An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

Jihad Al Wahshi

A thesis submitted in partial fulfilment of the requirements

for the degree of Doctor of Philosophy

The University of Sheffield

Faculty of Social Sciences

Information School

May 2024

Declaration

I, the author, confirm that the Thesis is my own work. I am aware of the University's Guidance on the Use of Unfair Means (www.sheffield.ac.uk/ssid/unfair-means**).** This work has not previously been presented for an award at this, or any other, university.

Abstract

Background and Aims: Money laundering (ML) poses significant risks to global financial systems in general and the banking sector in particular. The United Nations Office on Drugs and Crime estimates that the total amount of money laundered annually is 2–5% of global domestic product or roughly US$800 billion to US$2 trillion. However, the rapid growth of data/information in the form of large transaction volumes makes it challenging for banks to detect illicit financial flows from large volumes of transactional data. Information governance (IG) can play a critical role in mitigating ML risks by providing banks with a holistic framework for managing their information assets in a more organised manner. Despite IG's promising benefits, there is a lack of empirical studies in this area. This present research aims to address this gap by investigating how various IG practices can help banks in Oman to mitigate ML risks.

Methods: This study adopted a qualitative collective-case study approach underpinned by constructivist ontology and interpretivist epistemology. An IG theory by Tallon, Ramirez, and Short (2013) was used as a theoretical lens to guide this study. Data were collected using two primary methods: semi-structured interviews and document reviews. Participants were recruited from nine Omani banks: one regulatory, six local, one specialised and one foreign (international). Fifty semi-structured interviews were conducted with IG professionals from different organisational levels. A thematic analysis was used to analyse the collected data.

Results: This study showed that IG practices played a positive role in mitigating the risks of ML in the Omani banking sector. Analyses of interviews revealed various structural, procedural and relational practices that contributed to ML risk mitigation including data ownership responsibilities, compliance monitoring, data integration, data validation, access control, training and collaboration among key stakeholders. Additionally, the empirical findings suggest that the maturity of these governance practices and their impact on risk mitigation efforts is influenced by the degree of regulatory compliance, senior management support, technological capabilities and funding.

Contribution to knowledge: This study makes significant contributions to theory, methodology and practice. Theoretically, this study fills a gap in the literature by providing new insights into the role of IG practices in mitigating the risks of ML. It also contributes to the IG literature by extending IG theory to the banking sector and uncovering various empirical findings related to antecedents (enablers and inhibitors), governance practices and consequences. More importantly, the empirical findings shed new light on the relationships between these themes, enhancing the understanding of different contextual factors that may have a positive impact on the maturity of specific IG practices. The use of a collective-case study in the IG context can be considered a methodological contribution as it allowed for the investigation of various IG issues across different Omani banks, which enhanced the transferability of the results pertaining to Omani banking sector. This study provides practical recommendations for regulators, policymakers and banking institutions to improve the maturity of IG practices at the organisational and sectoral levels.

Keywords: information governance, data governance, money laundering, risk mitigation, the Omani banking sector, collective case study

Acknowledgements

I would like to thank my Almighty Allah for this opportunity. I would like to express my deepest gratitude to my esteemed supervisors, Dr. Jonathan Foster and Dr. Pamela Abbott, for their invaluable guidance throughout my academic journey. You have contributed greatly to the successful completion of my thesis. Your exceptional academic skills and careful attention to the details of my thesis were crucial in shaping the quality and coherence of my research. Thank you.

I would like to thank my family, particularly my Mom and Father, for their unconditional love, prayers, and encouragement. I owe a debt of gratitude to my brothers and sisters for their unwavering support and for always being there when I needed them.

Special and big thanks go to my beloved wife, Dr. Salima Al Alawi. Your unwavering support, understanding, and sacrifices have been pivotal in helping me navigate the challenges of this endeavour. Your belief in me has been a cornerstone of my success, and your love has been my greatest source of strength and motivation. I am eternally grateful for your patience and for standing by my side through every step of this journey. I also like also to thank my dear sons (Abdul Aziz, Abdul Rahman, and Yahya), your love and joy have been a constant source of motivation. Your smiles and laughter have brought light to my darkest days, and your understanding and patience have been remarkable. Thank you for being my inspiration and for giving me the strength to persevere.

I would like to thank the many friends, relatives, and supporters who have made this happen. My special thanks go to my exceptional friends who stand with me in every step during this journey, particularly Dr Anas Al Suhaibani, Dr Khalid Al Shumari, Dr Abdullah Al Mahrouqi, and Ahmed Anuhayt. I am also grateful to my information school friends and all staff.

I would also like to thank the Omani government for providing me a scholarship to study in the United Kingdom and sponsoring my research study.

I would also like to acknowledge the participants of this study, whose cooperation and willingness to share their experiences have been fundamental to the success of this research. Your contributions have provided invaluable insights and have significantly enriched this work.

A special note of appreciation goes to my employer, the Central Bank of Oman, for granting me the opportunity to pursue my studies abroad. Your support and flexibility have been crucial in enabling me to balance my professional and academic commitments.

Special thanks indeed go the Executive President, His Excellency Tahir Sailm Al Amari for granting me this opportunity.

Thank you all for your unwavering support and encouragement.

Dedication

With love, I dedicate this thesis to my beloved wife, Dr Salima Al Alawi, whose unlimited support, love, and encouragement have been my guiding light throughout this journey.

To my dear sons (Abdul Aziz, Abdul Rahman, and Yahya).

To my family (Mom, Father, brothers and sisters), whose collective support has been invaluable.

To the memory of those who have passed away.

To myself, for the relentless hard work, perseverance, and dedication that have made this achievement possible

List of Peer-Reviewed Publications

Al Wahshi, J., Foster, J., & Abbott, P. (2021). An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector. *IConference 2021*.

Al Wahshi, J., Foster, J., & Abbott, P. (2022). An investigation into the role of data governance in improving data quality: A case study of the Omani banking sector. *ECIS 2022 Research Papers*. Retrieved from https://aisel.aisnet.org/ecis2022_rp/121

Table of Contents

Declaration ii

Abstract iii

Acknowledgements v

Dedication vii

List of Peer-Reviewed Publications viii

Table of Contents ix

List of Abbreviations xviii

Chapter 1: Introduction 1

1.1 Introduction 1

1.2 Research Background 6

1.2.1 Overview of Money Laundering 6

1.2.2 Risks and Challenges of Money Laundering in the Banking Industry 9

1.2.3 Global and Regional Initiatives to Combat the Risks of Money Laundering 12

1.2.4 Oman's Efforts to Combat the Risks of Money Laundering 12

1.3 Research Aims, Objectives and Questions 15

1.3.1 Aim 15

1.3.2 Objectives 15

1.3.3 Research Questions 16

1.4 Thesis Structure 16

Chapter 2: Literature Review 18

2.1 Chapter Overview 18

2.2 Literature Search and Review 18

2.3 Information Governance and Its Concepts 21

2.3.1 Understanding the Concept of Governance 21

2.3.2 The Origins and Evolution of Information Governance 23

2.3.3 Definition of Information Governance 24

2.3.4 Information Governance, Data Governance and IT Governance 28

2.4 IG Frameworks 29

2.5 Antecedents of Information Governance 32

2.5.1 Enablers of Information Governance 33

2.5.2 Inhibitors of Information Governance 40

2.6 Information Governance Practices 43

2.6.1 Structural Practices 43

2.6.2 Procedural Practices 45

2.6.3 Relational Practices 46

2.7 Consequences of Information Governance 46

2.7.1 Intermediate Performance Effects 48

2.7.2 Risk Mitigation 50

2.8 Gaps in the Literature 51

Chapter 3: Research Methodology 52

3.1 Introduction 52

3.2 The Theoretical Framework of the Study 52

3.3 Philosophical Assumptions 54

3.3.1 The Ontological Stance 55

3.3.2 The Epistemological Stance 57

3.4 Research Approaches: Inductive and Deductive Reasoning 60

3.4.1 Rationale for Adopting the Inductive Approach 64

3.5 Research Design 64

3.5.1 Qualitative Research 65

3.6 Research Strategy 67

3.6.1 Case Study Research 67

3.6.2 The Case Study Design 70

3.6.2.1 Defining the Case: Unit of Analysis 70

3.6.2.2 Determining the Type of Case Study Design 72

3.6.2.3 Selection of Cases 75

3.6.2.4 Boundaries of the Cases 81

3.7 The Research Context 82

3.8 The Study Sample 84

3.9 Data Collection Methods 87

3.9.1 Semi-Structured Interviews 87

3.9.2 Document Review 92

3.10 Data Analysis Method 94

3.10.1 Thematic Analysis 96

3.10.2 Stage 2: Cross-Case Analyses 99

3.11 Reflections on the research process 99

3.11.1 The role of the researcher 99

3.11.2 Positionality Statement 103

3.11.3 Research quality 105

3.11 Ethical Considerations 109

3.11.1 Obtaining ethical approval 110

3.11.2 Informed consent 110

3.11.3 Data Management 111

3.11.4 Reflection on Ethical Challenges in the Banking Context 112

3.12 Strengths and Limitations of the Methodology Approach 113

Chapter 4: Data Analysis and Findings 115

4.1 Chapter Overview 115

4.2 Antecedents of Information Governance 119

4.2.1 Enablers of Information Governance 119

4.2.2 Inhibitors of Information Governance 135

4.3 Information Governance Practices 160

4.3.1 Structural Practices 160

4.3.2 Procedural Practices 170

4.3.3 Relational Practices 187

4.4 Consequences of Information Governance 194

4.4.1 Intermediate Performance Effects 195

4.4.2 Risk Mitigation 201

Chapter 5: Cross-Case Analyses 205

5.1 Introduction 205

5.2 Overview of the Case Classification 205

5.3 Similarities and Differences of the Cases.. 208

5.3.1 Antecedents of Information Governance 208

5.3.2 Information Governance Practices 213

5.3.3 Consequences of Information Governance 225

5.4 Strategies for Improving IG Practices: Practical Steps for Navigating From Basic to Advanced Levels.. 228

5.4.1 Conduct comprehensive training on IG 228

5.4.2 Develop clear policies and procedures 229

5.4.3 Assign clear roles and responsibilities 230

5.4.4 Leverage new information technologies 231

5.4.5 Develop an information culture 231

5.4.6 Integrate data into a single repository 232

Chapter 6: Discussion 233

6.1 Introduction 233

6.2 Antecedents of Information Governance 233

6.2.1 IG Enablers 233

6.2.2 IG Inhibitors 242

6.3 Relationships between the themes 248

6.3.1 Factors shaping structural practices 248

6.3.2 Factors shaping procedural practices 252

6.3.3 Factors shaping relational practices 254

6.4 Consequences of information governance 256

6.4.1 Intermediate performance effects 257

6.4.2 Risk mitigation 260

6.4.3 The Relationships between Intermediate Performance Effects and Risk Mitigation 263

6.5 Final research model 264

6.6 Chapter Summary 265

Chapter 7: Conclusion 266

7.1 Chapter Overview 266

7.2 Addressing the Research Questions 266

7.3 Contributions to Knowledge 286

7.3.1 Empirical contribution 286

7.3.2 Theoretical Contribution 288

7.3.3 Methodological Contribution 290

7.4 Recommendations for practice and policy 291

7.4.1 Omani banking institutions 292

7.4.2 Compliance and AML professionals 295

7.4.3 Central Bank of Oman 296

7.5 Limitations and Future Research 299

7.6 Reflection on the Research Journey 302

References 307

Appendices 345

Appendix 1: Interviews Guide 345

Appendix 2: Information Sheet 350

Appendix 3: Informed Consent 357

Appendix 4: Participant Profile 359

Appendix 5: Coding Framework 362

Appendix 6: Data Management Plan 372

Appendix 7: Descriptions of Case Studies 377

List of Tables

Table 1: Inclusion and exclusion criteria for literature selection 21

Table 2: Definitions of information governance, developed for this research 26

Table 3: IG frameworks identified in this review (developed for this research)......................... 31

Table 4: Synthesis of studies on IG enablers 40

Table 5: Comparison of inductive and deductive approaches (adapted from Bryman, 2004; Creswell, 2009).. 64

Table 6: A summary of methodologies adopted in IG Studies 67

Table 7: Factors influencing the adoption of the case study design (adapted from Yin, 2014)... 70

Table 8: Typology of a case study (Thomas, 2011, p. 518) 72

Table 9: Inclusion and exclusion criteria for case selection 80

Table 10: List of selected cases for this research 81

Table 11: Overview of Oman's banking industry (Central Bank of Oman, 2024)........................ 84

Table 12: Inclusion and exclusion criteria for the selection of participants................................ 85

Table 13: Examples of documents reviewed in this study 94

Table 14: Cross-Case Analysis of IG practices across eight banks 208

Table 15: Frequency counts of IG enablers across the eight banks 209

Table 16: Frequency counts of IG inhibitors across the eight banks... 212

Table 17: Frequency counts of structural practices across the eight banks 213

Table 18: Frequency counts of procedural practices.. 217

Table 19: Frequency counts of relational practices across the eight banks.............................. 225

Table 20: Summary Findings—Factors shaping structural practices.. 251

Table 21: Summary Findings—Factors shaping procedural practices...................................... 254

Table 22: Summary Findings—Factors shaping relational practices 256

Table 23: Summary Findings—Factors and/or IG practices led to intermediate performance effects 259

Table 24: Summary Findings—Factors and/or IG practices led to ML risk mitigation 263

Table 25: Summary of IG enablers in the Omani banking sector 268

Table 26: Summary of IG inhibitors in the Omani banking sector 272

Table 27: Summary of structural practices adopted by Omani banks 277

Table 28: Summary of procedural practices adopted by Omani banks 279

Table 29: Summary of relational practices adopted by Omani banks...................................... 281

Table 30: Summary of intermediate performance effects identified in this study 284

Table 31: Summary Findings—Consequences of IG on risks mitigation 286

Table 32: Islamic Products 383

Table 33: Specialised Products 386

List of Figures

Figure 1: The money-laundering process: Placement, layering and integration (adapted from UNODC, 2023) 9

Figure 2: The theoretical framework of this study (Tallon et al., 2013) 54

Figure 3: Basic types of case study designs (Yin, 2018) 74

Figure 4: A step-by-step process for selecting cases 78

Figure 5: Stages of TA (adapted from Braun & Clarke, 2006) 96

Figure 6: Thematic map of the study 118

Figure 7: Proposed Research Model 265

List of Abbreviations

AIG: Advanced Information Governance

AML: Anti-Money Laundering

AML/CFT: Anti-Money Laundering and Combating the Financing of Terrorism

ARMA: Association of Records Managers and Administrators

BIG: Basic Information Governance

CBO: Central Bank of Oman

CDD: Customer Due Diligence

CG: Corporate Governance

DG: Data Governance

EDRM: Electronic Discovery Reference Model

EU: European Union

FATF: Financial Action Task Force

FI: Financial Institutions

FIU: Financial Intelligence Unit

GARP: Generally Accepted Recordkeeping Principles

IFF: Illicit Financial Flows

IG: Information Governance

IGCMM: Information Governance Council Maturity Model

IGMM: Information Governance Maturity Model

IGRM: Information Governance Reference Model

IIG: Intermediate Information Governance

ILM: Information Life-Cycle Management

ITG: Information Technology Governance

KYC: Know Your Customer

MENAFATF: Middle East and North Africa Financial Action Task Force

ML: Money Laundering

NHS: National Health Service

PII: Personally Identifiable Information

RIM: Records and Information Management

STR: Suspicious Transaction Report

TF: Terrorism Financing

UNODC: United Nations Office on Drugs and Crime

Chapter 1: Introduction

1.1 Introduction

Money laundering (ML) is a complex and serious financial crime (Alldridge, 2008; Buchanan, 2004; Hopton, 2009). It often involves sophisticated techniques and a series of illicit financial flows that cross the borders of multiple financial systems located in different jurisdictions (Irwin & Turner, 2018; Levi et al., 2006; Naheem, 2018). In essence, ML involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through ML, a criminal transforms monetary proceeds derived from criminal activity into funds that have an apparently legal source. (Hopton, 2009). Organised crimes may include profits obtained from activities such as drug trafficking, corruption, tax evasion, robbery or fraud (Alldridge, 2003; Johnson, 2001; Levi, 2015). The United Nations Office on Drugs and Crime (UNODC) estimates that the total worldwide laundered proceeds per year amount to 2% to 5% of the global domestic product or roughly US$800 billion to US$2 trillion (UNODC, 2023).

At the regional level, a study conducted by the Middle East and North Africa Financial Action Task Force (MENAFATF) showed that between 2010–2012, there was a significant increase in ML cases, and the percentage of money laundered through banks rose from 83% to 90% (MENAFATF, 2013). According to the same study, non-financial institutions (e.g., real estate agents and accountants) account for 5% of the total ML cases across MENA countries. This misuse of banks confirms the findings of previous studies in the ML literature (e.g., Carrington, 2006; Sarigul, 2013; Yeoh, 2019).

Narrowing the scope to Oman, in its 2019 report, the National Centre for Financial Information (NCFI) reported an increase of 63% in the number of suspicious transaction reports (STRs) received from different reporting entities, including banks and other financial institutions, compared with the preceding five years (i.e., 2014–2019) (NCFI, 2019). The recent mutual evaluation report of anti-money laundering in Oman highlights that a significant number of backlog alerts have been flagged as 'suspicious', but many of these have not yet been forwarded to law enforcement bodies such as financial intelligence unit (FIU) (FATF, 2011). Moreover, the report emphasises the need for enhancing mechanisms to address the backlog and improve coordination between reporting entities and law enforcement agencies to strengthen the overall effectiveness of the anti-money laundering framework in Oman.

Due to globalisation, financial systems are now interconnected (Alldridge, 2008; Buchanan, 2004). This means that when a country fails to implement sound anti-money laundering (AML) governance, offenders' actions can affect other countries (Isa et al., 2015). Recently, ML has been implicated for financing terrorism (Biersteker & Eckert, 2007). Therefore, it affects both the stability of global financial systems and world peace (Aluko & Bagheri, 2012; Unger & Busuioc, 2007). For AML to be effective, best practices and preventive measures need to be implemented to enhance the capacity of financial institutions, which act as the frontline of defence in detecting and combating ML risks (Isa et al., 2015; Pramod, Li, & Gao, 2012; Simonova, 2011).

Thus far, research on ML has mainly focused on technology (Demetis, 2010; Gao & Ye, 2007; Pramod et al., 2012; Singh & Best, 2019; Yasaka, 2017) and regulatory approaches: for instance, the know your customer (KYC)[1] policy (Arasa & Ottichilo, 2015; Broek & Addink, 2013; Gill & Taylor, 2004; Mclaughlin & Pavelka, 2013). However, the role of information governance (IG) practices (or IG programme) in mitigating ML risks has received little attention, despite their usefulness in improving the reliability and trustworthiness of risk management information and organisational performance (Soares, 2011; Tallon et al., 2013).

Information governance is an emerging concept in the IM literature (Hagmann, 2013; Kooper et al., 2011) that has been developed in response to the increasing complexity and volume of information in modern organisation, coupled with the inadequacy of IT governance in managing various aspects of the information life cycle (Tallon et al., 2013). Although the term 'information governance' appears new, its core principles and practices have existed for many years (Hagmann, 2013; Peppard, 1999). While there is no generally accepted definition of IG, it can be broadly defined "a collection of capabilities or practices for the creation, capture, valuation, storage, usage, control, access, archival and deletion of information over its life cycle" (Tallon et al., 2013, p. 2).

The literature showed that new technologies—such as artificial intelligence (AI), big data analytics, blockchain, and cloud computing— has enhanced the capacities of banks in detecting and preventing suspicious activities associated with money laundering (Jullum, Løland, & Huseby, 2020; Singh & Best, 2019). For example, the adoption of AI and machine learning

[1] Know your customer (KYC) is one of the key regulations of AML that requires financial institutions to collect relevant evidence such as a copy of a passport or a civil identity card that can help a compliance officer identify a customer's true identity.

technologies has enabled banks to identify complex patterns and anomalies in transactional data (Jullum et al., 2020). Similarly, big data analytics facilitates real-time processing of large datasets, allowing bankers to uncover hidden trends that may indicate money laundering (Singh & Best, 2019). Additionally, blockchain technology ensures transparency and traceability in financial transactions through its decentralized and immutable ledger, reducing opportunities for illicit or fraudulent activities (Albrecht, Duffin, Hawkins, & Rocha, 2019). However, managing complex and massive amounts of transactional information like ML involves a coordinated approach and mechanisms, especially when information is seen as a strategic asset for survival in the industry (Fernan Faria et al., 2013). By drawing on an extensive review of the IT governance literature, Tallon et al. (2013) proposed a holistic IG framework based on qualitative data collected from 30 organisations across multiple industries, including financial services.

Tallon et al.'s framework comprises three key elements: antecedents, IG practices (structural, procedural and relational), and consequences. First, antecedents are subdivided into enablers and inhibiting factors: the former motivate or speed up the adoption of IG practices in an organisation while the latter creates obstacles that constrain or limit their capacity or use. Second, the composition of IG practices involves procedures for the allocation of decision rights, policies for ensuring effective management of information (e.g., backups, retention periods and information sharing) and relational practices for improving collaboration and training among key stakeholders. Finally, the study concluded that the increased use of IG practices across all participating firms led to intermediate performance effects and risk mitigation.

Tallon et al.’s (2013) framework serves as an important benchmark in the IG literature because it is grounded in empirical evidence rather than being focused on theoretical concepts (e.g., Abraham et al., 2019) or specific sector-based organisational contexts (e.g., Donaldson & Walker, 2004; Kusumah & Suhardi, 2014; Lajara & Maçada, 2013; Silic & Back, 2013). While Tallon et al.’s framework provides a systematic approach to understand conditions, practices, and consequences of IG within the organisational level; it is argued that it provides one way of viewing IG from an internal organisational perspective (Lomas, 2010). Because the scope of this study focuses on improving the internal IG capacities of banks, Tallon et al.’s (2013) framework was used as a theoretical lens in this study.

It has been argued that an IG programme can reduce risks and improve the performance of AML departments (Fernan Faria et al., 2013; S Soares, 2011). Soares (2011) observed that the adoption of IG practices in a large financial institution has led to improved KYC policies and reduced the number of false positives. Other studies (Fernando Faria & Simpson, 2013; S Soares, 2011; Traulsen & Tröbs, 2011) reported that the implementation of an IG programme has enabled bankers to integrate the related financial and operational data, such as opening accounts and cash deposits, into a centralised repository, which results in better analysis and assessment of ML risks. Having an integrated approach like IG not only connects data but also helps compliance officers predict and detect fraudulent or suspicious activities that cannot otherwise be observed through decentralised repositories (Ballard et al., 2014). However, analysing mountains of transactional information requires active monitoring and application of state-of-the-art techniques, such as artificial intelligence or data visualisation, to discover hidden patterns or criminal activity from complex datasets (Le Khac & Kechadi, 2010; Singh & Best, 2019).

While IG appears to play a critical role in reducing the risks of ML, limited empirical investigations have been identified in the current literature. The identified studies do not address ML problems per se, but they provide a general understanding of IG adoption in the banking industry (Fernan Faria et al., 2013; Fernando Faria & Simpson, 2013; Soares, 2011). To the best of the researcher's knowledge, this is the first study that attempts to provide an in-depth understanding of the antecedents, practices and consequences of IG implementation on the ML context.

1.2 Research Background

1.2.1 Overview of Money Laundering

Money laundering is one of the most pervasive and dangerous financial crimes in the world that can hinder economic growth and undermine financial stability in the country (Aluko & Bagheri, 2012; Basaran-Brooks, 2022; International Monetary Fund, 2008; Masciandaro, 2017). Therefore, regulators and international bodies, such as the Financial Action Task Force (FATF), the International Monetary Fund (IMF) and the World Bank have developed stringent measures and controls to help banks and other financial institutions safeguard their financial systems by detecting and reporting suspicious transactions to competent authorities, such as FIUs and central banks (FATF, 2023; Levi et al., 2006). According to the FATF, which is globally recognised as a policymaker for international AML laws and regulations, the term "money laundering (ML)" is defined as the process by which individuals attempt to disguise or hide the original source of their illicit proceeds (cash or funds) obtained from criminal activities, such as drug trafficking, arms smuggling, bribery, corruption, embezzlement and fraud (FATF, 2023).

In the context of the current study, a person is considered to be involved or participated in an ML crime if "he or she intentionally converts or transfers such funds to disguise or conceal the illegal nature or source of such proceeds, or if [he] assisting any person who committed the predicate offence to evade punishment for their acts" (Central Bank of Oman, 2016, Article 6). The techniques used for concealing illicit proceeds range from traditional cash deposits (Levi et al., 2006; Riccardi & Levi, 2018) to more sophisticated methods driven by new technologies, notably cryptocurrencies (Albrecht et al., 2019; Brenig et al., 2015; Wronka, 2022). Despite the differences between these ML techniques, there is a consensus that the money laundering process should involve three key stages: placement, layering and integration (Cassella, 2018; Levi et al., 2006; Sultan & Mohamed, 2022a).

Placement is the first stage where illicit or dirty money is introduced into formal banking systems via structured deposits of large cash or by mixing it with legitimate proceeds obtained from a cash-intensive business, such as a gas station, restaurant, café or casino (Cassella, 2018; Naheem, 2016a; Sultan & Mohamed, 2022a). In this way, money launderers aim to legitimise illicit proceeds by converting them into various types of assets to make them less suspicious of law enforcement and investigative authorities (Brenig et al., 2015). However, the placement phase is found to be more vulnerable and harmful to money launderers because illicit transactions can be detected and prevented by monitoring systems at this stage (Albrecht et al., 2019; Naheem, 2016a).

The second stage, layering, involves the transfer of illicit funds through a series of complex banking transactions (both electronic and wired) to distance or hide the ownership and source of laundered money (Cassella, 2018; Gilmour, 2023). This may include the transfer of small amounts of payments into multiple accounts at various banks (Naheem, 2016a), particularly those that operate in jurisdictions with weak or ineffective AML regulations (Brenig et al., 2015).

The third stage of the ML process is known as ‘integration’, by which laundered money is re-integrated into the mainstream economy as legitimate funds (Cassella, 2018; Sultan & Mohamed, 2022a). A simple technique to legitimise these illicit funds is by purchasing real investments like bonds, bank notes or properties, making it much more difficult for law enforcement authorities and financial institutions to detect and trace back the source of these funds (Albrecht et al., 2019; Wronka, 2022).

By explaining the ML process, it becomes clear that banks and other financial institutions are the primary target for criminals due to the complexity and variety of banking services (e.g., wire transfers, loans and foreign exchanges) that allow them to move and disguise their dirty money (Isa et al., 2015; Naheem, 2016a). Figure 1 below illustrates the three stages of ML that criminals often use to launder illicit proceeds.

