keyboard. It has uses in the study of human-computer interactions.

- **MCSs** are the structures employed by the organisation to monitor performance effectively so that corrective actions or measures can be taken where necessary and when appropriate (Noorein 2012, p. 12). However, it is widely accepted that the effective design of MCSs can stimulate organisational learning, which will ultimately enhance organisational performance (Shurafa & Mohamed 2016, p. 79).
- **Software** is a generic term applied to most nonphysical aspects of computing, that is, programs, operating systems, packages, compilers and, to some extent, systems in general.
- **White hat** is Internet slang that refers to an ethical computer hacker or a computer security expert specialising in penetration testing and other testing methodologies to ensure the security of an organisation's information systems. Ethical hacking is a term coined by International Business Machines (IBM) meant to imply a broader category than just penetration testing. White hat hackers may also work in teams called 'sneakers', red teams or tiger teams.

Index

A

ACL, 156, 159, 191, 216
advanced and emerging economies, 1, 15–16,
18, 36, 301, 307
African continent, 251, 254, 271, 305
African economy, 254
analytical hierarchy process (AHP),
79, 81–82
artificial intelligence, 81, 94, 109, 113, 244,
267–268, 302
asset misappropriation, 4, 20, 22–24,
147, 175–176, 188–189

B

big data technology, 15, 45, 95, 111–118, 120,
122, 124–125, 137, 158, 302, 309
bow tie, 235–238, 240–244, 246, 248–250

C

classification problem, 100
clustering, 93–96, 99–100, 104, 106, 109,
119–120
computerised forensic investigation, 131,
136, 213
coronavirus disease 2019 (COVID-19),
1, 3–5, 9, 18, 254
corporate social responsibility, 68, 70, 72
cyberattack, 6, 9, 16, 29, 32, 41, 58, 224, 230,
244, 254–255, 296, 304–305, 309
cybercrime legislation, 251, 264–265,
271–272
cyberfraud mitigation, 1, 13–14, 18–19, 33,
58, 65, 68, 79–82, 87, 90–93, 117–118,
135, 205, 214–215, 217–218, 226–228,
233, 235, 261, 267, 273–277, 281, 292,
298–299, 301–302, 304–306
cyberfraud risks, 235, 237, 241–242, 248,
250, 252, 293, 298, 303
cyberfraud, 1–10, 12–16, 18–19, 21, 25–28,
31–44, 46–52, 54, 56, 58, 60–62,
64–70, 72, 74, 76–77, 79–83, 87,
90–100, 102–104, 106, 108–109, 111,
116–118, 124–125, 127, 135–136, 155,
158, 173, 193, 205, 214–219, 222–228,
233–254, 256–268, 270–278,
280–296, 298–299, 301–309

cybersecurity, 13, 15–16, 18, 26, 34, 36, 41,
45, 82–91, 129, 135, 216–218, 221–222,
224, 227, 233, 236–239, 244, 252–254,
258–266, 269–271, 286–287, 293, 298,
302–303, 305–310

D

data mining, 162, 187, 228
digital crime, 194, 197, 216
digital forensics, 193–196, 198, 200, 202,
204, 206, 208, 210–212, 214–216
digital technologies, 2, 4, 8–9, 14, 18–19,
21, 26, 33, 35, 44, 49, 58, 74, 82–91,
94, 220, 247, 266, 268, 271–272, 293,
302, 308–309

E

emerging and advanced economies,
15, 18, 307
EnCase, 156, 159, 191, 216
evidence gathering and management, 191

F

financial institutions, 1–2, 6–10, 13–16, 25–28,
33–35, 37–39, 42, 44–45, 64, 74, 76,
79–80, 95, 109, 112, 144, 171, 173–178,
180, 182, 184, 186, 188, 190–192,
217–219, 221–222, 227, 233, 235–238,
240–242, 244, 250, 252, 256, 267,
274, 277, 287, 293, 295, 299, 302–304,
306–310
financial investigation, 114–115, 155–160, 162,
164, 166, 168–172
financial reporting, 23, 116, 118, 127, 142, 144,
149, 153, 156, 158–160, 169–171, 275
financial statement fraud, 5, 22–23, 111, 120,
124–125, 176, 188
forensic accounting software,
155–156, 158–160, 162–164, 166,
168, 170, 172, 191
forensic accounting, 15, 45, 55–56, 69,
71–72, 74–75, 127, 130–131, 133–135, 137,
141–142, 144–146, 150–152, 155–160,
162–164, 166–168, 170, 172–174,
176–188, 190–192, 197, 202, 273