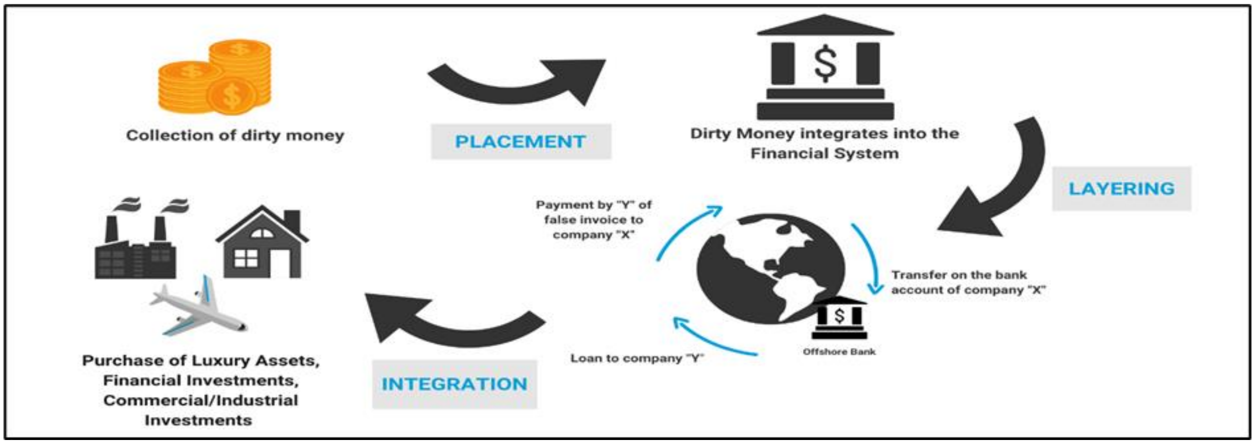

Collection of dirty money
PLACEMENT
Dirty Money integrates into the Financial System
LAYERING
Payment by "Y" of false invoice to company "X"
Transfer on the bank account of company "X"
Offshore Bank
Loan to company "Y"
INTEGRATION
Purchase of Luxury Assets, Financial Investments, Commercial/Industrial Investments

Figure 1: The money-laundering process: Placement, layering and integration (adapted from UNODC, 2023)

1.2.2 Risks and Challenges of Money Laundering in the Banking Industry

As indicated above, the complex array of financial services can provide a haven for money launderers, exposing banks to major risks that may destabilise the entire banking industry (Isa et al., 2015; Kot, 2021; Zaman et al., 2020). Broadly speaking, risks associated with ML can be classified into financial, legal, reputational, operational and regulatory risks (Isa et al., 2015). The most cited ML risks observed in the banking industry include financial penalties, regulatory sanctions, reputational damage, licence revocation, legal liability and loss of customer trust (Basaran-Brooks, 2022; Naheem, 2016b; Sarigul, 2013; Zaman et al., 2020).

In a study of 72 banks in Pakistan and Malaysia, Zaman et al. (2020) found that ML had a negative consequence on banking profitability due to substantial financial penalties imposed for noncompliance with AML regulations. For instance, the US-based HSBC bank was fined nearly US$1.9 billion to avoid legal prosecution after it was discovered that the bank had allowed Mexican drug traffickers to launder illicit proceeds through its banking systems (Naheem, 2016c, 2018). Undoubtedly, such a banking scandal can damage a bank’s reputation and diminish customers’ and investors’ trust (Brien & Dixon, 2013; Sarigul, 2013). Therefore, the FATF and the Basel Committee on Banking Supervision (BCSB) have provided banks with detailed guidance to assist them in developing a sound risk management programme for mitigating ML risks (BCBC, 2020; FATF, 2015a, 2022). Nevertheless, many banks are struggling to implement and comply with existing AML regulations due to several challenges including the illicit-transaction volume as well as a lack of information sharing, awareness and cooperation among stakeholders (Kot, 2021; Viritha et al., 2015).

The large volume of illicit transactions poses a significant challenge for banks in implementing effective AML governance because it makes it difficult or impossible to distinguish between suspicious and legitimate transactions in a sea of data (Irwin & Turner, 2018; Naheem, 2018; Viritha et al., 2015). The dynamic nature of these transactions leads to information overload, which exceeds banks' technological and human resource capabilities (Isa et al., 2015). Furthermore, the anonymity of new payment systems, such as cryptocurrencies and peer-to-peer networks, increases the rate of illicit financial transactions to an unprecedented level given the unique design that enables users to hide their true identities (Brenig et al., 2015; Irwin & Turner, 2018; Wegberg et al., 2018). This may pose risks to KYC regulations as banks are required to identify and collect accurate information about their customers before initiating a transaction (FATF, 2022; Renny & Miru, 2019).

Another challenge that hinders banks' efforts in assessing their customers' risk is a lack of information sharing (Sultan & Mohamed, 2022b; Viritha et al., 2015). Although the exchange of information has been emphasised in the FATF recommendation (FATF, 2017), this area is still lacking due to privacy concerns and legal restrictions that prevent the sharing of customer information within and across different financial institutions (Sultan & Mohamed, 2022b). This limitation impedes AML compliance officers' daily operations and provides an incomplete picture of financial transactions, which ultimately leads to erroneous risk assessment (Viritha et al., 2015). By sharing information, banks can avoid entering into relationships with suspected clients who have been blacklisted and reported by other banking institutions thereby preventing them from abusing the financial system by approaching one bank after another (Viritha et al., 2015). Currently in Oman, banks informally exchange ML-related information via telephone calls, emails and occasional meetings (Al Ghassani et al., 2017; Al Wahshi et al., 2021).

Lastly, and perhaps most importantly, previous studies have found that a lack of awareness of basic AML requirements is one of the biggest challenges facing commercial banks in complying with relevant AML laws (Naheem, 2016a; Subbotina, 2009; Viritha et al., 2015). According to AML law, banks must develop a comprehensive training programme for all employees, including the board of directors, covering key aspects of the AML regime, such as recordkeeping, KYC requirements, risk assessment, regulatory reporting and data security (FATF, 2022). Indeed, employees may overlook these requirements if they do not understand their negative impact on the bank's reputation and regulatory compliance (Sarigul, 2013; Zaman et al., 2020). Naheem (2016a) found that there is an "ever-increasing knowledge gap between the bank's awareness of financial crime and the criminal's knowledge of ML schemes" (p. 144). To close this gap, banks of all sizes must conduct regular training and awareness programmes for their employees to assess their understanding of recent ML trends and techniques (Simwayi & Guohua, 2011).

To summarise, a review of the relevant literature identified three key challenges hindering the implementation of AML regulations in the banking industry (Naheem, 2016a;

Subbotina, 2009; Viritha et al., 2015): the volume of illicit transactions, lack of information sharing and lack of employee training and awareness.

1.2.3 Global and Regional Initiatives to Combat the Risks of Money Laundering

Remarkable initiatives have been made at the international, regional and national levels to deter ML operations (BCBC, 2020; FATF, 2022; UNODC, 2009). The first international efforts began in 1988 with the United Nations Vienna Convention (UNODC, 1988), which mandates Member States to criminalise drug-related ML activities (Article 3b). Despite the restricted scope of this Convention, it contains a detailed definition of ML, which has served as the basis for AML regulations across the globe (Jayasekara, 2020). Since then, FATF has issued 40 recommendations that address various techniques that offenders could use to abuse financial systems (FATF, 2015b, 2022). At the regional level, the MENAFATF was established in 2004, and it works hand-in-hand with the FATF to ensure members' compliance with the 40 ML recommendations through mutual evaluation and follow-up efforts (FATF, 2011). Despite these initiatives, the overall effectiveness of the AML framework in banks is still low due to a lack of cooperation, trust and transparency across countries (Jayasekara, 2020; Naheem, 2016a).

1.2.4 Oman's Efforts to Combat the Risks of Money Laundering

The Sultanate of Oman, which is a member of FATF and MENAFATF, is committed to applying international best practices to combat ML by implementing some initiatives and measures, including enacting new AML regulations, establishing the NCFI, launching a national registry system (e-KYC), conducting regular awareness programmes and increasing cooperation with other countries (CBO, n.d.; NCFI, 2021). The country, according to the last mutual evaluation report conducted in 2011, largely complies with FATF recommendations and international standards (FATF, 2011). In line with FATF recommendations, the AML law of Oman criminalises any acts of ML and imposes heavy penalties on those who are found to be involved directly or indirectly in this criminal activity [Article 6]. Also, the law prohibits banks and other financial institutions from opening new accounts or providing services to anonymous customers until they verify and confirm the customer's identity [Article 35]. Given their anonymity and potential use in ML, the Central Bank of Oman (CBO) has recently cautioned the public from using, holding or investing in cryptocurrencies or similar products, and stated that "cryptocurrencies are not a legal tender in the Sultanate of Oman" (CBO, 2020, p. 22).

At the sectoral level, the government of Oman – via Royal Decree (38/2019)— has established a national databank known as the Oman Credit and Financial Information Centre (Mala'a), which contains financial and non-financial information about customers (individuals and corporates) aggregated from several data providers, including government entities, financial institutions, SMEs and telecommunications companies (CBO, 2019). Although this national databank is at the nascent stage of development, it helps banks and other financial institutions to streamline and automate the KYC and customer onboarding processes by accessing relevant, accurate and up-to-date information (Oman Observer, 2023).

The Sultanate of Oman, in collaboration with regulatory and investigative authorities, has conducted a series of training and awareness programmes to educate the public and financial institutions about ML risks and the importance of complying with established AML regulations (NCFI, 2021). The Sultanate also worked with international organisations, such as the US Department of Justice, to provide advanced AML training to law enforcement and other government agencies (Bureau of Counterterrorism, 2019).

Despite the significant efforts made by the Omani government to mitigate the risks of ML, several challenges persist. Many banks, including those of Omani banks, are struggling to follow AML requirements due to poor information management practices including lack of data quality, lack of information sharing, information silos, ineffective data retention policies and legacy information systems (Al Wahshi et al., 2022; Dadashzade, 2018; Tyagi, 2021). Previous research has suggested that weak governance of ML-related information can have negative consequences for a bank's reputation and compliance (Kristian et al., 2022; Naheem, 2016a). For example, Kristian et al. (2022) found that inaccurate and invalid customer information (KYC) can increase the risks of ML in banks because it leads to incorrect classification of a customer's risk profile, which makes it difficult for compliance officers to identify and track suspicious transactions.

While information servers are a core component of the AML framework, a few studies have empirically examined the role of IG in the ML context context (Al Wahshi et al., 2021). To date, the majority of ML studies have largely focused on regulatory (Issah et al., 2022; Jaffery & Mughal, 2020; Ofoeda et al., 2022), policy (Lokanan & Nasimi, 2020) and technical (Han et al., 2020; Jullum et al., 2020; Lokanan, 2022) aspects. To close this gap, this present study proposes an IG framework as a novel approach to mitigating the risks associated with money laundering-related information. The proposed framework includes areas of risk management, information management, compliance, decision rights, data quality, recordkeeping and training (Tallon et al., 2013).

1.3 Research Aims, Objectives and Questions

1.3.1 Aim

This current study investigated how various IG practices (structural, procedural and relational) can help Omani banks mitigate the risks of ML.

1.3.2 Objectives

The following objectives were developed to achieve the research aim:

1. Conduct semi-structured interviews to identify antecedents or conditions that enable or inhibit the adoption of IG practices in Oman.
2. Conduct semi-structured interviews to identify the structural, procedural and relational practices adopted by Omani banks to manage their AML-related data or information.
3. Identify the consequences of adopting IG practices on banks' intermediate performance and risk mitigation.
4. Perform a cross-cases analysis to identify the similarities and differences across Omani banks in relation to their antecedents, IG practices and consequences, and to understand why these differences exist.
5. To provide recommendations for Omani banks to other stakeholders to improve their current IG practices
6. Develop an IG model for Omani banks based on the empirical findings of the study

1.3.3 Research Questions

In light of the aforementioned objectives, the following research questions were formulated:

- **RQ 1:** What antecedents enable or inhibit the adoption of IG practices in Omani banks?
- **RQ 2:** What IG practices have Omani banks adopted to manage AML-related data or information?
- **RQ 3:** What are the consequences of adopting IG practices in Omani banks?
- **RQ 4:** What are the similarities and differences across Omani banks in relation to the antecedents, IG practices and consequences? Why do these differences and similarities exist? How might these practices or the governance of ML-related data/ information be improved?

1.4 Thesis Structure

The overall structure of this thesis is organised into seven chapters:

- **Chapter one:** Introduces the research context, followed by the research aims, objectives and questions. Also, it presents the intended contributions of this study from the theoretical, practical and methodological perspectives.
- **Chapter two:** Reviews theoretical concepts and previous studies related to the area of this research. The first section of this chapter defines the concept of information governance, and its origins. It then differentiate the IG concept from other similar terms such as data governance, IT governance, and corporate governance. It then reviews various structural, procedural and relational practices that constitute an IG programme. In this way, it provides a review of multiple IG frameworks, investigates, and selects the

suitable one for this study. At the end of this chapter, a summary and synthesis of the literature are presented, and research gaps are highlighted.

- **Chapter three:** Articulates the methodology, philosophies and theoretical dimensions underpinning this research. This chapter begins by introducing and justifying the theoretical framework chosen for this study. Next, it discusses the research paradigms and highlights the ontology and epistemology stances adopted. Next, it describes the methods applied in this research, followed by a rationale for their selection. The chapter also explains how the empirical data will be collected and analysed. Finally, the potential ethical issues emerging from this research are discussed, and a data management plan (DMP) is presented.
- **Chapter four:** Presents and summarises the findings that emerged from the analysis of interview data.
- **Chapter five:** Synthesises and compares findings from eight banks (cases) to identify their similarities and differences in relation to the antecedents, IG practices, and consequences.
- **Chapter six**: Contains a full discussion, interpretation and evaluation of the study results with reference to the literature.
- **Chapter seven:** Highlights this research's conclusions, limitations and recommendations: theory, practical implications and how this study can be extended.

Chapter 2: Literature Review

2.1 Chapter Overview

This chapter provides a review and theoretical discussion of the concepts of IG and ML. First, it introduces the term ML, providing an overview of its meanings, processes, challenges and risks. Second, it conceptualises the concept of IG, providing a review of its origin, definitions, goals and objectives. Third, it analyses and evaluates various IG frameworks and models identified in the literature, highlighting their strengths and weaknesses. Fourth, it investigates the antecedents, governance practices and consequences of IG in the banking industry. This chapter concludes with a focused synthesis of the most relevant literature and a discussion of the knowledge gaps in this literature.

2.2 Literature Search and Review

Undertaking a literature review reliably and transparently is considered a cornerstone of good research (Cronin et al., 2008; Levy & Timothy, 2006). According to Levy and Timothy (2006) and Tobin and Begley (2004), an effective literature review lies in its methodological rigour and ability to produce unbiased findings. This section outlines the steps followed to conduct the literature review for this research.

Following the best practices provided by Cronin et al. (2008), the literature review began by developing a search strategy, which involved the identification of the topic review, search terms and relevant databases. An initial scoping search was carried out using a "funnel" technique (Berthon et al., 2003), by which broad terms were used before gradually narrowing the focus to the specific topic under investigation. Grey literature (such as Ph.D theses and dissertations) was searched to identify relevant unpublished studies. This search was facilitated using electronic databases, such as the Ethos British Library and ProQuest Dissertations and Theses. However, no relevant studies were identified, except for a few studies (e.g., Randhawa, 2019; Seboka, 2015) that were more general in nature and did not directly address the research questions.

A further in-depth search was conducted using academic databases and search engines, which are known to have a wide collection of publications on IG and ML. Examples of the databases and search engines used to identify relevant literature included Google Scholar, ProQuest, Business Source Premier (EBSCO Host), Science Direct, Emerald Insight, Web of Science, ACM Digital Library, IEEE Xplore, JSTOR and AIS Electronic Library.

The identification of relevant studies was facilitated by using a combination of search terms, as shown below:

- "Information governance"
- "Information governance in banking"
- "Information governance" AND "Omani banking"
- ("Information governance") AND ("banking" OR "financial institutions")
- "Money laundering" OR "financial crime" OR "illicit transactions"
- ("Information governance") AND ("Money laundering" OR "financial crime" OR "illicit transactions")
- ("Information governance") AND ("risk management" OR "risk mitigation")

In some cases, however, the term “data governance” was used to expand the search scope and to ensure that no relevant studies were overlooked. This is because some researchers tend to use the terms “information governance” and “data governance” interchangeably. The inclusion and exclusion criteria used in this review are presented in the table below.

Criteria	**Inclusion**	**Exclusion**
Publication date	Studies published from 2013–2023	Studies published before 2013 (unless seminal work)
Language	Articles written in English	Articles written in languages other than English
Publication type	Peer-reviewed journal articles, conference papers, books, official governmental documents and banking reports	Non-peer-reviewed articles, grey literature, theses, dissertations working/white papers, letters, blogs and news articles
Research methodology	● Qualitative or quantitative studies ● Empirical studies with a clear methodology	● Editorial or conceptual papers presented as reviews ● Opinion pieces without empirical evidence
Databases/journals searched	● ProQuest, Business Source Premier (EBSCO Host), Science Direct, Emerald Insight, Web of Science, ACM Digital Library, IEEE Xplore, JSTOR, AIS Electronic Library, Google Scholar ● *Journal of Management Information Systems*, *International Journal of Information Management*, *Journal of Information Management*, *Journal of Money Laundering Control*, *Journal of Financial Crime*, *Journal of Banking* and *Finance* and the *Journal of Banking Regulation*	● Any other databases/journals

Keywords	• “Information governance”, “Data governance”, “Money laundering”, “financial crime”, “illicit transactions”, “risk mitigation”, “Risk management”, “Omani banking industry”	• Articles that do not match the keywords

Table 1: Inclusion and exclusion criteria for literature selection

2.3 Information Governance and Its Concepts

This section defines the IG concept and sheds light on its origins and development.

2.3.1 Understanding the Concept of Governance

The concept of ‘governance’ carries a vast and intricate meaning that encompasses various aspects of human society (Kooiman, 2003; Rhodes, 2007). In recent years, this concept has gained popularity in many social sciences disciplines, including political science, international relations, corporate management, economics and public administration (Kooiman, 1999, 2003; Rhodes, 2007). According to the Oxford Dictionary, the term “governance” was derived originally from the Greek word “*kubernan*”, which means “to steer” or “to guide” (Oxford English Dictionary, 2023). A review of the literature indicated that the notion of governance is not new despite being treated as a ‘fashionable word’ (Kooiman, 1999; Pechlaner et al., 2010; Rose-Ackerman, 2017; Stoker, 1998). Traditionally, this term was used by many researchers and international organisations (e.g., World Bank, 1997) to signify “a change in the meaning of government; referring to a new process of governing; or a changed condition of ordered rule; or the new method by which society is governed” (Rhodes, 1996, p. 652–653).

However, Rhodes (1996) and Pechlaner et al. (2010) argued that governance has a broader meaning, which goes beyond the realm of government; therefore, it should not be used interchangeably. According to Kooiman (2003), governance can broadly be defined as “the totality of interactions, in which public, as well as private actors, participate, aimed at solving societal problems or creating societal opportunities; attending to the institutions as contexts for these governing interactions; and establishing a normative foundation for all those activities" (p. 4). Simply put, governance can be understood as "interaction between the formal institutions and those of civil society" (Weiss, 2012, p. 797). It reflects how different actors or stakeholders interact with each other to achieve shared goals (Shleifer & Vishny, 2007).

The governance approach, as explained by Kooiman (2003), Font (2000) and Weiss (2012), is a complex, multifaceted and ever-changing process because it involves diverse systems and entities, such as governmental institutions, non-governmental organisations, and the broader community. A primary challenge encountered with governance is ensuring that every voice is acknowledged and taken into account (Weiss, 2012). This necessitates establishing effective mechanisms that promote citizen participation, transparency in decision-making processes and accountability of those in power (Kooiman, 2008; Rhodes, 1996).

Although there are many models of governance, they all share a common goal: to improve people's lives through collective action while exercising responsible leadership (Rhodes, 2007). However, attaining these goals can be challenging due to the complexity and diversity of socio-political issues within countries or regions (Kooiman, 1999). Consequently, many researchers (e.g., Font, 2000; Kooiman, 1999, 2016; Rhodes, 1996) consider 'interaction' as the core element of good governance, arguing that actors alone lack the knowledge to address complex, dynamic and diversified societal challenges.

Good governance serves as a fundamental pillar for both organisations and nations to achieve their goals through effective decision-making, leadership and policy implementation

(Weiss, 2012). However, there is a lack of consensus among scholars on what constitutes good governance because of the various meanings and interpretations attached to the term ‘governance’ (Barbazza & Tello, 2014). Pechlaner et al.’s (2010) analysis of published studies on governance revealed six overarching principles of good governance that are frequently cited in academic and practitioner publications: (1) accountability, (2) transparency, (3) stakeholder participation, (4) organisational structure, (5) effectiveness and (6) power.

Of course, these underlying dimensions may differ based on the characteristics of the system-to-be-governed, such as an organisation or a sector (Kooiman, 2008; Kooiman & Bavinck, 2005), which suggests that the one-size model does not fit all (Weber, Otto, & Osterle, 2009). Also, Pomeranz and Stedman (2020) found that the various principles of good governance are interconnected and influenced by each other, meaning that they cannot be separated in a practical setting.

To summarise, the term governance has been used in many different ways, but it is generally understood to mean ‘authority’, ‘steering’, ‘control’ and ‘democracy’ (Font, 2000; Rose-Ackerman, 2017). Interaction is considered a cornerstone of the governance approach for resolving complex issues and achieving shared goals (Kooiman, 2008). Good governance is characterised by several principles, including accountability, transparency, stakeholder participation, organisational structure, effectiveness and power (Pechlaner et al., 2010).

2.3.2 The Origins and Evolution of Information Governance

Information governance (IG) is an emerging concept in the IM literature (Hagmann, 2013; Kooper et al., 2011) that has been developed in response to the inadequacy of IT governance in managing various aspects of the information life cycle (Tallon et al., 2013).

Although the term ‘information governance’ appears new, its core principles and practices have existed for many years (Hagmann, 2013; Peppard, 1999). According to the literature review, IG concept was first introduced by Donaldson and Walker (2004) to address issues related to the confidentiality and privacy of patient information in the UK’s National Health Service (NHS). While IG has gained significant traction and development within the health sector, particularly due to the stringent requirements for the protection of personal health data including data privacy, security, and compliance (e.g., HIPAA in the United States), its foundational principles are deeply rooted in corporate governance (Shleifer & Vishny, 2007). The principles of accountability, transparency, and strategic oversight within corporate governance has significantly influenced the evolution of IG; thereby extending its applicability beyond healthcare sector, including banking (Faria et al., 2013; Okunleye, 2023; Tyagi, 2021), education (Daneshmandnia, 2019; Muhammad et al., 2022), manufacturing (Lajara & Maçada, 2013), telecommunication (Otto, 2011) and public administration (Grimstad & Myrseth, 2011). A More detailed discussion of corporate governance and its influence on IG development is provided in section 2.3.4.

2.3.3 Definition of Information Governance

While there is no generally accepted definition of IG, it can be broadly defined as managing information over its life cycle, from its creation to its destruction or deletion (Smallwood, 2014; Tallon, Ramirez, et al., 2013). Although some researchers (e.g., Abraham et al., 2019; Faria et al., 2013; Khatri & Brown, 2010; Lis et al., 2022) tend to use ‘information governance’ and ‘data governance’ interchangeably, they are not synonymous. While information governance focuses on managing all types of information assets (including records and documents) within an organization, data governance is specifically concerned with the management, quality, and security of data throughout its lifecycle (Bennett, 2017). Table 2 provides a list of core IG definitions that were identified based on the literature search strategy described earlier in section 2.2 of this chapter.

Reference	Definition
(ARMA International, 2017)	"Information governance is the establishment of authorities, supports, processes, capabilities, structures, and infrastructure to enable information to be a useful asset and reduced liability to an organisation, based on that organisation's specific business requirements and risk tolerance".
(Faria et al., 2013)	"Information governance is seen as the establishment of policies, through formal structures that define rules, procedures and decision-making rights regarding information management, to mitigate regulatory and operational risk, reduce costs and optimise the performance of the organisation" (p. 4444).
(Gartner, 2019)	"Information governance defined as the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals" (p. 1).
(Hagmann, 2013)	"IG is the art of trusted interaction between the major stakeholders of an IG programme (IT, Business, Legal and Compliance, RIM, Security and Privacy). They aspire to join up to minimise information risks to the enterprise while maximising the value of information assets through building desirable behaviours and enabling cross-functional decision-making" (p. 231).
(Hulme, 2012)	"Information Governance is a holistic approach to managing and using information for business benefits that encompasses information quality, information life-cycle management, and security, privacy and compliance" (p. 100).
(ISO, 2022)	"The strategic framework for governing information assets across an entire organization in order to enhance coordinated support for the achievement of business outcomes and obtain assurance that the risks to its information, and thereby the operation capabilities and integrity of the organization, are effectively identified and managed" (p. 3)
(Information Governance Initiative, 2016)	"The activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs".

(Kooper et al., 2011)	“Information governance involves establishing an environment and opportunities, rules and decision-making rights for the valuation, creation, collection, analysis, distribution, storage, use and control of information; it answers the question “what information do we need, how do we make use of it and who is responsible for it?” (p. 1–2).
(Lajara & Maçada, 2013)	“Information governance is a set of standards, guidelines and accountability controls designed to ensure value, quality and compliance of information” (p. 1).
(Lomas, Shabou, & Grazhenskaya, 2019)	“Information governance provides a holistic ethical framework which takes into account a range of societal and individual stakeholder information needs. It enables a just process of information co-creation, sharing, management, ownership and rights including retention and deletion rights, economics, accountability and openness considering confidentiality, privacy and security needs. It transcends organizational, national and technological boundaries but takes into account diverse cultural, individual/family, community, organizational and societal needs. It is supported in its delivery by a range of practitioner expertise and citizen engagement” (p.4).
(National Archives of Australia, 2013)	“Information governance addresses how an organisation’s information assets are managed to support organisational outcomes.”
(Peppard, 1999)	“Information governance entails outlining responsibilities and accountabilities, defining the set of rules guiding decision-making, and managing the interdependencies across the range of decisions with regard to information, systems and technology” (p. 1).
(Silic & Back, 2013)	“Information governance is an emerging term which can be used to define different policies, procedures, and processes aimed at managing information at an organisational level providing support for regulatory, legal, operational, managerial and environmental risks” (p. 75).
(Sloan, 2014)	“Information governance is an organisation’s coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimising information value” (p. 2).
(Smallwood, 2019)	“Information governance is how an organisation maintains security, complies with regulations, and meets ethical standards when managing information” (p. 9).
(Soares, 2011)	“Information governance is the formulation of policy to optimise, secure, and leverage information as an enterprise asset by aligning the objectives of multiple functions” (p. 1).
(Tallon et al., 2013)	“Information governance is a collection of capabilities or practices for the creation, capture, valuation, storage, usage, control, access, archival and deletion of information over its life cycle” (p. 2).

Table 2: Definitions of information governance, developed for this research

The IG definitions cited above have been extracted from academic and practitioner publications, including journal articles, practitioner websites and industry reports. A critical analysis of these definitions suggests that the diverse perspectives of stakeholders affect how IG is conceptualised or defined. While academic authors (e.g., Kooper et al., 2011; Smallwood, 2019; Tallon et al., 2013) focus on the theoretical underpinnings of IG, business authors (e.g., ARMA International, n.d.; Gartner, 2019; Hulme, 2012) focus on the technical and practical aspects of IG.

From an academic perspective, IG is understood as a holistic approach encompassing many principles and dimensions, such as information life-cycle management, information quality, information security and compliance. For example, Peppard (1999) and Kooper et al. (2011) emphasised the importance of accountabilities and decision-making rights in achieving IG goals.

Lajara and Maçada (2013) and Silic and Back (2013) expanded the scope of the IG definition by recognising the role of policies, procedures and standards in ensuring compliance with regulatory and legal requirements. However, effective IG should not only include policies and procedures but also culture, behaviour and human interactions. This view was supported by Hagmann's (2013) definition, which places a strong emphasis on collaboration among different stakeholders (such as IT, business, compliance and legal) to facilitate cross-functional decision-making. Tallon et al. (2013) provided the most comprehensive definition because it covers the entire information life cycle.

From the practitioner/ business perspective, IG is seen as a solution that can help organisations to achieve their goals. This perspective reflects the mindset of practitioners who pay more attention to the implementation and technical aspects of IG. In their definitions, ARMA International (2017), the Information Governance Initiative (2016) and Gartner (2019) introduced the concept of technologies to signify their role in maximising the value of information by facilitating and automating critical IG tasks. Additionally, most the practitioner' definitions cited here use the term 'IG' to highlight its importance in enhancing compliance and reducing risks. However, for this study, IG is defined as "a collection of capabilities or practices for the creation, capture, valuation, storage, usage, control, access, archival and deletion of information over its life cycle" (Tallon et al., 2013, p. 2).

While the table and discussion above primarily focus on definitions related to the organisational level, it is important to acknowledge the broader perspective of IG such as the definition provided by Lomas, Shabou, and Grazhenskaya (2019). This definition highlights dimensions such as social justice, ethical considerations, and cultural diversity, which are particularly relevant in public sector and interdisciplinary contexts. Although these aspects fall outside the scope of this research, they enrich the understanding of IG as a multifaceted discipline with applications in both public and private sector contexts.

2.3.4 Information Governance, Data Governance and IT Governance

The extant literature shows that there is considerable confusion around the term IG and other similar industry terms, including data governance (DG), information technology governance (ITG) and corporate governance (CG) (Smallwood, 2014). Although these terms have different meanings and goals, they play crucial roles in ensuring the successful implementation of IG programmes in organisations (Hagmann, 2013; Olaitan, Herselman, & Wayi, 2016). However, the three terms (i.e., IG, DG and ITG) are a subset of CG (Smallwood, 2014).

DG focuses on establishing frameworks for managing data assets at the root level (Bennett, 2017; Olaitan et al., 2016). It involves defining roles and responsibilities related to data quality standards, security measures and privacy considerations (Khatri & Brown, 2010). IT governance (ITG), however, ensures that organisations make informed decisions regarding technological investments while maximising value delivery from IT initiatives (Van Grembergen, 2004; Weill & Ross, 2004b). Lastly, CG provides overall strategic direction by setting forth guidelines for ethical behaviour, determining accountability mechanisms enacted by organisational leadership and providing a framework for stakeholder engagement (Pechlaner et al., 2010). Simply put, it defines how the organisation is directed and controlled.

2.4 IG Frameworks

As articulated in the previous sections, the adoption of IG programmes/ or practices in a specific organisation can be driven by their intended goals, which may range from compliance with regulatory requirements and improving data quality to mitigating information-related risks (Smallwood, 2014). The differences in IG goals have led to the development of several IG frameworks and models by different researchers and practitioners (see Table 3). These underlying frameworks, according to Foster et al. (2018), “to a greater or lesser extent, reflect the who, how and to what of information governance” (1422).

This statement suggests that IG frameworks may vary in terms of the key areas—namely roles and responsibilities (who is responsible for what information), governance practices (how information is governed) and scope of governance (what information is governed). Therefore, it is important for organisations to critically evaluate the strengths and weaknesses of each framework to select one that suits their unique requirements (Kooper et al., 2011). However, IG professionals must bear in mind that a “one-size framework does not fit all” (Weber et al., 2009).

Framework/model Name	**Research setting/perspective**	**Components/constructs dimensions/ domains**	**Goal/ focus of IG**	**References**
NHS’s Information Governance framework	Healthcare	Standards Arbitration (ownership) Indemnity and support Regulations	- Improve security and confidentiality of patient records	(Donaldson & Walker, 2004)
ARMA International Information Governance Implementation Model (IGIM)	Records and Information Management (RIM) perspective	Authorities Supports Processes Capabilities Structures Infrastructure Steering committee	- Risk mitigation - Value generation	(ARMA International, 2019)
Information Governance Reference Model (IGRM)	E-discovery	Duty Value Asset	- Enhance the collaboration and communication among key stakeholders	(EDRM.net, 2012)
IBM’s Information Governance Council Maturity Model (IGCMM)	Vendor perspective	People Process Technology	- Uncover new revenue opportunities - Reduce cost - Improve operational efficiency	(Hulme, 2012; IBM, 2014)
Tallon, Ramirez, and Short’s Information Governance framework	Multiple organisations from different industries	Antecedents (enablers and inhibitors) IG practices (structural, procedural, and relational) Consequences	- Risk mitigation - Maximising the value of information	(Tallon, Ramirez, & Short, 2013)
Faria’s Information	Banking industry	People Policy	- Mitigate regulatory and	(Faria et al., 2013)

Governance Framework (IGF)		Technology	operational risks - Optimise performance	
Lajara's Information Governance framework	Defence Manufacturing company	Information value Information quality Information compliance	- Improve information quality and compliance	(Lajara & Maçada, 2013)
Integrated IG framework	Country level (South Africa)	Corporate governance Records management IT governance Data privacy Knowledge management Master data management Information security Information risk	- Centralise and coordinate governance structure at a country level	(Mullon & Ngoepe, 2019)

Table 3: IG frameworks identified in this review (developed for this research)

From the records management perspective, ARMA International has proposed an IG model based on eight Generally Accepted Recordkeeping Principles (GARP)[2], focusing mainly on managing records from creation to destruction (ARMA International, 2019). Another framework called the Information Governance Reference Model (IGRM) emphasises the need to foster collaboration and communication among key stakeholders, including IT, RIM, the legal department and the business (EDRM.net, 2012). Likewise, IBM has created a maturity model that can help organisations bridge the gap between where they are currently and where they desire to be, thereby uncovering the business benefits of information (IBM, 2014).

From the banking industry perspective, Faria et al. (2013) established an IG comprising multiple factors grouped into three primary dimensions: people, technology and policy. However, this framework does not provide details on those factors that may enable or constrain the adoption of IG practices in banks. Recognising that executives and stakeholders

[2] More details about the principles can be found at https://www.arma.org/page/principles.

require access to accurate information, Lajara and Maçada (2013) built an IG model focusing on information quality, compliance and value. Mullon and Ngoepe (2019) developed an IG framework to elevate IG capacity at the country level. More importantly, Tallon et al. (2013) developed an IG framework based on an extensive review of IT governance literature and in-depth interviews with key IT/IS executives from different industries, including banking and finance.

Unlike the aforementioned frameworks, Tallon, Ramirez, et al.'s (2013) framework is more holistic because it encompasses key elements of IG, such as antecedents (enablers and inhibitors), governance practices and consequences. It also provides a road map and a ready-made structure that can be customised to tailor to an organisation's unique requirements. Given these reasons, Tallon, Ramirez et al.'s (2013) framework was adopted as a theoretical lens to guide this research. More details about the key constructs and components of this framework are provided in the Methodology chapter.

2.5 Antecedents of Information Governance

The previous sections focus on establishing background information about information governance, defining key concepts and reviewing IG frameworks. This section reviews and highlights the various antecedents of IG in the banking industry. Consistent with Tallon et al. (2013), the term 'antecedents' in this current study refers to those factors (both internals and externals) that enable or inhibit the adoption of IG practices in banks. These antecedents can have a positive or negative impact on the maturity and development of IG practices; therefore, organisations must strategically identify and assess them to ensure the success of their IG initiatives (Abraham et al., 2019; Kwan et al., 2022; Tallon, Ramirez et al., 2013).

A review of the literature, however, revealed that there is a scant amount of studies investigating IG antecedents in the banking industry. The majority of relevant studies either focus on the theoretical elements of the IG framework (e.g., Faria et al., 2013) or the effects of IG practices on banking performance (e.g., Okunleye, 2023; Soares, 2011). Despite this knowledge gap, an attempt was made by the researcher to anticipate and differentiate the antecedents from the banking industry by broadening the search scope to cover IG literature in similar industries, such as healthcare and telecommunications. The researcher also reviewed relevant publications in the grey literature, including industry reports, white papers, Ph.D. theses and regulatory guidelines, to gain a more comprehensive understanding of IG antecedents in the banking industry. Following Tallon et al.'s (2013) framework, the IG antecedents in this study are subdivided into (1) enablers and (2) inhibitors, as shown in the following two sections.

2.5.1 Enablers of Information Governance

2.5.1.1 Regulatory Compliance

Compliance with laws and regulations is a key antecedent factor that has pushed banks and financial institutions to implement robust IG practices (Fernan Faria et al., 2013; Traulsen & Tröbs, 2011; Tyagi, 2021). Extensive research has been conducted to examine the impact of data-related regulations, such as the General Data Protection Regulation (GDPR), on IG implementation (Schoch, 2016; Shu & Jahankhani, 2017; Ula et al., 2011). A review of the literature revealed a plethora of banking regulations and international standards (e.g., AML laws, Sarbanes-Oxley (SOX) Act, PCI DSS and Basel III) that mandate banks to frequently update or enhance their internal policies, procedures and technologies to comply with information-related requirements (Tyagi, 2021).

According to Soares (2011), the ever-increasing regulatory requirements of AML at both the national and international levels have put greater pressure on banks to enhance their information management capabilities by upgrading their IT infrastructure and data storage mechanisms. For instance, under AML laws and regulations, banks of any size have to establish a mechanism to retain customer-related information (both electronic and physical) for a long period—a minimum of five years (FATF, 2022). This often entails a significant investment in data archival systems and the recruitment of subject-matter experts in records management and compliance (Smallwood, 2014; S Soares, 2011). However, excessive regulation may lead to 'compliance fatigue' due to the increased burden on banks to comply with ever-changing laws and regulations, which renders them more vulnerable to noncompliance risks (Becher & Frye, 2011). Therefore, a balance between regulation and governance is recommended to ensure that all banks can effectively adhere to applicable information requirements without incurring additional costs or regulatory burdens (Becher & Frye, 2011).

2.5.1.2 Information Growth Rate

Banks are experiencing a massive growth of information due to the expansion of digital services, digitalisation, the use of big data analytics, an increased number of customer transactions and increased regulations (Beath et al., 2012; Delgosha et al., 2021; Fernan Faria et al., 2013; Parameswarappa, 2022). Also, fierce competition among banks has triggered them to collect more information about their customers from various social media platforms, such as

Twitter and Facebook, to improve their customer service and gain a competitive advantage (Coyne et al., 2018; Fernando Faria & Simpson, 2013).

In their qualitative study, Tallon et al. (2013) found that the information growth rate was the key driver that triggered many organisations to adopt more effective IG practices. This finding was supported by Faria et al. (2013) who found that the complexity and exponential growth of both structured and unstructured data forced banks to increase their expenditure on storage devices and data management solutions. However, evidence has shown that the exponential growth of raw data is likely to increase the risks of data leakage and criminal activities, especially when this data is being used or accessed by external users, such as digital banking customers (Azmoodeh & Dehghantanha, 2020; Safar & Al-Najjar, 2006). This means that the more data the organisation has, the likelier it is to implement IG practices to mitigate information-related risks (Coyne et al., 2018; Mathes, 2016).

2.5.1.3 New Information Technologies

The adoption of new information technologies such as artificial intelligence, big data analytics, blockchain and cloud computing has revolutionised and reshaped IG practices in the banking industry (Alhassan et al., 2019; Shetty & Mallick, 2022; Srivastava & Gopalkrishnan, 2015). The majority of IG studies (e.g., Aguboshim et al., 2019; Alhassan et al., 2019; Bazel et al., 2021; Faria et al., 2013; Muhammad et al., 2022; Smith, 2015) considered technology to be a fundamental element and key enabler of IG implementation. This is not surprising given the role that new technologies play in “automat[ing] repetitive IG activities and processes, enhancing productivity, and reducing operational costs” (Mahanti, 2021, p. 145).

Alhassan et al. (2019) found that the implementation of advanced analytics capabilities enabled banks to comply with regulatory requirements by automating complex IG policies and rules related to the retention and archiving of customer data. A similar finding was reported by Smith (2015) who cited “technology automation” as one of the critical success factors for IG implementation among Fortune 500 companies in the United States. As such, it can be argued that advanced IG technologies and tools have the potential to reduce or eliminate many of the challenges IG professionals face when implementing relevant information policies and processes manually (Mahanti, 2021; Smith, 2015). Despite IG benefits, organisations should bear in mind that technology does not replace the role of people, but rather it supports and complements them by enabling IG professionals to enhance their information management capabilities, make informed decisions and achieve higher levels of productivity (Mahanti, 2021; Saxena & Ali Said Mansour Al-Tamimi, 2017; Shetty & Mallick, 2022).

2.5.1.4 Information Security and Privacy

Information security and privacy are important factors that trigger banks to implement robust IG practices, not only to comply with regulatory requirements but also to maintain reputation and customer trust (Soares, 2011; Tyagi, 2021; Ula et al., 2011). The emergence of data protection regulations, such as the GDPR and the Payment Card Industry Data Security Standards (PCI DSS), is forcing banks to improve their security policies and mechanisms to ensure the confidentiality, integrity and availability of sensitive financial and customer data (Serrado et al., 2020; Soares, 2011).

Furthermore, the expansion of digital services has created a secure channel for hackers and cybercriminals to exploit and steal sensitive customer data thereby elevating the risks of data breaches in the banking industry (Alzoubi et al., 2022). For example, during the COVID-19 pandemic, many organisations, including banks, experienced a substantial surge in cyberattacks (Ahmed & Tushar, 2020). This trend highlights the urgent need to implement a holistic IG framework to safeguard banks from potential reputational, financial and legal consequences (Ahmed & Tushar, 2020; AlGhamdi et al., 2020; Lomas, 2020; Tyagi, 2021).

Lomas (2020) argued that implementing an IG framework enables organisations to align their data security policies with overall business goals, ensuring that data security practices (for example, access control, data classification and data encryption) are integrated throughout different levels of the organisation. By integrating such practices into their business operations, bankers can ensure that their information assets are protected in accordance with organisational, industry and international best practices (Serrado et al., 2020). However, research has shown that the human factor represents the most vulnerable part of information security governance (Rahman et al., 2021); consequently, banks must establish an effective training programme to educate their employees on emerging cybersecurity threats and best practices to reduce their risks. To summarise, having an effective IG programme can help banks mitigate reputational, legal and financial risks by enhancing the protection of sensitive financial information.

2.5.1.5 Organisational/IT Strategy

Empirical evidence has shown that organisations with strategic IT-business alignment can overcome IG challenges, such as budget constraints and technology limitations, making their governance practices more relevant, effective and sustainable (Burmeister et al., 2020; Mikalef et al., 2018a; Tallon et al., 2013). According to Smallwood (2019) and Soares (2011a), aligning IT and business strategies enables organisations to establish a shared vision for IG, allocate necessary budgets and resources and implement effective technologies to support the IG initiative. Furthermore, it is through this alignment that different IG stakeholders (including IT and information security) recognise the strategic importance of information in achieving organisational goals (Kooper et al., 2011).

In their interviews with IT executives, Tallon et al. (2013) found that data and its growth rate have become integral elements of IT strategies and plans. This finding not only demonstrates that IT managers are aware of the strategic role of information but also holds them accountable for applying best practices to ensure that this information is managed effectively and responsibly. However, aligning IT and business strategies is challenging because it requires a deep understanding of both business and IT requirements, ongoing communication and coordination, balancing competing priorities, effective resource management and ensuring that IT investments are aligned with the overall business strategy (Njanka et al., 2021; Soares, 2011a).

2.8.1.6 Information Culture

The literature review showed a positive relationship between information culture and IG effectiveness (Choo, 2013; Daneshmandnia, 2019; Lian et al., 2022; Svärd, 2014). According to seminal researchers (e.g., Choo et al., 2006; Curry & Moore, 2003; Oliver, 2008), information culture is shaped by employees' actions and interactions with information. They argued that the values, norms and attitudes that employees acquire from an organisation have a significant impact on how information is perceived, used, shared and governed. Because the underlying values and norms are developed and practised within an organisation, information culture is found to be intertwined with organisational culture (Choo, 2013; Oliver, 2008; Svärd, 2014).

Additionally, it has been suggested that compliance requirements (e.g., recordkeeping and the protection of customer information) play a critical role in shaping organisations' information cultures (Oliver, 2008; Wright, 2013). For example, increased regulatory scrutiny to maintain accurate customer information (i.e., KYC) can help banks develop a strong compliance culture by educating employees about the risks of non-compliance, which may influence employees' attitudes and behaviours towards information (Faria et al., 2013; Soares, 2011a).

Previous research has found that certain types of information culture enable firms to adopt more effective IG practices and thereby improve their business performance (Curry & Moore, 2003; Daneshmandnia, 2019; Oliver, 2008; Wright, 2013). Choo (2013) identified four types of information cultures: result-oriented, rule-following, relationship-based and risk-taking. Many researchers agree that leadership style is the key determinant of information culture, although an organisation's goals and structures may also play a role in determining acceptable information behaviours and practices (Abdullah et al., 2020; Daneshmandnia, 2019). In their case studies, Lian et al. (2022) and Svärd (2014) found that leaderships' attitudes towards competitiveness and innovation have led to the effective management of records and information. This view was supported by Daneshmandnia (2019) who reported that a culture of being result-oriented/competitive can produce high-quality information.

IG Enabler(s)	References
Laws and regulatory requirements	(Tallon, Ramirez, et al., 2013), (Alhassan et al., 2019a), (Muhammad et al., 2020), (Kwan et al., 2022), (Schoch, 2016), (De Abreu Faria et al., 2013), (AlGhamdi et al,2020), (Sloan, 2014), (Shu & Jahankhani, 2017), (Becher & Frye, 2011), (Weber et al., 2009), (Mullon & Ngoepe, 2019) and (Tyagi, 2021)
Information growth rate	(Tallon, Ramirez, et al., 2013), (Beath et al., 2012), (De Abreu Faria et al., 2013), (Tallon et al., 2013), (Sudra, 2020), (Tavakoli & Jahanbakhsh, 2013), (Delgosha et al., 2021), (Lis et al., 2022), (Mikalef et al., 2018) and (Malik, 2013)
Adoption of new technologies	(Bazel et al., 2021), (Winter & Davidson, 2019), (Aguboshim et al., 2019), (Al-Ruithe & Benkhelifa, 2017), (Holmes, 2016),
Senior management support	(Grimstad & Myrseth, 2011), (Shepherd et al., 2010) and (Alhassan et al., 2019b)
Information culture	(Daneshmandnia, 2019a), (Choo, 2013), (Svärd, 2014), (Wright, 2013), (Abdullah et al., 2020), (Lian et al., 2022), (Lauri et al., 2021), (Choo et al., 2006), (Liu, 2013) and (Oliver, 2008)
Organisation structure	(Otto, 2011) and (Tallon, Ramirez, et al., 2013)

Table 4: Synthesis of studies on IG enablers

2.5.2 Inhibitors of Information Governance

The previous section has provided a nuanced understanding of the factors that enable and facilitate the implementation of IG practices in the banking industry. While these enabling factors can help organisations achieve their IG goals, several challenges inhibit or hinder their IG efforts (Tallon et al., 2013). These challenges may arise from various sources, including technological limitations, organisational culture, product complexity, budget constraints and human resources. However, the ability to identify and address these challenges plays a pivotal role in determining the outcome of an IG project and, therefore, warrants critical examination. The following section highlights the key inhibiting factors that impede banks in implementing effective IG practices, categorising them based on their importance and impact.

2.5.2.1 Legacy IT Systems

Legacy IT systems pose a major challenge to the development of IG practices in the banking sector (Hayretci & Aydemir, 2021; Seboka, 2015). Despite lacking the technical capabilities required for IG implementation, these outdated systems contain valuable historical information that can be used for business benefit (Seboka, 2015). However, previous studies have shown that many organisations, including banks, struggle to capitalise on this information due to a lack of accessibility, flexibility, scalability and data integration capabilities (Ceruti, 2004; Hayretci & Aydemir, 2021).

According to Tallon (2013), the presence of 'silo-oriented legacy systems' in a highly complex environment like the banking industry hinders both process integration and data standardisation, making it difficult to implement unified data formats and standards across different systems within the organisation. Indeed, banks recognise the need to replace their core banking legacy systems with modern information systems, but their efforts are often hampered by the complexity of migrating data from old to new systems (Hayretci & Aydemir, 2021). Tyagi (2021) concluded that the complexity of migrating legacy systems in banks presents a significant challenge to data warehousing efforts, leading to data silos, non-compliance risks and data quality issues.

2.5.2.2 Data Quality Issues

Data quality problem is another significant challenge hindering the successful implementation of IG practices in the banking industry (Al Wahshi et al., 2022; Bruno et al., 2017; Karkošková, 2022). Research has shown that poor data quality can undermine many data management initiatives, particularly data warehousing and business intelligence (Debbarma et al., 2013; Li et al., 2010), resulting in financial and operational losses (Najjar & Bishu, 2005;

Redman, 1998). According to Dadashzade (2018), estimating the true cost of poor data quality is a difficult endeavour due to the hidden costs associated with ineffective decisions, customer dissatisfaction, regulatory fines and reputational damage. However, it has been argued that understanding the root causes of data quality issues is a critical first step in addressing their adverse consequences (Haug & Arlbjørn, 2011; Redman, 1998).

Dadashzade (2018) identified six key reasons behind data quality issues in local banks: (1) legacy systems, (2) lack of data integration, (3) lack of data standardisation, (4) outdated data, (5) incorrect data entry caused by human error and (6) weak CG. According to the same author, banks with legacy or unintegrated systems are more vulnerable to data inconsistencies since these systems often operate in silos, preventing them from implementing a uniform data standard across all systems.

Unfortunately, most banks are still using these fragmented systems to store critical information related to customer accounts, financial transactions, risk assessments, and regulatory compliance (Hayretci & Aydemir, 2021; Tyagi, 2021). However, relying on this fragmented data can lead to incorrect or inaccurate decisions, thereby exposing banks to financial, legal and reputational risks (Parker, 2007; Redman, 1998). For example, incorrect or incomplete KYC information (e.g., employment details, source of funds and address) can pose significant risks to AML governance by incorrectly assigning high-risk customers to lower-risk categories, enabling suspicious transactions to bypass monitoring systems without being detected (Soares, 2011). In light of the aforementioned, it is clear that data quality issues negatively impact the maturity of IG practices in the banking industry.

2.5.2.3 Lack of Clear Roles and Responsibilities

The absence of clear roles and responsibilities creates ambiguity and complicates IG efforts in the banking sector (Capgemini, 2019; Tyagi, 2021). This, in turn, could lead to uncertainty around who is responsible for managing and protecting sensitive customer data, which can have severe consequences for banks and their clients. Without clear guidelines on how to handle this information properly, banks risk violating existing laws and regulations or experiencing costly security breaches that damage their reputations.

2.6 Information Governance Practices

The previous section highlights the enabling and inhibiting conditions that could accelerate or slow down the adoption of IG practices in the banking industry. The following sections highlights a composition of IG practices that organisations often apply to effectively manage and protect their information assets throughout their life cycles (Abraham et al., 2019; DAMA International, 2010; Smallwood, 2014; Tallon et al., 2013). These practices, as was addressed by Foster et al. (2018), are shaped and influenced by a variety of contextual factors that stem from international, national, sectoral and organisational levels. Tallon et al. (2013) posit governance practices at the centre of their IG framework and further classify them into three sub-categories of IG practices: (1) structural practices, (2) procedural practices and (3) relational practices.

2.6.1 Structural Practices

According to Tallon et al. (2013), structural practices refer to “practices associated with setting the locus of IT decision-making or data stewardship; assignments of roles to key decision makers; practices associated with IT reporting structure; use of oversight committees or other high-level policy-setting/monitoring groups” (p. 56). As the definition implies, they comprise reporting structures, governance bodies, decision-making authorities and roles and responsibilities. In essence, structural practices serve as the backbone for IG implementation because they provide the foundation through which IG tasks can be assigned, implemented and monitored (Borgman et al., 2016). Previous studies have identified several structural roles underpinning these practices, including data owner, data producer/consumer, data steward, data quality manager, database administrator, data analyst, data scientist, data security officer, data modeller/architect and information governance specialist (Foster et al., 2018). Abraham et al. (2019) provided a comprehensive description of the scope and responsibilities of each of these roles.

Governance committees play a paramount role in improving IG practices by overseeing and providing strategic directions for the entire IG programme (Abraham et al., 2019; Tallon et al., 2013). They also monitor and evaluate the implementation of IG policies and procedures to ensure compliance with applicable laws and regulations. Of course, compliance with regulatory requirements is particularly critical for banks because it has a direct impact on their reputation and profitability (Shahin, 2013). Moreover, the governance committees contribute to the formulation of IG policies and procedures by reviewing, revising and approving them before they are implemented.

2.6.2 Procedural Practices

According to Tallon et al. (2013, p. 164), procedural practices are described as the "mechanical arm of information governance" as they identify and control how information assets are managed at different levels of an organisation. They aim to ensure that information is collected, accessed, used, secured and shared in a manner that reflects an organisation's policies, standards and regulatory requirements (Borgman et al., 2016).

The IG literature reveals a plethora of procedural practices that organisations adopt to achieve their strategic or operational goals, such as increased profitability, improved data quality and enhanced operational efficiency, by monetising the value of their information while protecting it from potential risks that could delay or impede the realisation of that value (Abraham et al., 2019; DAMA International, 2010; Smallwood, 2019; Tallon, Ramirez, et al., 2013). It is worth noting that these practices span all stages of an information life cycle and may encompass "practices for valuing information, user access, retention, archival and destruction; cost management; migration of data between storage tiers; cost recovery through chargebacks; use of e-discovery practices" (Tallon et al., 2013, p. 156).

Likewise, Abraham et al. (2019) in their systematic literature review have proposed additional procedural mechanisms, including data strategy, policies, procedures, standards, contractual agreements, performance measurement, compliance monitoring and issue management. However, these practices may vary widely across organisations based on specific circumstances, such as an organisation's size and complexity, availability of resources, organisational culture and the maturity level of IG practices (Abraham et al., 2019; Daneshmandnia, 2019; Kwan et al., 2022).

2.6.3 Relational Practices

Relational practices aim to establish a collaborative and supportive environment for IG initiative through active participation of key stakeholders, shared-learning, knowledge/ ideas exchange, communication, strategic dialogue, conflict resolution and training (Abraham et al., 2019; Borgman et al., 2016; Grembergen et al., 2011; Tallon et al., 2013). According to Peterson (2004), these practices are “voluntary actions”, “intangible” and “tacit” because they are shaped and developed through human interactions and collaboration with each other. Interactions, as argued by Kooiman (2003), are a cornerstone for establishing effective governance, and they are extremely crucial in the early phases of an IG initiative to avoid conflicts or communication gaps that may arise between IT-business stakeholders (Fernando et al., 2013). However, communication gaps have been found to be a key factor that inhibit the implementation of IG practices in banks (Fernando Faria & Simpson, 2013).

2.7 Consequences of Information Governance

The adoption of IG in the banking industry can lead to several outcomes or consequences. It can help bankers to ensure regulatory compliance (Randhawa, 2019; Sunil Soares, 2011; Tyagi, 2021), enhance operational efficiency (Fernan Faria et al., 2013; Okunleye, 2023; Sunil Soares, 2011), improve data quality (Al Wahshi et al., 2022; Karkošková, 2022), improve collaboration between business and IT (Fernando Faria & Simpson, 2013), reduce costs (Fernan Faria et al., 2013; Sunil Soares, 2011; Tyagi, 2021), develop new products (Najdanović & Tutek, 2021), improve customer service (Fernan Faria et al., 2013; Sunil Soares, 2011), increase profitability (Okunleye, 2023), improve data-driven decision-making (Fernan Faria et al., 2013), reduce data breaches (Ula et al., 2011) and mitigate ML risks (Al Wahshi et al., 2021; Sunil Soares, 2011).