- fraud detection, 25, 46, 54–55, 57, 72–73, 75–76, 96, 98, 111, 113, 117–119, 124, 130, 133, 140, 144, 149, 152–153, 158, 160, 162, 170, 177–178, 185, 191, 194, 205, 228–229, 295
- fraud deterrence cycle, 140–141
- fraud investigators, 9, 15, 34, 95, 104, 117, 122, 124, 133, 193, 220, 275–276
- fraud mitigation, 25, 34, 56, 58, 63–65, 67–68, 72, 77, 81, 87, 111–112, 114–116, 118, 120–122, 124–125, 127–128, 130–131, 135–137, 143, 151, 158–159, 169, 171, 173–180, 182, 184–186, 188, 190–192, 196, 201, 206, 217, 222, 225–226, 228, 233, 273, 276, 294
- fraud profiling, 77
- fraud risk scores, 93, 96, 109
- fraud types, 175
- fraud, 1–10, 12–16, 19–59, 61–65, 67–69, 71–77, 80–96, 98, 102, 104, 106, 109, 111–122, 124–125, 127–131, 133–138, 140–153, 155–162, 164–171, 173–196, 198, 200–202, 204–223, 225–230, 232–233, 236–237, 240–247, 252–254, 257, 265, 267, 271, 273–278, 280, 283, 286–288, 290, 293–299, 301–302, 304–305, 308–309
- FTK, 156, 159, 191, 216
- fuzzy analytical hierarchy process (FAHP), 79–82, 91–92
- G**
- global economy, 1, 16, 18–19, 44–46, 301, 303, 307
- I**
- information communication technology (ICT), 1–2, 6, 26, 30, 45, 116, 127–128, 130–133, 135, 151, 242, 262–263, 269–270, 303, 308
- IDEA, 49, 68, 147, 156, 159, 188, 191, 216
- information security, 13, 34, 39, 69, 81, 118, 211–212, 217–223, 227–230, 232–233, 238, 256, 267, 276, 293, 304
- internal controls, 31, 35–36, 49, 52, 64, 86–87, 136, 226–227, 242, 251, 272, 275–276, 293, 302
- internal fraud, 5, 12, 20, 24–25, 218, 228
- L**
- litigation, 35, 55–56, 71–76, 130, 133–134, 140, 143, 149, 156–157, 160–162, 174–177, 180, 183, 185–188, 190, 194–195, 199, 203, 205, 210–213, 243, 296, 303
- M**
- machine learning, 28, 93–96, 98, 100, 102, 104, 106, 108–109, 123–124, 228
- macroeconomy, 303
- management control systems (MCSs), 45, 56, 63–69, 135, 242, 274–277, 292, 298–299
- MCD, 79–83, 91–92
- multicriteria decision, 79
- P**
- pattern recognition, 94, 97, 109, 113, 170, 215, 229
- policy lessons, 301–304, 306, 308, 310
- R**
- rank, 10, 144
- regulatory framework, 184, 216, 251, 271
- risk assessment, 10, 13, 28, 75, 87, 133, 140–141, 177, 238–241, 274, 276, 287–289, 291, 294, 296–299
- risk management, 10, 25, 33, 35–36, 53, 68, 81, 87, 120, 122, 135, 182, 185–186, 188, 192, 221–222, 224–226, 228, 235–243, 247–248, 256, 266, 275, 293–296, 298, 309
- risk matrix, 248–249
- risk mitigation, 135, 235–236, 238, 240, 242, 244, 246, 248, 250, 294, 302, 305
- S**
- security breach, 219, 304
- security policies, 192, 224
- South African banking industry, 87, 267, 273, 277, 286, 298
- specialised algorithms, 94, 96, 109
- SPSS, 155, 160–161, 163, 171, 274, 277, 281–285, 288–292, 298
- statistical analysis, 116, 134, 155, 163, 171, 273, 277–278, 281–285, 288–293, 298
- systems thinking, 217–218, 220, 222, 224–226, 228, 230, 232–234
- T**
- Tableau, 156, 159, 191, 216
- technological requirements, 251, 271
- theoretical framework, 47–48, 77, 115
- third-party management, 274, 287–290, 293, 298–299
- W**
- weights, 79–81, 83, 86–87, 90–91, 97–98, 107–109

This book offers a comprehensive overview of global cyberfraud statistics in Africa alongside practical insights for scholars seeking effective risk management solutions in the modern age. It explores cutting-edge technologies such as information and communication technology (ICT) and forensic accounting, equipping scholars with the tools and analytics necessary to stay ahead of cyber threats. The editors have combined case studies, empirical findings, and systematic literature reviews to provide actionable strategies for mitigating cyberfraud, examining its causes, threat actors, and mitigation strategies. By taking a closer look at digital forensics and emerging technologies, scholars will be able to gain a deeper understanding of how fraud profiles and mitigation frameworks can be used. With its practical and systems-thinking approaches and in-depth analysis, *Understanding and mitigating cyberfraud in Africa* is an indispensable resource for scholars alike.

This book provides scholars with a unique reading experience as they shed light on an issue of paramount concern, *Understanding and mitigating cyberfraud in Africa* is an invaluable contribution to a world grappling with escalating cyber threats. By analysing this phenomenon through a multi-methodological approach, the book offers a comprehensive perspective on cyberfraud that transcends traditional boundaries, unveiling a holistic understanding of the complexities surrounding the mitigation of a growing concern in an increasingly technologically integrated world. Its emphasis on the African experience rectifies a conspicuous void in the current body of knowledge. The book effectively fills this gap by delving into the unique challenges and strategies specific to the African context to enrich the global discourse on cyberfraud.

This scholarly book is an essential reference for policymakers seeking innovative solutions considering the collected contributions. Its meticulously crafted insights provide a roadmap for crafting creative policies that safeguard economic prosperity to empower scholars to navigate the intricate terrain of cyberfraud prevention effectively. In a world marred by digital threats, this publication stands as a beacon of knowledge, ensuring its place as a pivotal resource in the fight against cyberfraud.

Dr Jacques de Jongh, Department of Economic Sciences, Faculty of Economic and Management Sciences, North-West University, Vanderbijlpark, South Africa



Open access at
<https://doi.org/10.4102/aosis.2024.BK485>



ISBN: 978-1-991269-08-9