To realise the benefits of IG on organisational performance, Tallon et al. (2013) divided IG consequences into two sub-categories: (1) intermediate performance effects and (2) risk mitigation. Intermediate performance effects refer to immediate or short-term goals, such as data quality improvement and cost reduction, which an organisation begins to realise before achieving its long-term goals (Abraham et al., 2019; Tallon et al., 2013). While these intermediate effects may not be entirely satisfactory, they can provide valuable indicators that the organisation and project team are making significant progress towards attaining strategic or long-term objectives, such as mitigating legal and non-compliance risks (Abraham et al., 2019; Smallwood, 2019). Risk mitigation, however, focuses on the management of information-related risks (e.g., data breaches and data loss) that may arise due to a lack of adherence to information policies and procedures (Abraham et al., 2019).

Tallon et al. (2013) suggested that “risk mitigation is a much-heralded consequence of information governance” (p. 150). Despite its promising benefits, it is widely held that quantifying the benefits of IG in terms of return on investment is challenging unless one “consider[s] the worst-case scenario of loss or misuse of corporate or agency records” (Smallwood, 2019, p. 26). The following two sections provide further discussion about the consequences of IG on a bank’s intermediate level and risk mitigation.

2.7.1 Intermediate Performance Effects

2.7.1.1 Enhance Compliance with Laws and Regulations

Enhancing compliance with laws and regulations, such as AML and PCI DSS, is a notable intermediate performance effect arising from the implementation of IG in the banking industry (Fernan Faria et al., 2013; Sunil Soares, 2011; Tyagi, 2021). Soares (2011a) and Tyagi (2021) argued that an IG framework offers effective strategies and procedures to manage information assets, which can help banks meet various information requirements, including record retention, KYC, regulatory reporting and information security and privacy. Through the enforcement of IG policies and procedures, organisations can manage their information more systematically and responsibly, thereby reducing the risk of incurring regulatory penalties or sanctions (Randhawa, 2019; Smallwood, 2019). Additionally, maintaining a robust compliance posture through IG can help profit-organisations (e.g., banks) protect their reputations and brand images in the market (AlGhamdi et al., 2020; Tyagi, 2021).

2.7.1.2 Improve Operational Efficiency

Improving operational efficiency is another important outcome of IG adoption in banks (Fernan Faria et al., 2013; Okunleye, 2023; Sunil Soares, 2011). In their quantitative study, Mikalef et al. (2018) found that the adoption of IG practices has a positive impact on organisations' dynamic and operational capabilities, which eventually leads to overall business performance. Arguably, efficient IG can help different business departments in banks reduce overheads and improve staff productivity by standardising and enabling easy access to relevant banking information (Fernan Faria et al., 2013; Randhawa, 2019).

For example, having access to the right information at the right time can increase the efficiency of compliance/AML departments in identifying, evaluating and reporting suspicious transactions more quickly (Kristian et al., 2022; Tyagi, 2021). This view was supported by Soares (2011a), who demonstrated how IG can help AML officers reduce the number of false positives through the integration and automation of the account-opening process. Likewise, previous research has shown that integrating customer data can streamline data storage processes, which leads to better utilisation of resources (Dyché & Evan, 2006).

2.7.1.3 Improve Data Quality

Improving data quality is another important benefit of IG adoption in the banking industry (Al Wahshi et al., 2022; Karkošková, 2022; Randhawa, 2019). Banking executives recognise the need for accurate, consistent and relevant data not only to comply with regulatory reporting requirements but also to make strategic decisions related to product design, customer service and risk management (Karkošková, 2022; Okunleye, 2023). Previous research showed that effective IG practices can result in high-quality data due to increased accuracy, consistence, availability and completeness of data (Abraham et al., 2019; Smallwood, 2019; Tallon, Ramirez, et al., 2013).

According to Randhawa (2019) and Karkošková (2022), banks with mature IG policies and procedures are likely to be more efficient in addressing data quality issues than those with inconsistent or weak IG practices. This is because the latter may require more time and effort to identify, correct and rectify data-related issues, which in turn hinder them from running core business activities (Bruno et al., 2017; Dadashzade, 2018). Furthermore, the literature review of this current study showed that high-quality data can reduce the costs and overheads associated with data cleansing activities, thereby enhancing overall operational efficiency and cost savings (Karkošková, 2022). Data quality, however, is largely influenced by the level of employees’ awareness and adherence to IG policies and procedures as well as the maturity of data quality management processes (Bruno et al., 2017; Karkošková, 2022; Kwan et al., 2022).

2.7.2 Risk Mitigation

In addition to its impact on a firm's performance level, IG plays a crucial role in mitigating various risks in the banking industry.

2.7.2.1 Mitigate Money Laundering Risks

Adopting effective IG practices can help banks and other financial institutions mitigate the risks of financial crimes such as ML (Al Wahshi et al., 2021; Sunil Soares, 2011). Despite the scarcity of empirical evidence in this area, the implications of IG on ML can be traced through its intermediate roles in enhancing data quality, operational efficiency, data-driven decision-making and compliance with regulatory requirements.

The integration of IG practices with the AML approach can increase banks' capacity to detect and report suspicious transactions (Al Wahshi et al., 2021; Sunil Soares, 2011). According to Soares (2011a), integrated IG can help banking professionals, such as AML and compliance officers, gain quick access to relevant information by consolidating customer-related information from disparate sources. This enables AML employees to conduct more accurate risk assessments and customer profiling, which in turn can help them implement proactive measures to enhance their transaction monitoring (Renny & Miru, 2019). Also, banks can reduce the risk of incurring regulatory fines or penalties while protecting a bank's reputation and customer confidence in the industry (Issah et al., 2022; Naheem, 2016a).

2.8 Gaps in the Literature

The review of the current IG literature showed that the role of IG in the banking industry in general, and ML in particular, has been neglected. A search of academic sources revealed very limited studies (Fernan Faria et al., 2013; Fernando Faria & Simpson, 2013; Okunleye, 2023; Soares, 2011; Tyagi, 2021) – all of which are either outdated or lack empirical evidence. Furthermore, most of these studies are focused on Western countries, neglecting the experiences of Middle Eastern countries like Oman.

Despite its unique regulatory environment and socioeconomic conditions, the Omani banking industry remains underexplored. At the time of writing this thesis, no empirical study has attempted to explore the role of IG in mitigating ML risks in the Omani banking sector. To date, much research on ML tends to focus on regulatory (Issah et al., 2022; Jaffery & Mughal, 2020; Ofoeda et al., 2022), policy (Lokanan & Nasimi, 2020) and technical (Han et al., 2020; Jullum et al., 2020; Lokanan, 2022) solutions for mitigating ML risks.

However, there is still much uncertainty around the conditions or factors that pave the way for or predict the adoption of IG practices to reduce ML risks. Given this knowledge gap, this current study, by extending Tallon's et al. (2013) model, attempts to develop a theoretical IG framework that will facilitate an understanding of the antecedents, practices and consequences of IG adoption in the ML context. To the best of the researcher's knowledge, this is the first empirical investigation that has attempted to tackle the ML problem from the perspective of IG in Oman.

Chapter 3: Research Methodology

3.1 Introduction

This chapter presents the research methodology employed in this current study to answer the research questions. It outlines the methodological choices undertaken, starting from the research approach, design, strategy and the rationale behind these choices. This chapter also discusses philosophical assumptions, including ontology and epistemology, and their roles in guiding the selection of these choices. Furthermore, the data collection and analysis methods are presented, followed by ethical considerations and limitations.

The development of the research methodology was based on the overarching aim of this study: to investigate how various IG practices can help Omani banks increase their capacity to manage their data/information in ways that enable them to mitigate the risks of ML. This chapter begins by introducing the theoretical framework underpinning this research. It then discusses the research paradigms that informed the methodological choices.

3.2 The Theoretical Framework of the Study

In this current study, Tallon et al.'s (2013) framework was chosen as a theoretical lens to explore the research problem. The rationale for selecting this framework lies on its foundation, which was derived from empirical data collected from thirty organisations across diverse sectors, including the financial sector. Additionally, this framework provides a holistic yet systematic approach to understand information governance by identifying not only the governance practices (structural, procedural and relational) necessary for managing the entire information lifecycle, but also the antecedents (enablers and inhibitors) that shape these practices, plus their impacts on organisational performance and risk management (see Figure

2). This holistic approach aligns with the objectives of this study, which aims to investigate how internal and external factors (such as regulatory compliance and technology) influence IG adoption in the Omani banking sector, and how different IG practices contribute to mitigating ML risks.

Our review of existing frameworks (see Section 2.4) reveals that the majority of them are focusing on specific domains such as data quality (Lajara & Maçada, 2013), record management (ARMA International, 2019), data security (Donaldson & Walker, 2004), and compliance (Faria et al., 2013). While these framework are valuable for addressing specific organisational needs, their narrow scope limits their applicability to broader context like the banking industry where IG practices must be integrated into multiple dimensions, including risk management, information lifecycle, strategic alignment, and regulatory compliance. For example, Faria et al.'s (2013) framework, although designed specifically for the banking industry, it focuses on compliance with regulatory requirements. It emphasises static components, including 'policies', 'technology', and 'people', without sufficiently addressing the dynamic interactions between these components or their alignment with broader strategic objectives. Additionally, Faria et al.'s framework does not provide a comprehensive view of the antecedents or conditions that enable or inhibit IG practices in the banking industry. Furthermore, it lacks a holistic perspective on the entire information lifecycle, which is critical for managing complex and evolving challenges like money laundering. These limitations in existing IG frameworks further underscores the suitability of Tallon et al.'s (2013) framework for this study.

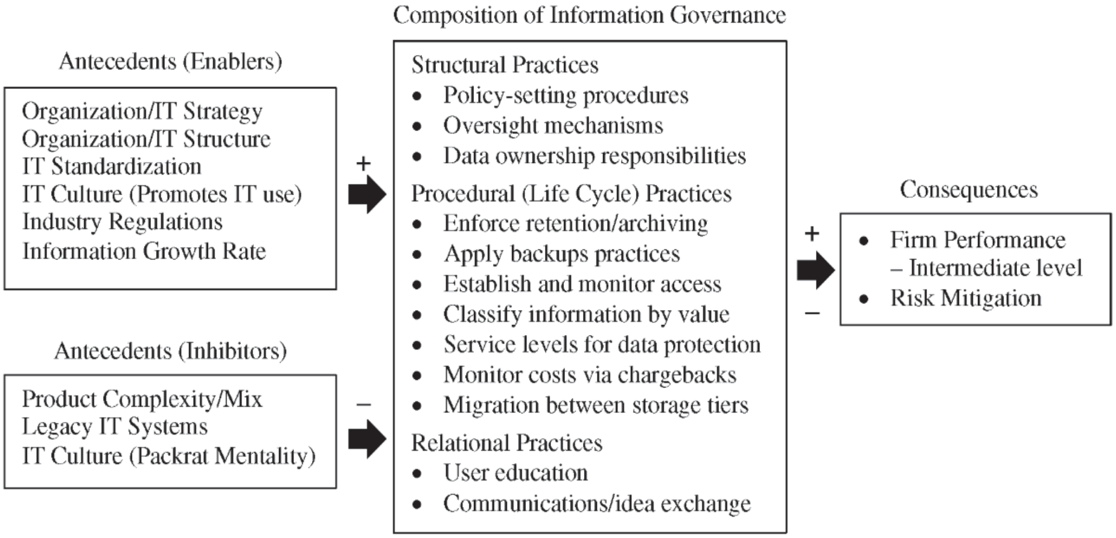

Antecedents (Enablers)
Organization/IT Strategy
Organization/IT Structure
IT Standardization
IT Culture (Promotes IT use)
Industry Regulations
Information Growth Rate
Antecedents (Inhibitors)
Product Complexity/Mix
Legacy IT Systems
IT Culture (Packrat Mentality)
+
–
Composition of Information Governance
Structural Practices
Policy-setting procedures
Oversight mechanisms
Data ownership responsibilities
Procedural (Life Cycle) Practices
Enforce retention/archiving
Apply backups practices
Establish and monitor access
Classify information by value
Service levels for data protection
Monitor costs via chargebacks
Migration between storage tiers
Relational Practices
User education
Communications/idea exchange
+
–
Consequences
Firm Performance
– Intermediate level
Risk Mitigation

Figure 2: The theoretical framework of this study (Tallon et al., 2013)

3.3 Philosophical Assumptions

Any social inquiry relies on the ability of the inquirer to obtain valid knowledge (Hughes & Sharrock, 1997; Kanellis & Papadopoulos, 2009). Valid knowledge is sought via a systematic methodological framework known as a paradigm or worldview (Creswell, 2009; Saunders et al., 2016). Guba and Lincoln (1994) defined the term ‘paradigm’ as “the basic belief systems [or worldviews] that guide the investigator, not only in choices of method but in ontologically and epistemologically fundamental ways” (p. 105). A paradigm, therefore, is the lens by which a researcher uses follow a certain methodology to address a particular social inquiry (Creswell, 2009; Krauss & Putra, 2005). However, the differences between understanding the nature of reality (ontology) and knowledge acquisition (epistemology) have led to philosophical debates: so-called ‘paradigm wars’ (Gage, 1989; Krauss & Putra, 2005; Saunders et al., 2016). These competing paradigms stem from the emergence of three important philosophical assumptions in social research: ‘positivism’, ‘interpretivism’ and ‘pragmatism’ (Bryman, 2004; Creswell, 2009; Guba & Lincoln, 1994; Saunders et al., 2016).

3.3.1 The Ontological Stance

Ontology is the foundation of any research. Defined by Richards (2003, p. 33) as "the nature of our beliefs about reality", it describes social reality or researcher's perspective (Bryman, 2004; Guba & Lincoln, 1994; Saunders et al., 2016). Researchers hold different ontological claims and assumptions (sometimes implicit) about the "nature of existence" and the reality that constitutes the social world (Bryman, 2004). Given this, it is important to ask how reality exists, what it looks like and what can be known about it (Grix, 2002; Guba & Lincoln, 1994). These ontological questions further lead to the question of whether reality is a singular verifiable truth or multiple realities that are socially constructed (Creswell, 2009; Grix, 2004). A researcher's answer to this social ontology question characterises his or her orientation and ontological position as either objectivist[3] or constructivist (Bryman, 2004; Saunders et al., 2016).

Objectivist researchers maintain that meanings exist independently of social actors (Bryman, 2004). This implies that social entities are external realities that exist as constant states; thus, they are not influenced or produced by social interactions (Bryman, 2004). The objectivist school also believes that there is a single reality created before, and hence independent of, human perceptions and that reality should not therefore be affected by the individual's own beliefs or worldviews (Gray, 2004; Saunders et al., 2016).

Conversely, 'constructivism' or 'social constructivism' is an ontological position that views the social world as being created through human interactions with and perceptions of the environment (Cohen et al., 2017). The constructivist approach opposes the idea of a pre-given

[3] Objectivism is also referred to as foundationalism or realism (see Hammond, 2013).

or pre-existing reality, maintaining that “social phenomena and their meanings are continually being accomplished by social actors” (Bryman, 2004, p. 17).

Saunders et al. (2009) emphasised the continuity of social interactions, arguing that social phenomena are in “a constant state of revision”; in other words, social entities and interpretations are continually being changed as a result of this interaction. To understand these different interpretations and realities, a constructivist researcher studies the details of phenomena by exploring the subjective meanings that motivate social actors’ consequent actions (Saunders et al., 2016).

This research embraces the ‘social constructivist’ ontological position, which emphasises how individuals and groups within organisations collectively construct knoweldge and practices through localised social interactions (Berger & Luckmann, 1968; Young & Collin, 2004). This ontological position is considered more appropriate for this social inquiry given that different groups of stakeholders carried out different activities related to IG. Likewise, different banks are exist within their different social worlds. Each bank operates within a unique social environment, shaped by its internal culture, organizational conditions, and stakeholder interactions. Social constructivism provides the lens to understand how these different social environments influence the development of Information Governance (IG) practices within banking institutions. Additionally, constructivism emphasizes individual and localized processes of meaning-making, which aligns with the study's aim to explore how different stakeholders (e.g., employees, managers, and decision-makers) shape and interpret IG practices at the organizational level. For example, the findings of this study showed how IG professionals construct their understanding of governance practices through training, communication, and collaboration. However, I also acknowledge the influence of external factors such as laws, regulations, and industry standards in shaping and constructing the IG practices.

3.3.2 The Epistemological Stance

Epistemology deals with the nature of knowledge and, in particular, the strategies, methods and validations used to acquire reliable knowledge about social reality (Bryman, 2004; Grix, 2004). In social science research, subscribing to a particular ontological belief guides a researcher to follow certain epistemological assumptions (Grix, 2002; Rehman & Alharthi, 2016). This, in turn, affects a researcher's views of "what constitutes acceptable knowledge in a field of study" (Saunders et al., 2016, p. 127). When, for example, reality is treated as a single verifiable truth, then a researcher must assume that a knower has an objectively detached or value-free position, which allows him or her to discover "how things really are and how things really work" (Guba & Lincoln, 1994, p. 108).

Conversely, a belief in socially constructed multiple realities will lead the inquirer to reject the notion that it is possible to study the social world in the same manner that the natural sciences are studied; consequently, they will interact with social actors and knowers to understand phenomena in their contexts (Bryman, 2004). Clearly, ontological assumptions affect the relationship between the known and the knower (Guba & Lincoln, 1994). From this, two contrasting epistemological positions emerged: positivism and interpretivism (Bryman, 2004; Grix, 2002).

The positivist school believes in a single reality; it assumes that reality exists "out there" independently of human beings (Creswell, 2009; Grix, 2002). It holds that social science can be directly investigated using the methods and procedures commonly applied in the natural sciences (Bryman, 2004; O'Gorman & MacIntosh, 2016). According to the positivist approach, only phenomena that can be confirmed by the human senses lead to the generation of valid knowledge (Bryman, 2004; Saunders et al., 2016). Positivist researchers hold that both the observer and the observable social reality exist in a value-free format, governed by universal laws in which knowledge can be discovered with experiments or quasi-experiments (Rehman & Alharthi, 2016; Saunders et al., 2016).

The assumption that social phenomena occur independently means that neither social actors nor researchers can affect their meaning (Creswell, 2009; Grix, 2002). In principle, this assumption is consistent with the objectivist ontological approach in which a researcher acts as an objective observer of social reality without impairing or interacting with its context (Cohen et al., 2017; Saunders et al., 2016). Positivists collect numerical data; therefore, positivism is mostly applied in quantitative research (Saunders et al., 2016).

Although the positivist paradigm has merits for studying natural phenomena or the physical sciences, it has been widely criticised by social scientists (e.g., Gage, 1989; Given, 2012; Wynn & Williams, 2012). One of the most frequent criticisms is that natural science methods, such as statistical analysis, cannot be used on their own to study social phenomena, especially human beings and their contexts, because, as Richards (2003) argued, such methods "are not designed to explore the complexities and conundrums of the immensely complicated social world that we inhabit" (p. 6). Furthermore, Bryman (2004) emphasised that social reality has a subjective meaning for individuals, so it must be interpreted from the individuals' perspectives. In general, these arguments indicate a clear rejection of the positivist approach, which can be attributed to the emergence of the interpretivist school of research (Bryman, 2004; Crotty, 1998; Saunders et al., 2016).

Interpretivist researchers, however, hold the view that reality is multiple and socially constructed (Denzin & Lincoln, 2018; Saunders et al., 2016) and influenced by human senses and experiences (Creswell, 2009; Grix, 2004). According to this assumption, multiple subjective meanings are attached to different social phenomena; therefore, it is imperative to understand and analyse phenomena from the perspectives of social actors (Krauss & Putra, 2005; Saunders et al., 2016). To grasp the interpretations of social reality, interpretivists position themselves in the phenomena being researched, and by interacting with individuals, the researcher obtains their worldviews and concepts (Bryman, 2004; Creswell, 2009). This research philosophy is aligned with the constructivist ontological position (Saunders et al., 2016).

To engage with participants, interpretivist researchers collect data by interviewing or observing the participants to gather qualitative data over a prolonged period, as in ethnography (Creswell, 2009; Rehman & Alharthi, 2016). Qualitative researchers adopt an inductive approach to data analysis because they "tend to see theory as deriving from data collection and not as the driving force of research" (Grix, 2004, p. 108). However, the interpretivist paradigm has been criticised for being "soft", unable to develop theories that can be generalised to broader populations and for lacking objectivity due to a researcher's involvement with the participants (Grix, 2004). However, Richards (2003) argued that qualitative research is not "soft … it demands rigour, precision, systematicity and careful attention to detail" (p. 6).

This current research adopted an interpretivist epistemological stance motivated by the ontological approach of constructivism, with which interpretivism is often interconnected

(Creswell, 2009). The positivist position was rejected in this study since this inquiry did not seek to verify hypotheses through an objective observation or to find a cause-effect relationship (Guba & Lincoln, 1994). Instead, this present study aimed to understand and interpret multiple subjective meanings of reality from the perspectives of different individuals (i.e., bankers and regulators). In this research, therefore, the experiences of people and their interpretations were essential for explaining the phenomenon on which the subjectivist paradigm was focused (Saunders et al., 2016). Unlike objectivism, the interpretivist position, by its nature, allows a researcher to obtain rich insights into human behaviours and interactions (Guba & Lincoln, 1994).

3.4 Research Approaches: Inductive and Deductive Reasoning

It is clear from the preceding discussion in section 3.3 that a research philosophy influences how social research is conducted (Grix, 2002; Hughes & Sharrock, 1997), which ultimately informs the choice of the research approach and the methods for the collection and analysis of the data (Saunders et al., 2016). In the social sciences, there are two contrasting research approaches to answering a research question: deductive and inductive (Azungah, 2018; Creswell, 2007; O'Reilly, 2012; Saunders et al., 2016). These approaches stem from different philosophical worldviews that differ in their ontology (Slevitch, 2011). While deductive researchers believe in "a single reality that can be measured reliably and validly using scientific principles", inductive researchers believe in "multiple constructed realities that generate different meanings for different individuals, and whose interpretations depend on the researcher's lens" (Onwuegbuzie & Leech, 2005, p. 270). Following Bryman (2004), inductive reasoning in this study is linked to qualitative research, whereas deductive reasoning is linked to quantitative research. A further discussion of the differences between the inductive and deductive approaches is provided below.

The deductive approach aims to discover causal relationships between theory and research through the application of natural scientific methods so that it emphasises the testing of theory to evaluate whether it can be generalised (Azungah, 2018; Bryman, 2004). Consequently, the deductive approach is more prevalent in scientific research, and it is particularly associated with the positivist view that social reality is an external object (Collis, 2014). Blaikie (2010) outlined a series of stages that an inquirer must follow, using a “top-down” approach when adopting deduction (see Figure 4).

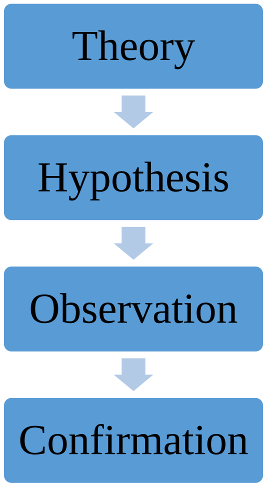


Figure 4: Stages of the deductive approach

First, a comprehensive review of the relevant literature is performed so that an established theory for a social inquiry under study can be established. Some testable hypotheses are then derived from the chosen theory. Following this, the observation phase involves examining hypotheses and comparing them with existing theories by collecting appropriate quantitative data and using testing procedures. In the final step, the hypotheses are either confirmed or rejected.

By contrast, the inductive approach, as illustrated in Figure 5, uses a “bottom-up” approach. It first collects relevant data within participants’ natural settings (fieldwork) and subsequently generates only theory (Bryman, 2004; Creswell & Poth, 2017). As inductive research aims to acquire a better understanding of “what is going on” in a social phenomenon or context (Saunders et al., 2016), it emphasises individuals’ interpretations and experiences, which are usually transcribed into words rather than being numerically quantified (Bryman, 2004).

By definition, this type of research approach fits with the epistemological orientation of interpretivism, which rejects the idea that the social world can be studied as a natural object (Bryman, 2004; Slevitch, 2011). Due to its interpretivist nature, inductive reasoning is usually used in qualitative studies where a detailed description and explanation can be obtained by employing a variety of data collection methods, such as in case studies (Creswell & Poth, 2017; Guba & Lincoln, 1994). Indeed, proponents of induction criticise the rigid methodology of deduction for its tendency to rely on a single source of data collection thus providing an inadequate explanation of social phenomena (Saunders et al., 2016). As with the deductive approach, Blaikie (2010) suggested a sequence of steps for conducting inductive research, as described below.

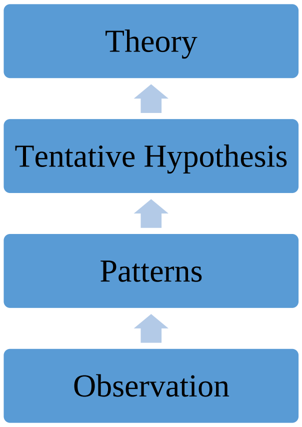


Figure 5: Stages of the inductive approach

The process of the inductive approach always starts with a specific observation of a social or human problem (Blaikie, 2010; Creswell & Poth, 2017), after which general research questions are formulated from related literature and a researcher's experience (Matthews, 2010; Strauss & Corbin, 2007). Next, different patterns and theoretical concepts are identified from observed data. Finally, general theories or conclusions are generated and the study's findings are explained (Blaikie, 2010). Table 5 summarises the main similarities and differences between the deductive and inductive approaches.

Feature	**Deductive**	**Inductive**
Direction	Top-down	Bottom-up
Role of theory	Theory verification	Theory-building
Ontological beliefs	Objectivism	Subjectivism/constructivism
Epistemological beliefs	Positivism	Interpretivism
Research type	Explanatory research	Exploratory or descriptive research
Research strategies	Experimental research and non-experimental research, such as a survey	Case study, grounded theory, ethnography, phenomenology and narrative research

Data collection methods	Closed-ended questionnaires	Interviews, observation, focus groups and document analysis

Table 5: Comparison of inductive and deductive approaches (adapted from Bryman, 2004; Creswell, 2009)

3.4.1 Rationale for Adopting the Inductive Approach

This present research began with the observation that there is a dearth of studies investigating the role of the IG programme in the Omani banking industry, particularly in the context of ML. Given this knowledge gap, few hypotheses or assumptions were made concerning the phenomenon of interest at the beginning of the research process. Therefore, the inductive approach is best suited to this inquiry to build such knowledge.

Trochim (2006) argued that a chosen approach should not be based on a researcher's personal preferences; instead, it should be driven by three important factors: the study's nature, purpose and research questions. Since this current study was exploratory, to obtain an in-depth understanding of the research problem, it relied on multiple observations and individuals' experiences rather than on a single reality (Creswell, 2007).

3.5 Research Design

Research design is an important element of a successful research project (Bryman, 2004). It embraces "plans and the procedures for research that span the decisions from broad assumptions to detailed methods of data collection and analysis" (Creswell, 2009, p. 22). The choice of a quantitative, qualitative or mixed methodology depends on the philosophical assumptions, the role of theory, the nature of the research problem, the enquiry strategies employed and a researcher's experience (Bryman, 2004; Saunders et al., 2016). The following subsections provide a brief overview of qualitative research, followed by justification for its use in this study.

3.5.1 Qualitative Research

Qualitative research is interpretive by nature and therefore it is generally associated with interpretivist epistemology and constructivist ontology (Creswell & Poth, 2017; Denzin & Lincoln, 2018; Guba & Lincoln, 1994). According to this research paradigm, social reality is constructed and assigned multiple subjective meanings based on the individual perspectives of the different people who experience the social or research problem under study (Antwi & Kasim, 2015; Denzin & Lincoln, 2018). According to Antwi and Kasim (2015), a qualitative design is best employed when scant information is available about a specific topic or phenomenon and when the research topic is inadequately covered by extant literature or theories.

Qualitative researchers are often referred to as “naturalistic” (Saunders et al., 2016) because they attempt to gain access to the inner reality of the participants (Bryman, 2004) through direct observations of the participants’ behaviours, actions, beliefs and attitudes within their natural setting (Creswell & Poth, 2017). With this in mind, a detailed description or theory-building is usually the outcome of a qualitative inquiry, and this approach emphasises how the findings of an inquiry are inductively produced and analysed from the empirical data (Saldaña, 2011).

Although qualitative researchers are less concerned about testing the laws of human behaviour through measurable data (Saldaña, 2011), they employ interactive, human-oriented data collection methods that are sensitive to participants and contexts (Neuman, 2014). Broadly speaking, qualitative research data are typically gathered by researchers themselves via in-depth interviews, observation of participants and focus-group discussions (Denzin & Lincoln, 2018). Therefore, in a qualitative study, a researcher is considered the “key instrument” for data collection and analysis (Creswell & Poth, 2017). Various strategies are associated with qualitative research because they are grounded in similar philosophical positions and share common characteristics (Antwi & Kasim, 2015; Slevitch, 2011). Examples of such strategies are case studies, narrative research, grounded theory, ethnography and action research (Creswell & Poth, 2017).

3.5.2 Rationale for Selecting Qualitative Research

For this current study, a review of the IG literature revealed a range of methodological approaches employed (see Table 6). Since there is a lack of research on the role of IG programmes in the mitigation of ML risks, a qualitative design was selected for this study. Qualitative methods are generally employed to answer research questions that centre on the perspectives and experiences of the participants who usually attach different meanings to the phenomena of interest (Creswell & Poth, 2017). Such meanings cannot be easily measured or calculated as in quantitative research (Guba & Lincoln, 1994). Given the exploratory nature of this study, the established research questions cannot be answered through numerical data; instead, they require gathering background information and understanding the participants' views on the topic under investigation.

Theme	Approach/Methodology/Strategy	Reference
Developing an IG theory/framework through the theoretical lens of IT governance	Inductive/qualitative research, grounded theory, semi-structured interviews	(Tallon, Ramirez, et al., 2013)
Discussing barriers that influence the adoption of an IG programme in an organisation	Inductive/qualitative research, such as a case study	(Hagmann, 2013)

Bridging the gap between business and IT in the banking industry from the perspective of IG	Inductive/qualitative research, interviews, case studies and document analyses	(Fernando Faria & Simpson, 2013)
Developing an Information Governance Framework (IGF) for banks	Inductive/qualitative research, interviews, multiple-case studies and document analyses	(Fernan Faria et al., 2013)
Investigating the role of IG in ensuring value, quality, and compliance of information	Inductive/qualitative research, case study, semi-structured interview, document analysis and observation	(Lajara & Maçada, 2013)
Identification of factors affecting the adoption of information governance in the public sector	Inductive/ qualitative research, case study, survey, interviews, observation and document analyses	(Abdul Halim et al., 2018)
Exploring the critical success factors for DG in a selected bank	Inductive/qualitative research, grounded theory, semi-structured interviews and observations	(Alhassan et al., 2019)

Table 6: A summary of methodologies adopted in IG Studies

3.6 Research Strategy

Saunders et al. (2016) stated that a research strategy is “a plan of how a researcher will go about answering her or his research question” (p. 177). Typically, there are five main strategies for qualitative inquiry: (a) case study, (b) grounded theory, (c) phenomenology, (d) ethnography and (e) narrative research (Creswell & Poth, 2017). In this current study, a qualitative case study was employed as an overarching methodology for approaching the research questions.

3.6.1 Case Study Research

The case study approach has become increasingly popular in the information systems field due to its ability to explore the phenomenon of interest within its natural setting or context (Baxter & Jack, 2008; Benbasat et al., 1987; Walsham, 1995). To date, there is no widely accepted definition for the term “case study”, albeit many researchers (e.g., Denzin & Lincoln, 2018; Eisenhardt, 1989; Merriam, 1998; Stake, 1995; Yin, 2014) have attempted to establish frameworks and guidelines to clarify its meanings and connotations. The purpose of a case study is to draw upon seminal methodologists, such as Yin (2014), Stake (1995) and Merriam (1998).

According to Yin (2014), the term “case study” is defined as “an empirical inquiry that investigates a contemporary phenomenon (the ‘case’) in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident” (p. 16). This definition is recognised as more comprehensive because it highlights two key aspects of case study research: (1) the scope of a case study and (2) the characteristics of a case study.

Stake (1995) emphasised the specificity and boundedness of the case and, therefore, he defined it as a “bounded system” that is “a specific, a complex, [and] functioning thing” (p. 2). Similarly, Merriam (1998) described a case study as “an in-depth description and analysis of a bounded system” (p. 39). Taken together, the case study approach is considered especially useful for answering “how” and “why” questions, and it is well suited for exploratory research where in-depth understanding and analysis of a complex phenomenon is required (Benbasat et al., 1987; Merriam, 1998; Yin, 2014).

While Yin, Stake and Merriam agree on the fundamental elements of the case study approach, they differ in their epistemological orientations or stances (Brown, 2008; Yazan, 2015). In his textbook, Yin reveals a tendency towards the positivist stance, emphasising the objectivity, validity and generalisability of the case study. For example, he advocates for a structured approach to case study research, including developing a clear protocol for data collection and analysis to ensure reliable and valid findings.

In contrast, Stake positioned his case study approach towards constructivism, arguing that “there are multiple perspectives or views of the case that need to be represented, but there is no way to establish, beyond contention, the best view” (p. 108). According to Stake (1995), “knowledge is constructed rather than discovered” (p. 99); therefore, he maintains that seeking a single interpretation of a case is impossible due to the inherent subjectivity of both researchers and participants.

Like Stake (1995), Merriam’s (1998) epistemological stance seems to be aligned with the constructivism paradigm, as evident in her statement: “Reality is not an objective entity; rather, there are multiple interpretations of reality” (p. 22). Given the philosophical stance of this study, it is clear that Stake’s and Merriam’s approaches to a case study are more applicable to this present study. However, Yin’s textbooks were consulted for valuable insights into designing and implementing the case study.

3.6.1.2 Rationale for Selecting the Case Study Strategy

Given the current study is inductive, the case study design is particularly well suited to this inquiry because it enables a researcher to “generate theories from practice” (Benbasat et al., 1987, p. 370) by engaging in direct conversations with practitioners who experience a phenomenon in its natural context (Stake, 1995). Due to limited theoretical knowledge about IG practices in the Omani banking sector, the phenomenon under investigation cannot be investigated outside of its real-life context without capturing the experiences of key actors (i.e., bankers). Furthermore, using a case study method enabled a research question to be answered with a full exploration of the complexities of a phenomenon by gathering a range of evidence from multiple data sources – sometimes referred to as 'data triangulation' (Farquhar, 2012; Stake, 1995).

The type of research question posed	Case study design is the preferred research methodology when a "how" and "why" question is asked.	The principal research question of the current study is: *"How can information governance practices help Omani banks in increasing their capacities in managing AML-related data/information in a way that enable them to mitigate ML risks"*
The extent of control over behavioural events	Case study design is ideally suited when the relevant behaviours cannot be controlled or manipulated.	The present research seeks to investigate the phenomenon of IG from the perspective of its participants (i.e., banks) without controlling their interactions with the context or the meanings they attach to the case under study.
The degree of focus on a contemporary case	Case study design is the preferable method when investigating contemporary events.	To obtain a thorough understanding of "current" IG practices and frameworks adopted by banks in Oman, this study should be conducted within the real-life context of the Omani banks.

Table 7: Factors influencing the adoption of the case study design (adapted from Yin, 2014)

3.6.2 The Case Study Design

3.6.2.1 Defining the Case: Unit of Analysis

Defining a case (or unit of analysis) is the first critical step in designing successful case study research (Thomas, 2016; Yin, 2014). According to Miles and Huberman (1994), a case can be defined as "a phenomenon of some sort occurring in a bounded context" (p. 25). A case can be anything, such as a person, organisation, project, programme, system, practice, event, process or even a country (Merriam, 1998; Yin, 2014). However, Stake (1995) argued that not everything qualifies as a case because some cases are too broad and "lack the specificity and boundedness" (p. 2). Therefore, it is argued that a well-defined case can directly affect the research design since it informs the subsequent phases of data collection and analysis (Baxter & Jack, 2008; Martinsuo & Huemann, 2021; Stake, 1995). However, determining a unit of analysis (e.g., a case) is challenging; it requires careful analysis and consideration of multiple factors, including the research questions, theoretical framework, level of analysis and context (Martinsuo & Huemann, 2021).

To overcome this challenge, several approaches have been proposed by different scholars (e.g., Miles & Huberman, 1994; Stake, 1995; Thomas, 2016). Miles and Huberman (1994) suggested that case study researchers should start delineating the case by asking themselves whether they intend to "analyse", for example, an individual, a programme, process or differences between organisations. Likewise, Yin (2014) recommended seeking an opinion from a colleague by explaining why a selected case (or unit of analysis) is the best option for addressing the research question.

Thomas (2011) developed a case study typology to help a case researcher systematically define the subject and object of the study. According to the same author, the subject that represents a case or phenomenon of a study can be selected based on three possible routes or types: the local knowledge case, (2) key case, and (3) outlier case. First, the local knowledge case can be followed if a chosen case is situated within a researcher's personal experience and knowledge, such as one's workplace. Second, the subject (case) may become the centre of a study when a researcher is more interested in learning about the case itself. Third, the case may be selected due to its different or outlier status. For this research, the case (subject) is selected based on a key case given a researcher's intrinsic interest in understanding the complexities and dynamics of IG practices (e.g., within the Omani banking sector). This interest is driven by the fact that a case has received significant attention from academics and practitioners, making it valuable to be explored and analysed from multiple perspectives.

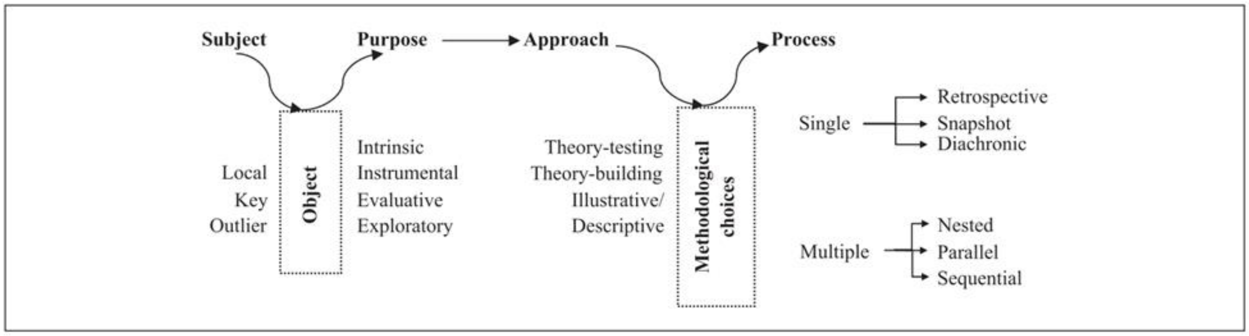


Table 8: Typology of a case study (Thomas, 2011, p. 518)

3.6.2.2 Determining the Type of Case Study Design

After a case is defined, a researcher must decide whether to adopt a single- or multiple-case study (Stake, 2005; Yin, 2018). According to Baxter and Jack (2008), choosing a specific type of case study design should be guided by a study's overall purpose (i.e., exploratory, explanatory or descriptive). Yin (2018) distinguished between four types of case study designs: (1) holistic single-case study, (2) embedded single-case study, (3) holistic multiple-case study and (4) embedded multiple-case study (see Figure 3). Similarly, Stake (2005) identified three types of case study design: intrinsic, instrumental and collective. Further discussion of these types is followed in this section.

A single-case study design focuses on a single case (Meyer, 2001; Yin, 2018). This type of design is analogous to a single experiment (Yin, 2018). According to Yin (2018), single-case studies are suitable when "the case represents (a) a critical test of existing theory, (b) an extreme or unusual circumstance, or (c) a common case, or where the case serves a (d) revelatory or (e) longitudinal purpose" (p. 90). Stake (1995) suggested that a single-case study can be adopted if a researcher has a genuine interest in understanding the unique characteristics and complexities of a particular case.

As indicated above, there are two variants of the single-case study design: holistic and embedded. While a holistic design involves a single unit of analysis, an embedded design involves multiple units of analysis within the same case (Yin, 2018). A holistic design might be adopted when "no logical subunits can be identified or when the relevant theory underlying the case study is mainly holistic" (Yin, 2018, p. 88). In contrast, an embedded single-case study design might be used when a case study aims to gain a deeper understanding of various components or subunits within a single case (Yin, 2018). Although a single-case study can allow a researcher to delve into the complexities of a case, it suffers from selection bias and a lack of transferability (Curini et al., 2020; Eisenhardt, 1989).

In contrast, a multiple (or collective) case study design involves studying two or more cases from different contexts to understand their similarities and differences (Stake, 2005). This approach is akin to multiple experiments and has two variants: holistic and embedded (see Figure 3). Research has shown that multiple-case studies are particularly valuable when a researcher aims to develop a theory (Eisenhardt, 1989) or understand how a particular phenomenon operates or varies across different contexts (Baxter & Jack, 2008; Stake, 2005).

Eisenhardt (1989) argued that the evidence from a multiple-case study is more compelling and reliable than a single-case study since it allows the data to be compared within and across cases. Meyer (2001) suggested that adopting a multiple-case study can enhance the generalizability of findings and reduce selection biases. However, evidence has shown that conducting multiple-case studies is expensive and time consuming, requiring extensive resources and efforts that might go beyond a researcher's capabilities (Yin, 2014).

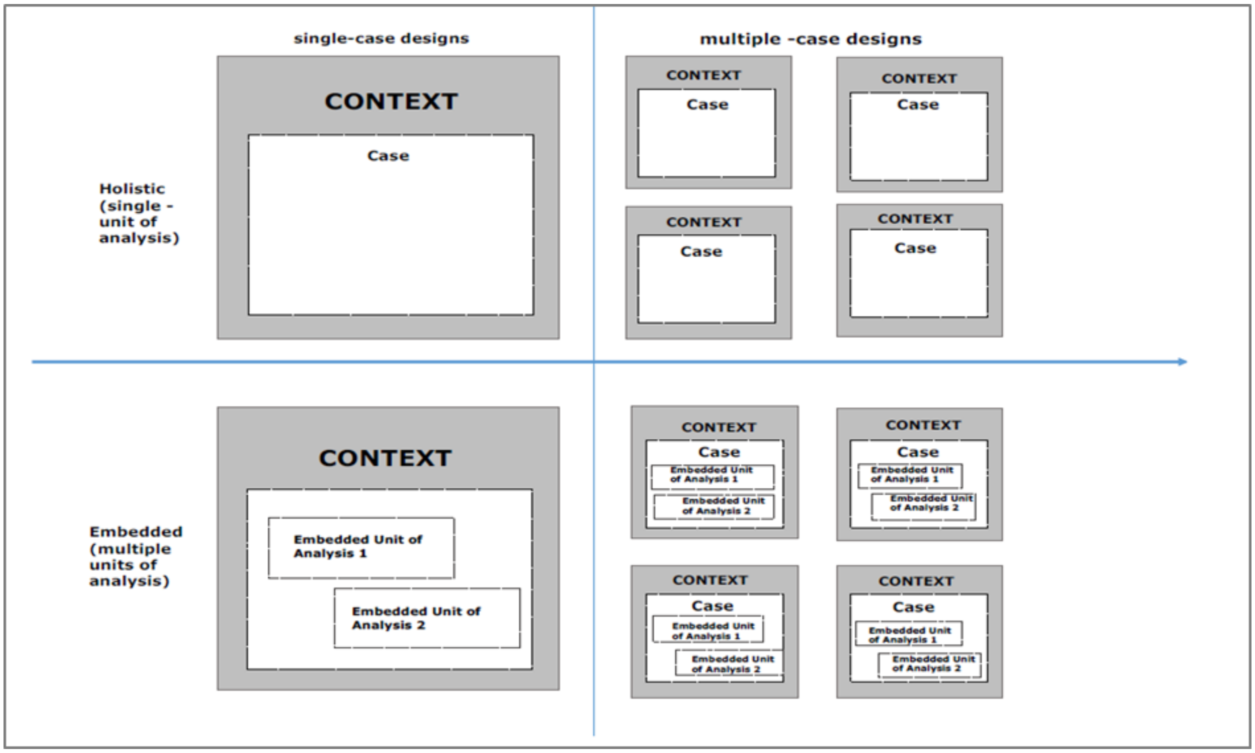

single-case designs
multiple -case designs
Holistic (single - unit of analysis)
Embedded (multiple units of analysis)
CONTEXT
Case
Embedded Unit of Analysis 1
Embedded Unit of Analysis 2

Figure 3: Basic types of case study designs (Yin, 2018)

3.6.2.2.1 Rationale for Adopting a Multiple-Case Study Design

This present study adopted a holistic multiple-case study, as it sought to gain a comprehensive understanding of a phenomenon across different contexts but with a single unit and level of analysis. This study aimed to understand the similarities and differences across different Omani banks in relation to their antecedents, IG practices and consequences. Thus, the intention was not to analyse specific groups or subunits but rather to explore how different contextual factors affect the implementation of IG practices across different banks. Accordingly, the data collected from this study were analysed at the bank level to facilitate a cross-case analysis. This level of analysis allowed the researcher to obtain better insights into the relationships between themes and constructs. Lastly, adopting a multiple-case study approach improved this study's external validity by facilitating data triangulation.

3.6.2.3 Selection of Cases

Selecting cases is another crucial step that requires careful and strategic decisions before collecting case study data (Seawnght & Gerring, 2008; Shakir, 2002; Stake, 1995; Yin, 2014). Arguably, the strategic selection of cases can illuminate the phenomenon of the study by generating rich information that may extend, modify, build or even challenge existing theories (Curini et al., 2020; Eisenhardt, 1989, 2007; Stake, 1995). As such, case study researchers are advised to conduct an early assessment of potential cases to validate whether the chosen cases have the necessary information to address the research questions at hand (Mills et al., 2012). They are also encouraged to document the steps and procedures followed during the case selection process to enhance the validity of a research design (Mills et al., 2012).

In a qualitative case study, cases are often selected purposefully (or strategically) rather than randomly (Emmel, 2013; Mills et al., 2012). In his seminal work, Eisenhardt (1989) criticised the idea of the sampling selection of cases, arguing that "random selection is neither necessary nor even preferable" (p. 537). In support of this view, Stake (1995) stated that "a sample of one or a sample of just a few is unlikely to be a strong representation of others (p. 4). Unlike quantitative sampling, which aims to improve the representativeness and generalizability of findings, qualitative sampling selects cases based on their potential to provide information-rich insights (Curtis et al., 2000; Meyer, 2001). Therefore, it is crucial that a case study researcher select cases that can offer the "maximum opportunity" to learn about the phenomenon being studied (Stake, 1995).

The literature suggests that selecting cases should be driven by theoretical, empirical and practical considerations (Kahwati & Kane, 2020; Stake, 2005b). According to Stake (2005), there are three main criteria for selecting cases in multiple-case studies: (1) relevance to the quintain (or the phenomenon of interest), (2) diversity of cases and (3) opportunities to learn about complexities and contexts. However, theoretical relevance is regarded as the most important criterion for case selection (Kahwati & Kane, 2020; Stake, 2005). In exploratory research questions, for example, cases that contribute to developing theories or "extending the relationship of the constructs" should only be selected (Eisenhardt, 2007, p. 27). This idea is like the theoretical sampling of grounded theory, which was introduced by Glaser and Strauss (1967).

Additionally, case selection should balance diversity and homogeneity (Stake, 2005; Yin, 2014). While diverse cases can help a researcher uncover different dimensions of the phenomenon, the cases must be similar in some way to ensure meaningful comparisons (Kahwati & Kane, 2020). To ensure case diversity, Yin (2014) proposed a replication logic by which cases are selected because they are expected to produce similar results (literal replication) or contrasting results (theoretical replication). In some cases, however, it might be challenging to anticipate the outcome of the case beforehand due to the unavailability of outcome data; therefore, conducting a pilot study is necessary to gather preliminary results for each potential case (Kahwati & Kane, 2020). In response to this challenge, Kahwati and Kane (2020) suggested reviewing the relevant literature to identify the conditions under which a particular phenomenon may or may not be found. Lastly and more importantly, the researcher should take into consideration other practical issues related to the accessibility of data, resource availability, funding, time constraints and geographical location (Kahwati & Kane, 2020; Yin, 2014).

Given the above discussion, the cases for this study were chosen purposively using a set of inclusion and exclusion criteria (discussed later). Following the advice of Stake (2005) and Kahwati and Kane (2020), three key criteria were used for selecting case studies: theoretical relevance, diversity and accessibility. Purposive selection of cases was more appropriate for this multiple-case study research because it allowed the researcher to balance breadth (i.e., number of cases) and depth (Stake, 2005), ensuring a comprehensive understanding of various IG issues across the Omani banking sector. It also allowed the researcher to achieve a diversity of cases, which facilitated comparative analysis across different banks (Stake, 2005). Figure 4 summarises the steps followed to select the cases for this current study.

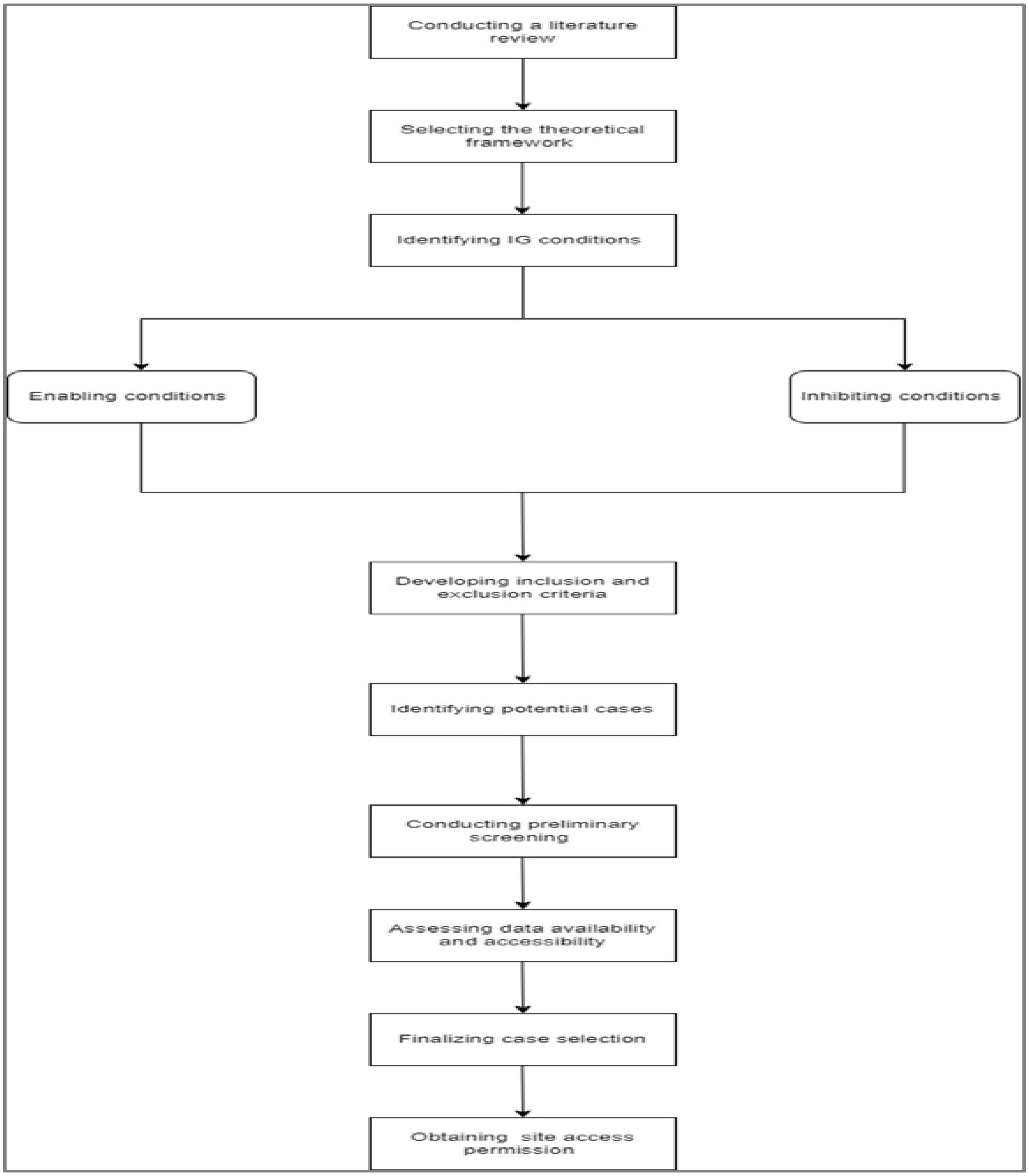

Conducting a literature review
Selecting the theoretical framework
Identifying IG conditions
Enabling conditions
Inhibiting conditions
Developing inclusion and exclusion criteria
Identifying potential cases
Conducting preliminary screening
Assessing data availability and accessibility
Finalizing case selection
Obtaining site access permission

Figure 4: A step-by-step process for selecting cases

The first step in selecting cases for this study involved a thorough review of the existing literature on IG. This was a critical step not only in identifying gaps in the existing literature but also in selecting the most relevant theoretical framework for the given study (Step 2). As recommended by Eisenhardt (1989) and Stake (2005), the cases were selected based on theoretical interest rather than personal preference or convenience. The literature review and theoretical framework helped identify the key conditions that enable or inhibit the adoption of IG practices in organisations.

By drawing on the theoretical framework of this study, it was possible to anticipate which banks (or cases) were likelier to have advanced or basic IG practices. For instance, it was expected that banks with large customer bases and massive transactional data would have more advanced IG practices than those with small data or limited resources (e.g., legacy IT systems and insufficient funding). Therefore, it was decided to include banks with different capabilities and sizes to explore how different contextual factors affect the implementation of IG practices in different Omani banks. Further details about the inclusion and exclusion criteria are presented in Table 9.

Criteria	**Inclusion**	**Exclusion**
Geographic location	Banks operating in Oman (i.e., having a physical presence within the country). These banks should also be licenced by the CBO	Banks operating outside of Oman
Regulatory environment	Banks that are subject to Omani banking regulations and other laws imposed by the country where the bank operates	Banks that subject to non-Omani banking laws and regulations
Bank size	All sizes (small, medium and large)	Not applicable, as all sizes are included
Type of Bank	Banks from different categories (i.e., Regulatory, local, Islamic, specialised and International) were included	- Money exchange companies - Finance and leasing companies - Purely international banks with no operations in Oman

Availability of Data	Willingness to provide relevant data for research	- Unwillingness or legal constraints in providing necessary data

Table 9: Inclusion and exclusion criteria for case selection

Out of 20 banks, only 10 agreed to participate in this study. However, one Islamic bank announced a merger with another local bank, so it was excluded from the list of potential cases. As a result, nine cases were considered for this study. To ensure these cases matched the selection criteria mentioned above, a preliminary screening was conducted by reviewing each bank's publicly available information including annual reports, organisational structure and CG records; this was followed by direct communication with the banks to validate and collect additional information related to the phenomenon under investigation.

In some cases, the researcher conducted pilot/ informal interviews with key stakeholders from the compliance and IT departments through his professional networks. This enabled the researcher to gain initial insights into the selected banks, thus ensuring that they had the necessary information to help address the established research questions. Table 10 summarises the selected banks (cases) for this study. For confidentiality reasons, the names of the banks were anonymised using pseudonym codes.

Case No.	Bank Code	Bank location	Type of Bank	Number of Branches	Number of Customers	Total Assets (USD)
1	Bank 1	Oman	Local	173	2.4 million	86,1 million
2	Bank 2	Oman	Local	66	525,000	33.2 billion
3	Bank 3	Oman	Local	65	N/A	23.3 billion
4	Bank 4	Oman	Local	75	N/A	12.0 billion
5	Bank 5	Oman	International	31	N/A	16.53 billion

6	Bank 6	Oman	Islamic	19	207,931	4.05 billion
7	Bank 7	Oman	International	900	25 million	328.6 billion
8	Bank 8	Oman	Specialised	12	N/A	553.2 billion
9	Bank 9	Oman	Regulatory	3	N/A	17.91 billion

Table 10: List of selected cases for this research

3.6.2.4 Boundaries of the Cases

A common pitfall when designing a case study is trying to answer research questions that are too broad or include an unrealistic number of objectives (Baxter & Jack, 2008). Another pitfall, especially in a multiple-case study design, is selecting cases without clear inclusion and exclusion criteria (Shakir, 2002). In so doing, the research would become more generic and unmanageable, which could lead to inconsistent and irrelevant findings (Baxter & Jack, 2008).

To avoid these issues, Stake (2005) and Yin (2014) suggested placing some limits or boundaries on the cases so that they could remain within a reasonable scope of length and cost. Additionally, binding the cases can help determine the scope of data collection by excluding those that fall outside the context and boundaries of a study thereby ensuring more focused and relevant information that aligns with research questions (Yin, 2018). There are many ways to bind cases, including time and activity (Stake, 2005), place (Creswell & Poth, 2017) or definition and context (Miles & Huberman, 1994).

For this current study, the cases were bound by place, context and activity. The decision to select these binding criteria was because this study focused in exploring IG capacities and practices (activity) within the natural setting of the banking sector (context), more specifically in Oman (place). This decision was also informed by relevant IG studies in the banking sector (e.g., Faria et al., 2013; Okunleye, 2023). For example, in their multiple-case study, Faria et al. (2013)

selected three countries–namely the United States, Brazil and China—as the places for binding cases. In the context of this study, binding cases to a specific place, context and activity allowed the researcher to avoid unnecessary trials and errors while focusing on collecting data relevant directly to the research questions.

3.7 The Research Context

The Omani banking sector plays a major role in preserving financial stability and growth in the country. The sector is regulated by the CBO, which has overall accountability to ensure that banks comply with both national and international regulations. The banking institutional framework in Oman combines seven local banks, nine foreign banks, two specialised banks and two full-fledged locally incorporated Islamic banks with a total network of 559 branches (see Table 11).

Broadly, the sector is dominated by conventional banks, which hold 92% of the financial sector's total assets (Central Bank of Oman, 2019). The top three leading banks (i.e., Bank Muscat, Bank Dhofar and the National Bank of Oman) hold 36.3% of the sector's total assets (see Central Bank of Oman, 2019). Oman's banking industry remained resilient (IMF, 2010) and supportive of national initiatives and economic diversification by offering the necessary credits (Al Ghassani et al., 2017). To ensure long-term resilience, the government enacted a new banking law in December 2000 (Royal Decree 114/2000)[4], which clearly highlights the regulations and obligations of banking institutions. This law, in tandem with other regulatory practices and policies implemented by the CBO, including risk-based supervision, has facilitated the development of a stable banking system in recent years (Central Bank of Oman, 2019).

[4] See https://cbo.gov.om/Pages/BankingLaw.aspx.

With the risk-based approach in mind, the CBO has issued detailed procedures for off-site examinations of banks' AML/CFT compliance. These procedures allow the supervisory team of the CBO to better understand and assess the risks of ML in banks, which accordingly helps them prioritise resources to enhance Oman's AML regime (Central Bank of Oman, 2019).

It is worth noting that Islamic banks, although they operate under the same regulatory frameworks, are additionally governed by Sharia principles that distinguish them in terms of operations and financial offerings. Islamic banks, for example, prohibit the charging or payment of interest (riba), and instead emphasize risk-sharing, ethical investments, and asset-backed financing. These principles have led to the development of specific products such as mudarabah (profit-sharing), murabaha (cost-plus financing), and ijara (leasing).

The dual compliance with CBO regulations and Sharia law necessitates unique governance practices within Islamic banks, particularly with respect to transparency and ethical oversight. These banks must ensure strict adherence to Sharia principles while maintaining robust mechanisms for compliance monitoring and data validation. As a result, Islamic banks contribute to the diversification and inclusivity of Oman's banking sector, offering culturally aligned alternatives to conventional banking products and services. This governance framework not only reflects the cultural and religious values of the population, but also ensure effective compliance with both national and international regulatory requirements.

Bank Category	Number of Banks	Number of Branches
Local banks	7	420
Foreign banks	9	31
Specialised banks	2	26
Islamic banks	2	82
Total	**20**	**559**

Table 11: Overview of Oman's banking industry (Central Bank of Oman, 2024)

3.8 The Study Sample

The participants in this study were meticulously chosen (Ritchie et al., 2003) using a purposive sampling strategy (Patton, 2014). This strategy aims to ensure that the selected participants or stakeholders have the necessary knowledge and experience about the phenomenon under investigation, which enable them to provide rich, relevant, and diverse insights to address the research questions (Devers & Frankel, 2000; Patton, 2014). The rationale for adopting a purposive sampling technique in this study lies in *a priori* understanding that certain individuals within the Omani banking sector hold pivotal roles and possesses unique expertise on information governance and money laundering domains, and therefore likelier to offer practical insights into the research questions (Mason, 2002).

To facilitate the selection of the study sample, inclusion and exclusion criteria were developed (see Table 12). The selection of these criteria was inspired by the principal aims of this study, the researcher's experience, and the careful examination of key IG studies (e.g., Faria et al., 2013; Tallon et al., 2013).

Selection Criteria	Inclusion	Exclusion
Geographical location	Oman	Any other countries
Nationality	Omani	Non-Omani
Bank setting/type of work	● A participant must work in one of the nine banks chosen for this study as a 'full-time' employee. ● A participant must work at the head office of the bank.	● Part-time employees; non-selected banks ● Work at bank branches
Years of experience in the banking sector	Minimum of five years	Less than five years
Language	English or Arabic	Any other languages
Gender	Males and Females	N/A
Academic and education qualification	Bachelor's degree and above	Below bachelor degree
Key business departments/organisation structure	C-level executives, AML/compliance department, IG/IT department, risk management, information security, risk management, legal	Any other departments
Participant job titles	Chief information officer, Chief technology officer, IG/IT executives, AML/compliance officers, risk managers, and quality analysts	Any other designations

Table 12: Inclusion and exclusion criteria for the selection of participants

Participants for this research were Omani practitioners working in one of the nine banks selected as case studies. The reason for only including citizens of Omani nationality in the study sample was to understand the central themes of interest from the perspective of local experiences. This study was also limited to full-time staff who work at a bank's headquarters because, based on the researcher's experience, those people are likelier to be involved in policy-setting and ML matters than those at branches or part-time employees. To ensure balance, both males and females were equally considered during the process of sample selection (Patton, 2002). However, non-English or Arabic speakers were excluded to avoid problems associated with misinterpretation and translation, which could affect the validity of the results.

Given the complexity of the research topic, the participants were required to have solid experience in the banking industry with a minimum of five years in the domain. Of course, an acceptable level of education or academic qualification was required to ensure that the interviewees have a basic understanding of theoretical concepts. A detailed profile of the study participants is provided in Appendix 4.

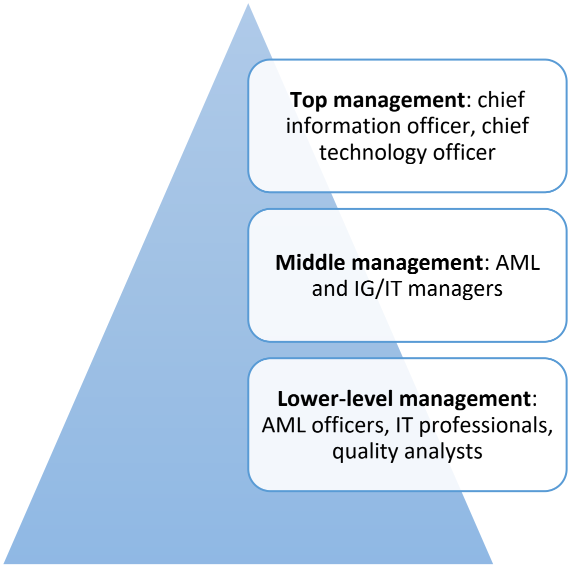

Top management: chief information officer, chief technology officer
Middle management: AML and IG/IT managers
Lower-level management: AML officers, IT professionals, quality analysts

Figure 6: The study’s participants by organisational levels

3.9 Data Collection Methods

A range of methods for data collection can be employed in qualitative research, including interviews, focus groups, document reviews and observations (Creswell & Poth, 2017; Denzin & Lincoln, 2018; Yin, 2014). One of the strengths of the case study methodology is that it allows the topic of interest to be studied from multiple perspectives using data triangulation (Baxter & Jack, 2008; Stake, 1995). Triangulating data enables a researcher to cross-validate multiple realities obtained from different sources, which in turn "helps to strengthen the construct validity of the case study" (Yin, 2014, p. 120). In this present research, semi-structured interviews, and document reviews were used to collect empirical data.

3.9.1 Semi-Structured Interviews

Qualitative interviews are the data-gathering method most frequently employed in case study research (Merriam, 2009; Yin, 2014); they are the "main road to multiple realities" (Stake, 1995, p. 64). While interviews emphasise "a face-to-face verbal exchange" (Denzin & Lincoln, 2018, p. 578) as a key mode for constructing knowledge from the interviewees' perspectives (Gubrium & Holstein, 2012; Kvale, 2011b; Myers & Newman, 2007), they tend to adopt a constructivist rather than a positivist philosophy (Rubin & Rubin, 2012). Through in-depth interviewing, a case study researcher can develop a rapport with participants (Qu & Dumay, 2011) allowing him or her to uncover new insights into interviewees' inner social lives (Kvale, 2011b).

Interviews can be classified into three types: structured, semi-structured and unstructured (Myers & Newman, 2007; Saunders et al., 2016). In structured interviews, interviewees are usually asked to answer a prepared set of standardised questions, as in questionnaires, to provide quantifiable data on a topic (Qu & Dumay, 2011; Saunders et al., 2016). Structured interviews tend to provide less in-depth data about an interviewee's experience (Myers & Newman, 2007; Rowley, 2012). Unstructured interviews, in contrast, are "informal" interviews (Saunders et al., 2016). They are generally used when an interviewer has an incomplete script or questions to ask (Myers & Newman, 2007) and hence rely heavily on participants' responses to obtain an in-depth understanding of an investigated area (Bryman, 2004; Rowley, 2012).

Semi-structured interviews are halfway between structured and unstructured (Qu & Dumay, 2011; Rubin & Rubin, 2012). They are the most commonly employed interviewing approach in qualitative case study research (Rubin & Rubin, 2012; Yin, 2014). Semi-structured interviews may be undertaken when a researcher has a specific theme to explore during an interview. Open-ended questions are used, often referred to as an "interview guide" (Bryman, 2004; Qu & Dumay, 2011; Saunders et al., 2016). The interview guide or protocol serves as a map for the interviewer, directing the conversations towards the core themes and topics of the study (Kvale, 2011b; Rubin & Rubin, 2012). When semi-structured interviews are used, interviewees are given the freedom to reflect on particular events (Bryman, 2004) while probing questions are developed by a researcher "to draw out more complete narratives from the interviewees, drilling down a particular topic" (Qu & Dumay, 2011, p. 247).

In this current research, semi-structured interviews were used as the main data-collection method. By conducting semi-structured interviews, a researcher can probe interviewees' responses, which can help them explore new relevant themes that arise from the interview. This allows a researcher to gain insights into the meanings that research participants assign to a theme of interest (Saunders et al., 2016). They can also add depth and breadth to data since different interpretations and responses can be obtained from the same interviewees (Qu & Dumay, 2011; Saunders et al., 2016). It is worth noting that all interviews in this study were conducted in English, with each lasting between 45 to 90 minutes.

3.9.1.1 Interview Guide

Before conducting semi-structured interviews, a researcher should prepare an interview protocol or guide to steer the conversation in the desired direction (Kvale, 2011a; Myers & Newman, 2007). However, to allow room for creativity and improvisation, the interviewer should not over-prepare the interview script (Myers & Newman, 2007). For qualitative researchers, there is no standard format for designing appropriate interview questions that fit all interviewees. This is because of differences in the social settings of interviews, an interviewer's background and an interviewee's perspective (Qu & Dumay, 2011). Kvale (2011a) highlighted that the contents of an interview protocol should be designed based on the research questions posed, the existing literature and the researcher's personal experience.

For this investigation, the basis of the interview guide was the principles and guidelines put forward by Creswell and Poth (2017) and Brinkmann and Kvale (2015). The researcher also adapted some questions from Tallon et al.'s (2013) interview protocol due to its relevance to this present inquiry. An outline of the proposed interview guide for this study is presented in

Appendix 1.

3.9.1.2 Conducting Interviews

Before conducting an interview, a researcher needs to decide whether to conduct the interviews in person (i.e., face to face), by telephone (Kvale, 2011a; Rubin & Rubin, 2012), or by an online method such as Skype (Deakin & Wakefield, 2014). Most semi-structured interviews are carried out face to face (Saunders et al., 2016). Although this was the favoured approach in this study, given its exploratory nature and the need for close interaction with the research participants to develop rapport (Roulston, 2014), the current COVID-19 situation called for consideration of other approaches, particularly telephone and online interviewing. Despite the theoretical debates about the limitations of online interviews (both audio and video), they have the potential to reduce travel costs, increase the speed of the data collection phase and facilitate access to participants who may be unreachable due to geographical distance (Deakin & Wakefield, 2014; Saunders et al., 2016).

The interviews will commence as soon as The University of Sheffield's ethics committee gives its approval. Before the interviews, the potential interviewees were sent an email with pre-interview information, which included the following:

- Background information about the researcher (including the university's name and courses attended) and the reasons for conducting the research.
- A brief summary of the research aims, objectives and expected outcomes.
- A copy of the ethical approval.
- A copy of the consent form

- A clear statement about the participants’ rights, including confidentiality and anonymity of information.

Once the participants agreed to take part in this study, they were asked to choose a time, place and medium for the interview that was most convenient for them. Regardless of the interview method, all the interviews were audio-recorded after the necessary permissions were elicited from the participants. Recording the interviews allowed the researcher to concentrate on the key points made by the interviewees (Kvale, 2011c). It also “permits repeated examination of the interviewees’ answers”, which can help to verify data accuracy and detect inconsistent responses (Bryman, 2004, p. 330). However, notes were taken as a backup in case of equipment failure.

To record the face-to-face interviews, the researcher borrowed audio-recording equipment offered by the university as an extended IT service for students (The University of Sheffield, 2024). To ensure the quality of the equipment, a pilot interview was conducted to avoid technical issues or inconveniences that could have affected the progress of the interviews. To prepare the interview data for analysis, the audio recordings of the interviews were transcribed into written text (Kvale, 2011c). Although the transcription procedure can be a very time consuming[5] and tedious task (Bryman, 2004; Saunders et al., 2016), it was carried out by the researcher himself. This enabled the researcher to recall the social interaction of an interview, which can, to some extent, interpret interviewees’ words more meaningfully (Kvale, 2011c; Rubin & Rubin, 2012).

[5] Bryman (2004) estimated that the transcription of a one-hour interview takes approximately five to six hours, depending on the quality of the recording.

Another advantage of transcribing the data is that a researcher can critique and enhance his or her interview style by reflecting on the questions being asked of the interviewees (Gubrium & Holstein, 2012). To reduce transcription time, a few of the interviews were transcribed and analysed in detail, after which the researcher decided which of the remaining interviews required detailed transcription (Silverman, 2013). However, interview transcripts need to be validated before starting the analysis phase, a task that is more complicated than ensuring reliability (Kvale, 2011c).

Whenever possible, all of the completed transcripts were sent to and validated by the participants themselves after their approval was ascertained (Qu & Dumay, 2011). Alternatively, a post-interview follow-up, if necessary, was arranged between the researcher and an interviewee to clarify or validate uncertain points in a transcript. It is worth noting that all interviews were conducted in English.

3.9.2 Document Review

In addition to semi-structured interviews, documents were collected and analysed in this study to provide additional context, support data triangulation, and validate findings derived from the interviews (Stake, 1995; Yin, 2014). According to Bowen (2009), document analysis can be defined as “a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material” (p. 27). Yin (2014) and Stake (1995) argued that documentary evidence is particularly relevant to qualitative case studies as it offers stable, original textual sources that are specific and cover a wide range of topics related to the phenomenon of interest. Furthermore, Merriam (1998) indicated that “documents of all types can help the researcher to uncover meaning, develop understanding, and discover insights relevant to the research problem" (p. 118). However, documents have their own limitations, including potential biases in selection and reporting, as authors may present information selectively or with a particular agenda, compounded by difficulties in accessing and retrieving certain documents (Bowen, 2009; Merriam, 2015, Yin, 2014). To ensure the quality of document data, Scott (2014) suggested four key criteria for selecting and evaluating documents: authenticity, credibility, accuracy, and relevance to the research questions. As such, documents in this research were gathered from credible sources, including official bank websites, regulatory publications, and formal access to private records such as organisational policies, annual reports, data management procedures, commercial proposals, regulations, and compliance policy documents. The rationale for using document review in this study was to triangulate and cross-validate data collected from interviews and vice versa (Bowen, 2009). It is worth noting that document review was used as a supplementary to semi-structured interviews rather than a standalone method. Therefore, the codes, themes, and analytic procedures (discussed later in section 3.10.1) used to analyse interview transcripts were applied to the content of documents.

Depending on the goals of the study, documents can be analysed quantitatively using content analysis that involved counting the frequency of specific terms, phrases, or concepts within the documents (Bowen, 2009; Bryman, 2004; Vaismoradi, Turunen, & Bondas, 2013). Alternatively, they can be analysed qualitatively using the thematic analysis (TA) approach by examined emerging themes and patterns across the selected documents (Bowen, 2009). For the purpose of this study, the latter approach was applied to analyse the documents to identify and interpret key themes related to information governance practices across different Omani banks. Examples of the documents selected and analysed are given in Table 13 below.

Document(s) name	**Description**
On-site examination procedures	This document is classified as "private" and was obtained via a formal request from the CBO. It provides rich information about the key areas in which financial institutions in Oman are examined by the CBO team. These areas include, for example, governance, risk assessment, implementation of a risk-based approach, customer due diligence, STR reporting, recordkeeping, wire transfers, cash transactions and employee training.
The Law on Combating Money Laundering and Terrorism Financing	This document was obtained from the official CBO website.
Mutual evaluation report of Oman's AML/CTF regime	This report was obtained from the official NCFI website. It presents the results of a recent joint assessment conducted by the MENAFATF and FATF teams.
Annual reports	These documents were downloaded from the official websites of banks.

Table 13: Examples of documents reviewed in this study

3.10 Data Analysis Method

The analysis phase involves assigning meaning to and making sense of data (Stake, 1995). In case study research, analysing data remains a difficult task, as there is a lack of well-defined procedures and guidelines (Eisenhardt, 1989; Yazan, 2015; Yin, 2014). However, different analytical techniques with different ontology and epistemology assumptions have been developed (Saunders et al., 2016) to reduce the risk of "death by data asphyxiation"

(Pettigrew, 1988, p. 281). In this current research, the interview data were analysed and coded using thematic analysis (TA) (Braun & Clarke, 2006). TA is considered one of the most common and flexible analytic tools; it does not subscribe to or is influenced by a particular paradigm, which means that it can be applied within positivist, constructivist or critical realist studies (Braun & Clarke, 2006).

According to Kiger and Varpio (2020), TA is particularly suited to constructivism because it can explain how a certain social construct develops by analysing and searching for themes across a large volume of datasets. The theme, which is the output of the TA process, is simply defined as “a patterned response or meaning within the dataset” (Braun & Clarke, 2006, p. 82) that informs research questions. TA is differentiated from other qualitative methods because it allows the researcher to identify themes inductively or deductively (Braun & Clarke, 2006; Saunders et al., 2016).

When the inductive TA (data-driven) approach is used, themes are derived from data or “grounded up” and thus may not reflect a researcher’s exact interest in a particular subject (Alhojailan & Ibrahim, 2012; Kiger & Varpio, 2020). In contrast, in the deductive TA (or theory-driven) approach, theme identification is often informed by and linked to existing theories or theoretical frameworks. Accordingly, a researcher may focus on specific segments of datasets that can illuminate a topic of interest (Braun & Clarke, 2006; Kiger & Varpio, 2020). This current study’s data analysis followed a six-step TA process, as illustrated in Figure 5 and described in the subsequent section.

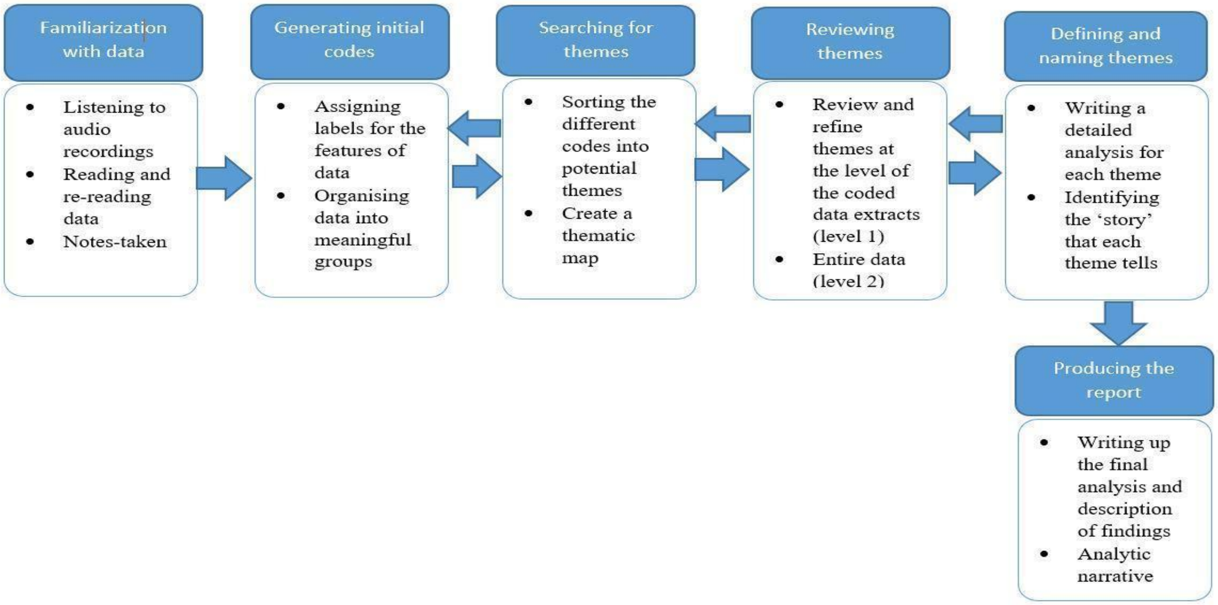

Familiarization with data
Listening to audio recordings
Reading and re-reading data
Notes-taken
Generating initial codes
Assigning labels for the features of data
Organising data into meaningful groups
Searching for themes
Sorting the different codes into potential themes
Create a thematic map
Reviewing themes
Review and refine themes at the level of the coded data extracts (level 1)
Entire data (level 2)
Defining and naming themes
Writing a detailed analysis for each theme
Identifying the 'story' that each theme tells
Producing the report
Writing up the final analysis and description of findings
Analytic narrative

Figure 5: Stages of TA (adapted from Braun & Clarke, 2006)

3.10.1 Thematic Analysis

Step 1: Familiarisation with data

As the first step of TA, it is important to become immersed in and familiarised with an entire dataset by listening to audio recordings, transcribing the interview data and actively reading the data to establish preliminary theoretical insights or ideas about possible codes or themes (Braun & Clarke, 2006). As Yin (2014) put it, getting started with the analysis involves "playing" with the data to "move toward a general analytic strategy" (p. 136).

As part of the familiarisation and analysis process, it is recommended that a researcher keep a diary or write self-memos that reflect his/her critical reflexivity on the data (Vaismoradi et al., 2013; Yin, 2014). Taking personal notes can encourage a researcher to think beyond the surface meaning of words by critically asking questions to make sense of data (Braun & Clarke, 2013).

Step 2: Generating initial codes

The second important step in TA involves "coding" (i.e., data categorisation), through which similar evidence is aggregated and linked into a common code to help a researcher answer the established research questions (Braun & Clarke, 2006; Miles & Huberman, 1994; Saldaña, 2013). Coding data, in effect, depends on the role of theory in defining the themes of a study (Braun & Clarke, 2006). When themes are defined using pre-existing theory or a theoretical framework, a researcher is likely to code the dataset that only answers the specific questions of interest (Braun & Clarke, 2006). Alternatively, when themes are more 'data-driven', the entire contents of the dataset are coded (Braun & Clarke, 2006). In this case, a researcher is highly advised to code as many codes as possible – either manually or using CAQDAS software like NVivo (Saldaña, 2013) – to support the development of initial codes (Kiger & Varpio, 2020). A detailed coding framework, including descriptions of all codes and themes developed for this study, is provided in Appendix 5.

Step 3: Developing themes

This stage involves the identification of potential themes at a higher level of abstraction by sorting, analysing and comparing a lengthy list of initial codes (Braun & Clarke, 2006). During this process, it is recommended that the researcher use diagrams or visual representations like 'thematic maps' or 'mind-mapping' as they help to identify and make sense of the relationships between codes (Kiger & Varpio, 2020). However, a researcher should bear in mind that there might be a set of codes that do not fit within the identified themes, and thus a theme called 'miscellaneous' can be created to contain them (Braun & Clarke, 2006). When this phase is complete, the researcher should have a short list of candidate themes and subthemes (Clarke & Braun, 2013).

Step 4: Reviewing themes

In the fourth phase, which Braun and Clarke (2006) described as a two-level analytical process, the themes are reviewed and refined at the coded extracts (Level 1) and the full dataset (Level 2). In so doing, the themes may be added, collapsed into a single theme, separated into different themes or even discarded (Saunders et al., 2016). This review process aims to ensure that the themes have adequate supporting data and to check whether additional data needs to be coded (Kiger & Varpio, 2020).

Step 5: Defining and naming themes

During this phase, a researcher should be able to provide a summary description of each theme and explain how it relates to or fits into the broader research questions (Braun & Clarke, 2006). A good theme will probably be connected to the topic of interest, and it has a singular focus with no overlap with other themes (Kiger & Varpio, 2020). When naming the theme, it is suggested that a 'punchy' or concise name is chosen so that it immediately informs a reader about its story or contents (Braun & Clarke, 2006). When this phase is completed, a researcher should have a clearly defined list of established themes that form the basis of the study (Nowell et al., 2017).

Step 6: Producing a report

This final step involves writing up the data, which goes beyond a mere description of the findings (Braun & Clarke, 2006). This is the point where a researcher makes a convincing argument related to the research questions and literature by providing the analytic narrative and (vivid) data extracts (Clarke & Braun, 2013). To be credible, a researcher is encouraged to use his/her reflexive journals to cross-check whether the findings have been correctly interpreted and analysed (Nowell et al., 2017). The final report of the analysis should tell a complete story of the different themes of the study.

3.10.2 Stage 2: Cross-Case Analyses

Following Eisenhardt (1989) as well as Eisenhardt and Graebner (2007), in stage two, each case's core categories are compared to identify common themes and patterns across the cases. Furthermore, cross-case analysis is used to explore case-specific issues that may vary by context and setting (Lauckner et al., 2012). The issues identified are re-examined and replicated to verify their relevance/or effects on other cases. To facilitate the comparison, a 2 × 2 table is used to combine and compare the differences and similarities of the categories between each case (Eisenhardt, 1989).

3.11 Reflections on the research process

3.11.1 The role of the researcher

A qualitative researcher plays an active role throughout the entire research process, from designing a study to collecting, analysing and interpreting data (Creswell & Poth, 2017; Denzin & Lincoln, 1994; Strauss & Corbin, 1990). Therefore, many scholars (e.g., Berger, 2015; Braun & Clarke, 2022; Hellawell, 2006) consider the researcher to be a key instrument in shaping the direction and outcomes of a study. While quantitative researchers detach themselves from a study to maintain objectivity, qualitative researchers are deeply attached to and immersed in the research context (Bryman, 2004; Creswell, 2007). According to Bonner and Tolhurst (2002) and Berger (2015), a researcher's personal experiences, biases, preconceptions and beliefs are paramount in constructing knowledge and making sense of qualitative data. However, a researcher must "bracket" and put aside bias so that his or her influence on the research can be minimal (Adu, 2019; Ahern, 1999). It is argued that the ability of a researcher to bracket personal feelings and preconceptions depends mainly on his or her level of reflexivity rather than objectivity because it is impossible to put aside things that he or she is not conscious of (Ahern, 1999; Berger, 2015; Braun & Clarke, 2022).

Berger (2015) defined the term ‘reflexivity’ as “turning of the researcher lens back onto oneself to recognise and take responsibility for one’s own situatedness within the research and the effect that it may have on the setting and people being studied, questions being asked, data being collected and their interpretations. As such, the idea of reflexivity challenges the view of knowledge production as independent of the researcher producing it and of knowledge as objective” (p. 220).

Being a reflexive researcher entails ongoing evaluation, examination and reflection of one’s own biases and their influence on different stages of the research, including participants’ recruitment, data collection, data analysis and interpretation of findings (Ahern, 1999; Finlay, 2002). Therefore, a researcher must disclose his or her positionality and background concerning a studied phenomenon so that potential readers can assess the credibility of the research findings (Adu, 2019).

The literature has identified two different roles or positions that a researcher can adopt: “insider” and/or “outsider” (Berger, 2015; Bonner & Tolhurst, 2002; Dwyer & Buckle, 2009; Hellawell, 2006). Being an insider suggests that a researcher has a *priori* intimate knowledge about a person or community, place and people of the group being studied (Chavez, 2015; Kerstetter, 2012; Merton, 1972). He or she may also share some common characteristics (such as religion, race, language and gender) with research participants, enabling the gaining of deeper insights into participants’ lived experiences (Chavez, 2015). Being an insider, however, does not necessarily require a researcher to be a member of a community or organisation being studied (Berger, 2015).

In contrast, an outsider-researcher approaches research without any prior knowledge or familiarity with the setting and people being studied (Hellawell, 2006; Merton, 1972). In this case, a researcher is considered a “stranger” or external to the communities and groups under study, which allows him or her to explore the phenomenon of interest from new perspectives (Berger, 2015). For a positivist researcher, taking an outsider position is more acceptable as it helps maintain objectivity and naturality (Chavez, 2015). However, many scholars (e.g., Dwyer & Buckle, 2009; Kanuha, 2000; Kerstetter, 2012) have argued that neither insiders nor outsiders can achieve total objectivity. Thus, Dwyer and Buckle (2009) advise researchers to take a dual role rather than strictly aligning with either extreme.

The advantages and disadvantages of insider/outsider positionality have been widely discussed and documented in the literature (Berger, 2015; Bonner & Tolhurst, 2002; Chavez, 2015; Kerstetter, 2012). However, it is still unclear whether insider or outsider positionality can lead to better outcomes in qualitative research (Dwyer & Buckle, 2009). According to Bonner and Tolhurst (2002), there are three key benefits of being an insider-researcher: (1) a strong understanding of a group’s social and cultural dynamics, (2) natural interactions with participants and (3) greater relational intimacy between the researcher and participants. Additionally, being an insider can facilitate data collection by allowing easy access to participants and data (Chavez, 2015).

Indeed, when researching in a familiar setting, insiders may already have access to participants through professional networks or friendships (Chavez, 2015; Unluer, 2012).

However, several drawbacks are associated with an insider perspective (Asselin, 2003; Bonner & Tolhurst, 2002; Chavez, 2015). A researcher's familiarity with a community and its members can lead to potential biases, particularly when analysing and interpreting data (Bonner & Tolhurst, 2002; Dwyer & Buckle, 2009). Due to their close relationships, insiders may have difficulty separating their interpretations and biases from those of participants (Dwyer & Buckle, 2009).

Additionally, assumptions of shared understanding between a researcher and participants may put responsibility on the researcher's shoulders, assuming that they are aware of unspoken issues (Hayfield & Huxley, 2015; Merton, 1972). This issue poses a risk to data analysis, as the researcher may overlook essential parts of the data and hence skew research findings towards their own experiences instead of the participants (Hayfield & Huxley, 2015). Moreover, ethical issues may emerge when boundaries between the researcher and the researched become very close or blurred, potentially leading to the disclosure of sensitive information that exceeds the participants' comfort zone (Asselin, 2003).

However, it has been suggested that being an outsider can have some advantages to the research process (Bonner & Tolhurst, 2002; Hayfield & Huxley, 2015; Merton, 1972). The most commonly cited advantage is that outsider-researchers can produce more objective conclusions, as they are not influenced by prior knowledge or commitments related to a community or group under study (Hayfield & Huxley, 2015). Additionally, it has been argued that outsiders can provide new perspectives on the researched topic by asking "naïve questions" and seeking further clarifications (Berger, 2015; Hayfield & Huxley, 2015).

However, outsider-researchers may face challenges in building rapport with participants, gaining access to data or study sites and overcoming cultural or linguistic barriers (Bonner & Tolhurst, 2002). Unlike insiders, outsider-researchers may require more time to understand a community's cultural norms or an organisation's internal dynamics, which delay their development of the research (Bonner & Tolhurst, 2002).

Outsider-researchers may also be prevented from accessing sensitive information and documents due to a lack of trust between the researcher and participants (Breen, 2007; Walsham, 1995). This can undermine the validity and credibility of research findings, as the constructed may be based on a partial or superficial understanding of the subject matter (Bonner & Tolhurst, 2002; Breen, 2007). Also, it has been suggested that outsider-researchers may be less sensitive to internal issues and challenges affecting marginalised groups, making it difficult to accurately represent their voices (Hayfield & Huxley, 2015).

3.11.2 Positionality Statement

In this current study, the researcher played a dual role in navigating between 'insider' and 'outsider' positions. This dual role enabled the researcher to explore the topic of interest from the inside while maintaining an objective position. According to Walsham (1995), qualitative researchers conducting case studies may adopt different roles while in a research setting ranging from being a complete 'insider' to a stranger or 'outsider'.

Before starting this current Ph.D. study, the researcher was known as an Omani employee who worked at the CBO, which is responsible for regulating the Omani banking sector by formulating relevant laws and regulations. Recently, the researcher was promoted to the head of data management. During my work at the CBO, I was involved in several projects that served the banking sector and, therefore, I interacted with different Omani banks where the participants were located. The researcher is also a member of technical committees, such as Fintech (financial technology), and I participated in workshops and meetings attended by the employees of different banks.

Additionally, as a business analyst who supports banking applications, I interacted with various banking professionals via email and phone. Therefore, I became familiar with the issues and challenges facing the Omani banking sector in general, but I was less aware of the internal issues and dynamics of individual banks. This provided me with an insider perspective of the CBO and a more outsider view of other Omani banks.

Having said that, I acknowledge that my insider–outsider position influenced the selection of the research topic, participants' recruitment and data collection and analysis. My insider position also allowed me to access private (classified) documents related to IG and ML, which would otherwise be inaccessible to outsiders. These documents were a good starting point for designing the interview guide as they directed me to the most important issues on IG and ML.

Several strategies were used in this study to minimise the potential effects of being both an insider and an outsider-researcher. It is believed that sharing specific characteristics and information about a researcher can impact how participants engage with the research (Berger, 2015). Despite being a member of the group under investigation, I identified myself as a researcher rather than as an employee. Even when interviewing participants from the CBO, I refrained from wearing an employee badge to distance myself from my professional role and to mitigate any power dynamics that could influence the interview process. This approach put participants at ease and encouraged them to share their experiences and views without being influenced by my position, even though I had no power or authority over them. Furthermore, I maintained a research journal as an audit trail to document and track my decisions, reflections, assumptions, feelings, thoughts and impressions. I also wrote detailed descriptions of the participants and their settings to ensure that my personal experiences and assumptions did not affect my interpretations of data. I invited participants to review and validate my interpretations of specific aspects of their interview data. Moreover, I collected and analysed relevant documents to triangulate and cross-validate the research findings.

3.11.3 Research quality

Ensuring the quality of qualitative research is crucial for establishing the trustworthiness and rigor of the findings (Lincoln & Guba, 1985; Rolfe, 2006). Research quality refers to the standards and criteria used to assess the credibility and reliability of the study's design, methodology, data collection, and analysis (Healy & Perry, 2009; Joppe, 2000). In qualitative research, quality is often defined by how accurately the research findings reflect participants' experiences, and how rigour and consistency are maintained during data interpretation (Creswell & Poth, 2017). However, there is a lack of consensus among scholars on how to assess the quality of qualitative researchers (Patton, 2014; Strauss & Corbin, 1990; Tracy, 2010). This has led to the development of various strategies that aim to ensure the trustworthiness and accuracy of qualitative studies (e.g., Healy & Perry, 2009; Korstjens & Moser, 2018; Lincoln &

Guba, 1985). Lincoln and Guba (1985) proposed four key strategies for evaluating the trustworthiness of a qualitative research, including (1) credibility, (2) dependability, (3) transferability, and (4) confirmability. The following section explains how each of these strategies was maintained in this study.

3.11.3.1 Credibility

According to Lincoln and Guba (1985), credibility refers to "the confidence that can be placed in the truth of the research findings. It establishes whether the research findings represent plausible information drawn from the participants' original data and is a correct interpretation of the participants' original views" (p. 290-291). In quantitative research, credibility is corresponds to internal validity, which focused on the aspects of 'truth-value' (Korstjens & Moser, 2018). Several strategies have been proposed for qualitative researchers to enhance the credibility of study's findings. These included triangulation (using multiple data sources or methods to confirm findings), member checking (allowing participants to review and validate findings), prolonged engagement (spending sufficient time in the field), and peer debriefing (discussing the research process and findings with colleagues to gain external perspectives) (Joppe, 2000; Lincoln & Guba, 1985; Merriam, 1998; Noble & Smith, 2015). In this study, credibility was enhanced through the use of triangulation method (Patton, 2014), where data from multiple sources (namely semi-structure interview and documents review) were compared and cross-verified. Member checking (respondent validation) was also employed, allowing the participants to review and provide feedback on the researcher's interpretations to ensure that their views were accurately captured. Participants were also invited to review their interview transcripts and suggest any corrections or clarifications. Additionally, peer debriefing was conducted by discussing the emerging themes and interpretations with fellow researchers and colleagues to gain external perspectives, validate the analysis, and enhance the overall credibility of the study.

3.11.3.2 Dependability

Dependability refers to the stability and consistency of the research process over time (Lincoln & Guba, 1985). It aims to ensure whether the research findings are consistent and repeatable if the same research context and procedures were applied again (Korstjens & Moser, 2018). In social science research, dependability can be achieved by maintaining a detailed 'audit trail' that documents all the research steps taken from the beginning of the research project to the development and reporting of the findings (Bryman, 2004; Lincoln & Guba, 1985; Patton, 2014). To address dependability issue in this study, the researcher maintained a full record of documents and procedures, including interview transcripts, audio records, reflexive journals, methodological decisions, research team meetings, analysis/field notes, consent forms, information sheets, ethical application and approval, as well as relevant policy documents collected during the data collection phase. The use of NVivo software for coding and managing data also ensured that the analysis was systematic and replicable.

3.11.3.3 Transferability (Applicability)

Transferability refers to the extent to which findings of the study can be applied or transferred to other settings or contexts (Lincoln & Guba, 1985). While generalisation is not the primary goal of qualitative research, case-to-case transferability remains an important criterion for assessing its quality (Creswell & Poth, 2017; Merriam, 1998; Miles & Huberman, 1994; Stake, 1995). According to Lincoln and Guba (1985), the researcher can enahnce tranferability of the findings by providing ‘thick description’ of the reseach context, settings, participants, and findings. These descriptions should be supported with sufficient evidence from interview quotes, filed notes, and document review (Merriam, 1998; Patton, 2014). However, it is the reader’s responsbility to judge whether the findings are applicable to their own context or situation (Korstjens & Moser, 2018). In this study, the researcher proivded a rich account of the research context (refer to section 3.7), detailing the structure of the Omani banking sector, including the types of banks and their operational environments. Additionally, this study provides details of the participants’ characteristics, including demographic information (e.g., gender, educational background, job title, and year of experience), plus the inclusion/ exclusion criteria used for participant selection (see section 3.8).

3.11.3.4 Confirmability (Neutrality)

Confirmability aims to ensure that “data and interpretations of the findings are not figments of the inquirer’s imagination, but clearly derived from the data” (Lincoln & Guba, 1985, p. 290). This means that the study’s outcomes should be derived from the actual data collected from the informants rather than being influenced by the researcher’s own biases and assumptions (Korstjens & Moser, 2018). While it is impossible to eliminate the researcher’s bias completely, researchers are advised to strive for a high level of objectivity (R. Berger, 2015; Braun & Clarke, 2013, 2021). Because the researcher is an Omani employee who working within the Omani banking sector where the study was conducted, he was familiar with the culture, language, and institutional practices. In this study, confirmability was ensured by using reflexivity (see section 3.11.1), where the researcher set aside his personal biases and preconceptions to remain as objective as possible. Furthermore, the use of triangulation method facilitated confirmability by ensuring that the findings were derived from multiple data sources rather than a single perspective (Patton, 2014). Additionally, all activities and procedures were documented throughout the research process, providing a comprehensive audit trail that would allow an external reviewer/ or auditor to trace each step taken in data collection, coding, and analysis (Lincoln & Guba, 1985).

3.11 Ethical Considerations

Ethical concerns may surface at any stage of a research process – most notably, before, during and after the collection and analysis of data (Hesse-Biber & Leavy, 2010; Israel & Hay, 2006). In social science research, ethics refers to "the standards of behaviour that guide your conduct in relation to the right of those who become the subject of your work, or affected by it" (Saunders et al., 2016, p. 239). The UK's Social Research Association states that it is essential to follow good ethical practices to minimise harm to participants, satisfy a funder's demands, ensure research integrity and follow legislation (Social Research Association, 2003). Creswell and Poth (2018) suggest that ethical considerations are particularly important for a case study research due to the close relationship that may develop between the researcher and the participants during the study. As noted previously, semi-structured interviews were employed in this research to collect empirical data, which involved physical and cognitive access to the participants (Saunders et al., 2016). Previous research highlight some of the key ethical considerations that are associated with any study, including the ethical approval, informed consents, confidentiality, and data management (Saunders, Lewis, & Thornhill, 2016). In order to ensure that this study adheres to high-quality ethical standards, these considerations were implemented and discussed in the following sub-sections.

3.11.1 Obtaining ethical approval

This research strictly followed the formal ethics policy of The University of Sheffield for research that involves human participants and the collection of personal data (The University of Sheffield, 2020). In compliance with this policy, no data were gathered before ethical approval from the university's research ethics committee was received.

In addition to meeting institutional requirements, a researcher is obliged to conduct research in a way that aligns with a funder's scholarship agreement and guidelines (Social Research Association, 2003). To this end, the researcher sought written approval from the Ministry of Higher Education in Oman – the funder – to proceed with the proposed study after it was reviewed and approved by the researcher's scholarship committee.

3.11.2 Informed consent

Gaining informed consent is an important principle of research ethics to ensure that participants are well informed about a research scope, their rights and obligations and any potential risks associated with their participation (Social Research Association, 2003; The University of Sheffield, 2020). Furthermore, an individual's consent must be granted freely and voluntarily in writing without a researcher applying pressure or coercion to take part in the study (Israel & Hay, 2006).

Broadly speaking, a standard consent form should inform potential participants about the research's purpose, procedures, risks and possible outcomes, how their information will be kept confidential and whether the results will be disseminated (Israel & Hay, 2006). Participants should also be informed that they have the right to refuse to answer any question or that they can withdraw from the study at any point without giving a reason (Hesse-Biber & Leavy, 2010; The University of Sheffield, 2020). In line with the University's ethics policy, all consent forms were obtained from the participants before conducting the interviews.

3.11.3 Data Management

A DMP is an essential component of the research process. It "provides a framework for how to handle the data material during and after the research project" (CESSDA, 2020, p. 9). It is a useful tool for controlling research data (e.g., interviews, documents and voice recordings), as it encourages a researcher to think ahead and prepare for the resources and tools required to fulfil the requirements of an institution (i.e., university policy) and the research-funder (CESSDA, 2020; Michener, 2015).

The University of Sheffield considers DMP to be a principle of good research and innovation practices, emphasising that it is a researcher's responsibility to ensure the integrity of research data throughout its life cycle (see The University of Sheffield, n.d.-b). The university's research data management policy states that a DMP should address the areas related to the collection and storage of data, along with data sharing and data security (The University of Sheffield, n.d.-b). An outline of the DMP for this research is presented in Appendix 5.

3.11.4 Reflection on Ethical Challenges in the Banking Context

Researching sensitive topic like money laundering in the banking sector presents unique challenges. Banks operate in a highly regulated environment, where disclosing failings or sensitive information can have reputational and legal implications. This may lead participants to withhold information or present biased views. Acknowledging these challenges, the researcher adopted additional strategies to build trust and ensure ethical integrity:

- **Confidentiality and Anonymity:** Confidentiality and anonymity are critical to protect participants' identities, and reduce the perceived risk of participating in the study (Israel & Hay, 2006; Saunders et al., 2016). In social science research, confidentiality refers to the researcher's obligation to safeguard participants' personal information and ensure that it is not disclosed in a way that could identify or harm them (Saunders et al., 2016). It also concerns how their data will be stored, used, and presented in the study (Israel & Hay, 2006). Anonymity, on the other hand, aims to ensure that participants' identities are not linked to their responses (Saunders et al., 2016). To maintain confidentiality in this research, all collected data and documents were stored on the University's hard drive and protected with a secure password. Only the researcher and his supervisors had access to this data. The anonymity issues were also addressed in this research to avoid accidental disclosures. Participants were informed that any personal information, such as their names, job titles, and organisational affiliations, will be anonymised. They were also told that if there is a need to present any script from their interview in the study or journal publications, then, their names will be replaced by codes like P01.

Likewise, the names of banks were replaced with generic terms such as "Local Bank 1" or "Bank A".

- **Sensitivity to Context:** Additionally, participants were reassured that their responses would be used only for academic purposes and presented in aggregated format, focusing on overarching themes rather than individual accounts. This assurance was critical in mitigating fears of negative consequences, such as reputational harm or scrutiny from regulatory authorities. For example, instead of quoting specific responses that might reveal gaps in IG practices or compliance gaps, the findings highlighted patterns or trends across the banking sector, ensuring no single participant or institution could be identified.

  Ethical Limitations: While every effort was made to encourage candid responses, the inherent difficulties in obtaining fully transparent insights in this sector are acknowledged. This limitation highlights the ethical and practical challenges researchers face when addressing sensitive topics in highly regulated industries.

3.12 Strengths and Limitations of the Methodology Approach

Evaluating the strengths and limitations of the research methodology is essential for demonstrating transparency, rigor, and reliability in academic research (Creswell & Poth, 2018). A critical assessment of methodological choices allows researchers to acknowledge the boundaries of their findings while emphasizing the validity of their approach in addressing the research questions (Saunders et al., 2016). This reflective process enhances the credibility of the study and provides a framework for future research to build upon its contributions (Bryman, 2016). In this study, the chosen methodology was designed to explore the role of information governance practices in mitigating ML risks in the Omani banking sector. The key strengths and limitation of this approach are described below.

One of the key strengths of this study was the adoption of collective-case study approach. This approach allowed for in-depth exploration of IG practices across multiple banking institutions in Oman. It also provided a comprehensive understanding of context-specific factors influencing IG adoption and their contribution to ML risk mitigation. Additionally, the inclusion of different types of banks—such as regulatory, local, Islamic, specialised and foreign—offered a diverse range of perspectives, which enriched the analysis by highlighting variations in IG practices and governance frameworks. This diversity helped in understanding how different organisational and cultural contexts shape the implementation of IG practices in the banking sector. Furthermore, the application of semi-structured interviews and document analysis can be considered a strength in this study as it allowed for data triangulation, thereby enhancing the validity and reliability of the study’s findings. Semi-structured interviews facilitated the collection of rich insights from IG professionals across various organisational levels while offering the flexibility to explore participants’ unique experiences and perspectives. The open-ended nature of questions enables participants to elaborate on their responses, and providing in-depth qualitative data. The inclusion of document analysis further strengthened the study by providing an additional layer of evidence to support and corroborate the insights obtained from interviews. Organisational documents such as IG policies, compliance reports and operational guidelines offered concrete examples of how IG practices were formalised and operationalized within the banking institutions participated in this study.

Nevertheless, certain limitations must be acknowledged. The qualitative approach, while providing depth, the absence of quantitative measures may restrict the ability to statistically validate the relationships between different components (i.e., antecedents, IG practices, and consequences) of the IG framework. In addition, the focus on the Omani banking sector may limit the applicability of findings to other contexts, due to variations in regulatory and cultural environments. Furthermore, this study focused primarily on internal IG stakeholders without considering the perspectives of external factors–such as customers, citizens, financial intelligence unit (FIU), and National Centre for Financial Information—who may play significant role in shaping the implementation of IG practices in the Omani banking sector. Moreover, the reliance on the researcher to interpret complex and subjective data, such as interview transcripts and organisational documents may introduce potential bias during the data analysis phase even if rigours analytical methods are applied.

Chapter 4: Data Analysis and Findings

4.1 Chapter Overview

This chapter presents and summarises the findings that emerged from the analyses of interview data. The aim of the semi-structured interviews undertaken in this study was to explore how various IG practices can increase the capacity of Omani banks to govern their information assets in a way that enables them to mitigate the risks of ML.

This study adopted a collective-case study approach (Stake, 2005) that involved nine Omani banks from different categories: one regulatory, five local, one Islamic, one specialised and one foreign (international). Data for this study were derived from semi-structured interviews and document reviews. Participants from different functions (e.g., IT, compliance, information security and risk management) were purposely chosen based on their involvement in information governance-related activities.

This study involved 50 participants including chief technology officers, chief information security officers, chief compliance officers, chief audit officers, IT managers, data quality analysts, data stewards, database administrators, data analytics professionals, compliance officers, heads of big data/business intelligence, risk managers, heads of performance management, heads of IT governance and heads of legal. The participants' years of experience ranged from 5–40 years.

The data collected for this study were analysed using TA by Braun and Clarke (2006, 2013, 2018, 2019, 2021). NVivo 2020 software was used to facilitate the data analysis and coding process. The codes for this study were systematically generated through two iterative phases. In phase one, deductive (or top-down) coding was applied, by which a predefined list of codes was used to code the relevant data (Saldaña, 2013). In the second phase, inductive coding was used to develop new codes directly from the raw data (Saldaña, 2013).

In terms of coding strategy, both descriptive (i.e., a word or short phrase) and in vivo (i.e., participants' exact words) were applied to label the codes. The themes for this study were selected based on their prevalence across the datasets (i.e., interviews) and their keyness to the research question. Data were collected until they were replicated or saturated (i.e., "no new codes or themes 'emerge' from data" (Braun & Clarke, 2021, p. 201).

To address the overall aims of this study, the following research questions were formulated:

- **RQ 1:** What are the antecedents that enable or inhibit the adoption of IG practices in Omani banks?
- **RQ 2:** What information governance practices have Omani banks adopted to manage ML-related data or information?
- **RQ 3:** What are the consequences of adopting IG practices on firm performance and risk mitigation in the Omani banking sector?
- **RQ 4:** What are the similarities and differences across Omani banks in relation to the antecedents, IG practices and consequences? How might these practices or the governance of ML-related data/ information be improved?

Figure 6 shows a visual thematic map summarising the key themes and sub-themes identified in this study. It is important to note that the findings (enabling/inhibiting conditions) are presented in the order of their prevalence across the dataset.

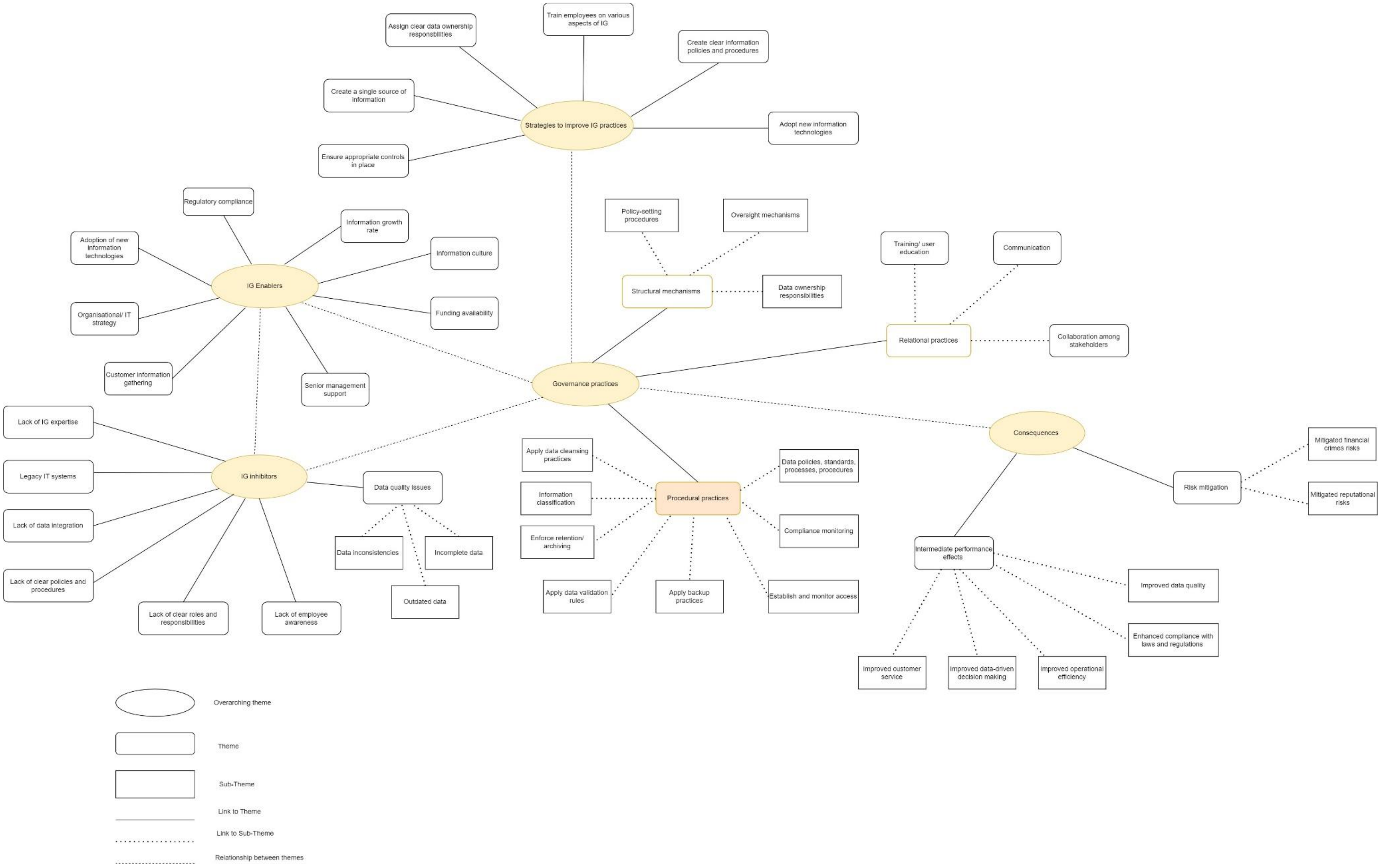

Strategies to improve IG practices
Assign clear data ownership responsbilities
Train employees on various aspects of IG
Create clear information policies and procedures
Create a single source of information
Adopt new information technologies
Ensure appropriate controls in place
Regulatory compliance
Information growth rate
Adoption of new information technologies
Information culture
IG Enablers
Organisational/ IT strategy
Funding availability
Customer information gathering
Senior management support
Policy-setting procedures
Oversight mechanisms
Structural mechanisms
Data ownership responsibilities
Training/ user education
Communication
Relational practices
Collaboration among stakeholders
Governance practices
Lack of IG expertise
Legacy IT systems
IG inhibitors
Data quality issues
Lack of data integration
Data inconsistencies
Incomplete data
Outdated data
Lack of clear policies and procedures
Lack of clear roles and responsibilities
Lack of employee awareness
Apply data cleansing practices
Information classification
Enforce retention/ archiving
Procedural practices
Data policies, standards, processes, procedures
Compliance monitoring
Apply data validation rules
Apply backup practices
Establish and monitor access
Consequences
Risk mitigation
Mitigated financial crimes risks
Mitigated reputational risks
Intermediate performance effects
Improved data quality
Enhanced compliance with laws and regulations
Improved customer service
Improved data-driven decision making
Improved operational efficiency
Overarching theme
Theme
Sub-Theme
Link to Theme
Link to Sub-Theme
Relationship between themes

Figure 6: Thematic map of the study

4.2 Antecedents of Information Governance

This section highlights the key factors that enable or inhibit the adoption of IG practices in the Omani banking sector. These findings are significant because it provide actionable insights for decision-makers on how IG practices are shaped and influenced.

4.2.1 Enablers of Information Governance

The outcomes of the data analysis show that there are six enabling conditions/factors that contribute to IG adoption in Oman's banking sector: regulatory compliance, information growth rate, adoption of new technologies, senior management support, organisational/IT strategy, customer information gathering, information culture and funding availability.

4.2.1.1 Regulatory Compliance

This theme refers to banking laws and regulatory requirements (e.g., PCI DSS, Basel II and AML/CTF act) that mandate banks and other financial institutions to govern and control their information artefacts. According to the interview findings, industry regulations were identified as the key enabler factor for adopting IG in Omani banks. The majority of participants agreed that the increased pressure from regulators forced them to align their IG policies and procedures with legal and regulatory requirements. Talking about this issue, an IT director (P28) from a specialised bank commented that "…the [regulatory] pressure [came] from the CBO and external auditors. These are the two main controllers that push[ed] our organisation to do more governance of data". Another AML director (P27) added, "There is increased pressure from the CBO on the periodic reviews of customers' data. More questions are being asked from the correspondent banks about … the customers' data".

This means that banks and other financial institutions in Oman must adhere to industry regulations to avoid penalties, reputational damage and other regulatory risks associated with non-compliance. To support this claim, a head of information security (P20) from an Islamic bank said:

> Anything that is mandated by regulation and by country level, [it is taken] very seriously in our bank and that gives a very high priority for the implementation…We [already] comply with the ISO [International Organisation for Standardisation], PCI DSS; we are also following BASEL, FATF and any circulars from [the] Central Bank …

Additionally, it was reported that new regulations enacted by national and international authorities require Omani banks to collect more information about their customers, motivating them to implement some sort of IG practices to ensure compliance.

As a head of legal (P48) from a local bank put it:

> There are regulatory obligations to keep the [customer] information for a certain period and archive it. Now this is an ocean of work of regulations, international laws, treaties, policymakers sometimes locally, sometimes outside because you're bound by certain agreements with outside banks…so, information governance is the way [to] handle that information in accordance with whatsoever rules or regulations that apply to that handling.

Some participants (e.g., P13 and P27) felt that the more information collected about customers, the better they could provide better services and make informed decisions. The analysis of interview data further showed that the regulators were clear about the data requirements in their laws and regulations. As one of the compliance officers argued (P18):

> If they [employees] are revising the law of AML, they can find what data we need from the customer ... even if they refer to 40 recommendations by FATF [Financial Action

> Task Force]. So, the problem is how we can research the information, how we can implement it [information governance] ourselves.

However, some respondents demonstrated that industry regulations helped them resolve various information issues related to data quality and security. As confirmed by an experienced employee (P06) from the regulatory bank:

> The law gives permission to banks that in case they can’t get all the information [about customers], they can close their accounts. So now some banks are starting to send messages to customers to come and update their information and if they fail to come, the bank will send a message telling them that their debit card will be blocked and internet banking or mobile banking will be blocked.

4.2.1.2 Information Growth Rate

The analysis of interview data revealed that the actual and predictable growth of raw data was regarded as the second most important factor (or condition) that enabled the adoption of IG in all eight Omani banks. Most of the respondents viewed data growth as a strategic asset that helped them increase revenue and gain a competitive advantage by providing more personalised products to their customers. For example, a head of the database (P39) stated, “Data is a future asset, it is the bank trendsetter, it defines the business of what kind of segmentation, what type of customer[s] do we have ”. Another IT manager added, “I don’t think it [data growth] is a challenge from an IT perspective. I see it as a very great opportunity for the business to have such information inside of the transactions”.

A review of the transcripts from all 50 interviews showed a significant increase in the total raw data for all participating sites –including local, Islamic, international and regulatory banks—except one specialised bank, which reported a slight decrease in the data growth due to limited business activities during the COVID-19 pandemic. When asked about their annual rate of information growth, some respondents were reluctant to share this information due to privacy concerns. However, they alluded to rough estimates to shed light on data-related trends.

As noted by a senior IT manager (P23) from a large local bank:

> Data is in terabytes, and it's growing heavily, so soon we can be in the petabytes … from the overall growth perspective, it is a very huge growth, every month I think we are getting several terabytes of data being increased in our overall infrastructure.

It was frequently reported that the annual growth of structured and unstructured data had doubled in the last two years due to the increased use of digital services during the COVID-19 pandemic. This is not surprising since customers were encouraged to perform their transactions online through, for example, mobile banking services. However, linking data growth to COVID-19 is exaggerated because, as is evident from the data, most interviewed banks were undergoing digital transformation projects, which means that their data volume is expected to increase in the coming years due to increased transactions. Conversely, it was argued that the information growth rate added further complexity to the quality and security of customers' data. This was supported by a head of compliance (P04), who stated:

> Challenges go to the quality of data and go to the volume…of data that the bank is responsible for maintaining and making use of. So if you don't have appropriate governance and robust control on top of that, then that [will be] the main challenge for [all] financial institutions …

Several compliance professionals argued that regulatory requirements were a key driver of data growth in their organisations because regulators forced them to collect more information about customers. This view was confirmed by a head of legal (P48) who has extensive experience in regulatory compliance requirements:

> The first reason for [our] bank to relook at these practices in terms of information governance … [was due to] … a heavy regulation, whether [form] the Central Bank of Oman, or any other regulators that we are subject to, they are actually very strict about this, and we are obliged to [collect] those customer data and store them in our databases.

While some participants, particularly compliance officers, described the data collection process as a ‘daunting’ and ‘overwhelming’ task, others considered it an excellent opportunity to enable data-driven analysis and decision-making. For them to monetise and gain valuable insights from massive amounts of data, banks need to develop appropriate governance practices with structures and policies designed to maximise their value while protecting customer information from unauthorised or illegal use.

4.2.1.3 Adoption of new Information Technologies

Most respondents described themselves as pioneers in adopting new technologies, such as artificial intelligence (AI) and machine learning, compared to other industries in the country. As noted by a head of legal (P48), “Banks are the biggest buyers of IT software and systems for handling information. So, nobody can compete with a bank[s] in terms of technology implementation”.

Respondents agreed that new technologies, particularly big data analytics and business intelligence, enabled them to analyse large volumes of data and automate various IG tasks. They also added that the new technological capabilities improved their capacity to reduce the time, cost and risk associated with human data errors.

In this regard, a senior compliance manager (P26) from a large local bank in Oman commented:

> Machine learning and AI helps you [us] to reduce the false-positive numbers, that … consumes the manpower, the headcount, … [previously] we have so much [many] staff looking at transactions but limited STRs [Suspicious Transaction Reports] coming out because a lot of them are false positives. So technology helped us to reduce those numbers and [also] provided us with more meaningful reports.

However, this does not mean that the technology will eliminate the role of people who are viewed as the core for successful IG implementation; rather, technological capabilities have shaped how data professionals interact with data more efficiently. With these capabilities in mind, several IT professionals (e.g., P28 and P40) indicated that their performance was significantly enhanced by employing extract, transform and load (ETL) technologies, which allowed them to automatically collect and integrate diverse data sources into a unified repository, a task that is traditionally known as time consuming and labour intensive.

This view was reinforced by an information security manager (P14):

> We have [use] something called extract, transform and load (ETL). So, we get data from a conventional core banking system, we get data from Islamic core banking system, we get data from credit card management system, debit card management system, we get all this data, [and we] put it in something called an ETL warehouse. Then, for our data analytics requirements, we use these data for fraud monitoring, for developing different kinds of models. We also use it for AML [anti-money laundering] monitoring and customer classification.

Additionally, the evidence shows that new technologies play a significant role in increasing a firm's performance in data classification and data quality. From the technical standpoint, many IT professionals perceived the functionalities associated with new data management technologies as a 'lifesaver' since they helped them to automatically cleanse and detect data anomalies by enforcing data validation rules at the file or system level. In practice, this means that the data administrator or steward is no longer required to verify which data should be accepted or rejected manually. This was particularly beneficial for business users, including retail and compliance, who were more concerned than others about the accuracy of customer data, as confirmed by a head of branch operations (P45):

> We have [implemented] new systems for KYC [know your customer], which are showing [us] how much missing data is still not filled. That has helped us to go to the head of that department or branch [and] highlight that this [data] is wrong and not as [per] our bank instructions of KYC.

Similarly, the findings showed that new technologies provided information security personnel with powerful tools that enabled them to reduce data breaches by preventing unauthorised access to or sharing of customers' sensitive information.

As described by an information security manager (P34):

> If you try to write a full card number and send it to someone … that application [will] detect this information, so it will tell you this document [information] is confidential because …there is [it has] some artificial intelligence …[so] it will force you to click [declare] whether that data is confidential or restricted.

It was suggested that the implementation of data analytics improved customer service and banking products due to their ability to mine, analyse and extract meaningful patterns from complex historical data. This idea was nicely articulated by a data analytics manager (P40):

> Data analytics help[ed] us in providing better customer experience because capturing the data, and building combined analytics across different systems enabled us to build better monitoring tools to prevent [data] errors, fix the root causes and accordingly … we could design a better product that fulfils this type of customer.

4.2.1.4 Senior Management Support

The interview data revealed that the active support of senior management, including the board of directors and C-level executives (e.g., chief executive officers, chief information officers and chief technology officers), has been identified as a critical factor for IG success in several Omani banks. Indeed, this is not surprising given that senior management has a higher level of authority and power over the organisation, enabling them to overcome financial, technological and cultural impediments.

Participants (e.g., P10, P21, P42 and P44) frequently used the terms “lead by example” and “governance by act” to highlight the need for IG champions to be involved in various activities associated with the IG initiative. According to them, support from senior management was invaluable in resolving conflicts associated with data ownership, allocating the necessary budget for training and IT equipment and recruiting subject-matter experts in the IG domain. As confirmed by an IT manager (P25):

> Our top management is well aware of the importance of data and the need for governance … so there is a management buy-in. There is an intention; there is seriousness about the evolving and developing of the DG function [framework]. And technology is aligned to facilitate it, as an enabler to implement the right solutions and infrastructure for the DG…When you have management buy-in and you have the technology, tools and infrastructure, of course, that [will] facilitate and will help [to] develop the [data] governance framework.

Other interviewees mentioned similar positive aspects of senior management in relation to continued follow-ups on information-related projects, resolving data ownership conflicts and promoting collaboration between different business functions.

For example, a head of branch support (P45) said:

> Every quarter, the board [of directors] meets, and they ask [us] what do you want from us to be compliant with the instructions of CBO [Central Bank of Oman] and other regulators, so we are getting full support from top management. This made our job to connect [with] other departments in the bank easier.

It was noted that respondents' perceptions of management support varied according to their positions and responsibilities in the organisation, with compliance departments being more privileged than IT departments to work closely with senior executives. As a compliance manager (P10) from the Islamic bank put it, "Whenever I report [raise] any request for data correction or data management to the [senior] management, they immediately take action". This is likely because the board is aware that these requests are being raised in response to specific regulatory requirements; therefore, they must be addressed to avoid any penalties associated with noncompliance.

Establishing an IG programme in a complex and dynamic environment like banks required a cultural change driven by top-down leadership. Therefore, it was argued that steering committees and other senior executives should influence the behaviour of their employees through active supervision, direction, encouragement and motivation. For example, a compliance officer (P18) from a specialised bank said, "We are getting support from the board, from the CEO himself, by issuing internal circulars and guidelines; [therefore] we are getting encouraged from their side".

A data analytics manager (P40) from a large local bank added that “the top management has said that our [new] way of designing any product should not be based on R&D [research and development]. [Rather] it should be based on analysis of our own data”. This indicates that senior management sets a clear tone and expectation for employees on how data should be governed, which, according to some, has led to the development of an information culture.

This claim was supported by a chief internal auditor (P21), who asserted:

> When the initiative of [information] governance is pushed by the board of directors, which is then pushed by the top management … which is then trickled down to the heads, which is then taken to the level of the individuals who are actually doing this, then … definitely things will improve,

Most compliance professionals hold senior management responsible for urging employees and other business departments to comply with relevant information management policies and procedures. They stressed that their ability to conduct proper risk assessments depends heavily on customer information quality, such as KYC, which front-office employees often collect. In this context, participants, such as P48, described the current leadership in the banking sector of Oman as “supportive”, “open-minded” and “dynamic” and who strive to get regular updates about information-related issues via direct communication with key stakeholders. This view was echoed by an information security manager (P29):

> Almost every quarter [we conduct] steering committee meetings … which [involve] the top management, a minimum of C-level executives, and we have the CEO [chief executive officer] or the deputy CEO to be [act as] the chairman, and we bring to

> them … all the issues or risk[s] related to data … So basically, we do have these communications, ongoing with our senior management every quarter.

4.2.1.5 Organisational/ IT Strategy

The majority of participants in this study highlighted the importance of aligning IT strategy with the overall business strategy to prevent conflicts while ensuring smooth implementation of IG practices, as noted by the head of IT governance (P32):

> IT strategy mainly is like a roadmap of where I am currently sitting and where I want to be in five years from now … So IT strategy is always equipped with the business strategy, otherwise conflicts will happen. As I mentioned earlier, we are the enabler of the businesses

Additionally, IT professionals of this study confirmed that data growth has become a core component of their IT strategies and goals. This in turn enabled them to secure the necessary IT infrastructure and storage devices necessary to accommodate the current and future growth of data:

> Data growth is one part only of our IT strategy. However, the strategy of IT focus mainly on having more digitized channels, and the infrastructure upgrade. But yes, as I said, we have a backup, a good infrastructure, infrastructure that can accommodate new data requirements or new systems with the proper backup, different types of backup to ensure the [data] availability. (P28, Bank H)

These results collectively highlight the integrated approach of aligning IT with business strategies to ensure effective implementation of IG practices.

4.2.1.6 Customer Information Gathering

The findings showed that customer information gathering triggered many Omani banks to adopt effective IG practices. Several IG professionals in this study highlighted the importance of collecting diverse customer information to enhance customer experience, develop products, mitigate risks and achieve competitiveness. For example, the vice president of performance management (P17) stated:

> For us information governance or data governance is in terms of the banking, what is the most important is customer data. The name of the customer, personal details, national ID and everything. This is one part of it, which is very critical and in case of a data leakage or anything that is very harmful to the organisation. So we need to gather all these information to ensure proper management of customer data.

Additionally, the interview data showed that banks need to collect more information from customer in order to improve their customer service by personalised their products and services. This idea is clearly captured in the following excerpt:

> The bank is now following the segment wise, to personalize the products, which is the ultimate [goal] of the bank, to reach [the point of] personalising the product to meet the needs of each customer. [To reach this] we require a lot of data from the customer and even now as a bank, we have started this initiative for the customer through mobile banking, which is we are going to updating the customer information with the latest [details], because they opened their accounts for many years (P45, Bank C)

The above quotation suggest that banks need to implement effective information management practices in order to ensure customer information is managed in a way that enabled them to achieve business growth while adhering to established regulatory requirements.

4.2.1.7 Information Culture (Promotes Information Use)

The results of this study revealed that the values, norms, and attitudes played a critical role in shaping IG practices in Omani banks by influencing how employees use, access, share, and manage information. According to the interview data, data is currently viewed by many senior managers as a ‘new oil’ for achieving bank’s strategic goals and objectives. Several participants indicated that their management encouraged them to use information for making business decisions. For example, the head of data analytics (P40) for larger bank said:

> So, from the top management, it was said that our way of designing a new product shouldn't be based on R & D [Research and Development]. It should also be based on analysis of our own data, so there was a need to design better products, not based on R & D only, but more of our own data.

Respondents of the current study perceived communication from the top management to be effective in making cultural changes and directing employees towards a more data-driven culture. In this regard, it has been suggested that participatory leadership that encourages information/ ideas sharing between employees can help banks to overcome many challenges associated with resistance to change, facilitating them to nurture an integrated information culture.

Another interesting finding is that regulatory requirements were identified by participants as a significant factor shaping information culture in their banks. This finding was unexpected and suggests a relationship between regulatory requirements and information culture. This idea was clearly highlighted by the head of information security (P14) who said:

> What we're seeing is people [employees] are open to hear what are the regulatory requirements, they're open to understand more about GDPR [General Data Protection Regulation]. They're more interested to understand privacy, they're more interested to understand what data governance is. [So] I think that the culture of knowing more improved our knowledge on data and its importance for the business

Taken together, it is clear that there is a strong realisation of the role of data and its impact in driving business growth, which in turn help in facilitating the implementation of IG practices in Omani banks.

4.2.1.8 Funding Availability

Analysis of interviews revealed that funding availability enabled Omani banks to eliminate many obstacles to IG's success. Interviewees indicated that allocating adequate funds was critical to acquiring cutting-edge technologies, upgrading IT infrastructure, hiring IG professionals, and conducting training necessary for implementing and sustaining effective IG initiatives. For instance, a head of IT manager (P35) stated:

> We have been given the green light from the Board of Directors to invest whatever needed to improve our IT systems and data management. We are leveraging the support of the board of directors on that to accomplish all the needed projects … (Bank C)

Additionally, IG professionals of this study emphasised the role of senior management in allocating necessary budget for training programs, as highlighted in the below quote:

> I [will] tell you from the training department itself. They always have a budget for the next year. And they communicate with other departments [to ask] what type of training you need for the next year. So if I talk about operational risk management, we have a budget in place for this year, to have awareness sessions for the staff and to educate them about data management (P43, Bank H)

These findings highlights the importance of allocating necessary budget for upgrading IT infrastructure, enhancing data quality, hiring specialised IG staff, and providing training.

4.2.1.10 Summary

To summarise, analysis of interview responses revealed several factors enabling IG adoption in the Omani banking sector. These included (1) regulatory compliance, (2) information growth rate; (3) use of information technologies; (4) senior management support; (5) organisation/ IT strategy; (6) customer information gathering; (7) information culture; and (8) and funding availability. The study also found that these factors are interconnected and affecting each other. For example, the results showed how the regulatory requirements increase information growth, and how senior management support help in shaping the information culture.

4.2.2 Inhibitors of Information Governance

The previous discussion in section 4.2.1 highlighted certain enabling factors or conditions that positively impact the adoption of IG practices in different Omani banks. This section, however, sought to shed light on the key challenges that hindered the adoption of IG practices in Omani banking sector.

4.2.2.1 Data Quality Issues

In response to the question, "What are the major challenges inhibiting the adoption of IG practices in your organisation?" data quality issues were the most prevalent theme in the interview data. This theme was strongly discussed by almost all research participants who viewed it as a key obstacle to IG success at their respective banks. Participants frequently used words such as 'information', 'data' and 'quality' to voice their concerns about data quality. Likewise, some participants, such as P07 and P17, used the phrase "garbage in, garbage out" to describe the negative consequences that may emerge from poor data quality.

Although participants have similar banking backgrounds, their experiences with the data quality problem were diverse. As expected, compliance professionals were more concerned about the accuracy of the data than were other business departments. This is perhaps because they largely rely on high-quality information to make complex decisions related to financial crimes, risk management and regulatory compliance.

For example, a chief compliance officer (P13) at a large local bank in Oman stated:

> If you have an issue with data quality, you're going to capture incomplete details, which means that you will not be able to … assign them [customers] to the right profile, so you won't be able to split them into high, medium or low risk, which means that … [the] whole AML [anti-money laundering] programme could be undermined because [you]

> don’t [apply] a risk-based approach. For example, you could have a customer who is a high risk, but you [wrongly] classified him as low risk, so you will simplify due diligence and reduce monitoring. Whereas you should [perform] enhanced due diligence, getting more information and increase monitoring.

Establishing an effective IG initiative requires a comprehensive understanding and deeper insight into the reasons that could lead to data quality problems. This study revealed that the main reasons for poor data quality in most Omani banks interviewed were incorrect data entry, missing and duplicated data and outdated customer data. Local banks were among the other bank categories that strongly enriched and contributed to the discussion of data quality issues. This result may be explained by the fact that local banks have many customers in the industry, which means that they are likelier to incur significant profit losses if wrong decisions are made based on inaccurate customer data.

Data entry errors were generally viewed as one of the main reasons for data quality issues across most of the participating Omani banks. The data analysis revealed several conditions that might motivate employees or data inputters to enter erroneous data into systems. Depending on the person, these could be intentional or unintentional. Of course, educated employees who appreciate the value of data will not intentionally enter the wrong data, but without an effective governance framework, errors are unavoidable. Interestingly, the findings showed that the majority of Omani banks assigned data-collection tasks to inexperienced staff, such as clerks who lacked basic skills in IG.

This idea was supported by a credit and market risk manager (P33) from a local bank:

> The quality of the data is a challenge that we are facing. The people who actually input the data into the system, I would say [they are] junior staff who do not understand the importance of the data that they are inputting.

It was identified that another reason for data professionals inserting incorrect data is that sometimes, they do not have a formal procedure to guide them on how and what information must be entered into the system. According to the interview data, this problem was particularly prevalent among small banks.

As a senior compliance officer (P18) from a specialised bank put it:

The issue of [data quality] is there because we have no KYC policy in the bank … if there is a clear guideline or framework … maybe we can manage the data properly, and in a high quality”. This result, however, must be interpreted with caution because data quality policies do not guarantee that employees will adhere to specified data quality requirements.

However, evidence shows that customers sometimes refuse to share their true information with banks, which, in turn, forces data professionals to enter false information to fill in mandatory fields in the systems. For example, some participants reported that customers with criminal records always try to provide fake phone numbers to evade possible tracking or monitoring. With the development of data protection regulations such as the GDPR, people have become more inclined to not share their sensitive information with a third party, such as banks, without a clear, lawful basis.

While many businesses, including financial institutions, may use customers’ personal information for commercial purposes, customers must have the right to know how their data will be handled to protect their privacy. However, the analysis of the data shows that most customers are unaware of the rationale for collecting their personal information.

As one chief compliance officer (P27) explained:

> We often face challenges when it comes to obtaining and more [when] updating customer information because the awareness is not there. We have a law, but many people [customers] are not aware of the requirements of the law and the regulations. So they don’t know why we are asking for this information. We try to educate the public through our branches, but still, they are adamant. The culture is that they will not provide what we ask them. So, it takes a lot of time and effort to gather this information [that] we require under KYC [know your customer] and CDD [customer due diligence] guidelines.

The preceding quote clearly suggests the need for the regulator and banking institutions to work together to educate the public about the importance of customer information through various channels including social media, campaigns, public meetings and seminars.

Several interviewees expressed serious concerns about outdated customer data collected before the implementation of data-related regulations in the Omani banking industry. These interviewees reported that this legacy or outdated customer data was recorded in physical documents and lacked basic demographic details, making it difficult to reach customers to update their information. This issue was clearly highlighted by a branch manager (P45) from a large local bank: “The big issue we are facing is old accounts … [because] there is no phone [number], no address, nothing … we don’t know [if] this client is still alive or dead, no one knows”.

According to the same participant, banks have no authority to close or delete old accounts from the core banking system as long as these accounts have active transactions. In this regard, some IG professionals were confused about what to do with legacy accounts, arguing that it was not their fault since some customers' details were not required to be collected in the past. However, the findings of this study showed that outdated data stored in the core banking system not only delays data migration projects but also affects the monitoring of customer transactions. As one chief compliance officer (P10) put it, "We are facing [the challenge of] receiving outdated data … because if we get wrong inputs into the system, we will get wrong outputs. So, our monitoring framework will be useless or pointless". The convenience of using social networks and financial services in recent years has given clients more flexibility to modify their information, such as mobile numbers and employment, making it extremely difficult for bankers to update their old data.

4.2.2.2 Lack of Clear Policies and Procedures

The interviews conducted with IG professionals from different Omani banks revealed a significant concern over the ambiguity of existing IG policies and procedures. Such confusion led to inconsistent implementation of various IG practices across different departments, leading to substantial regulatory risks or penalties. Interestingly, some participants attributed this this problem to the lack of clear guidance from the regulators.

For example, the head of compliance monitoring (P12) stated:

> We feel like the regulatory should give us more details and guidance so that all banks are in line … the basics have to be there and clear for all banks in order to develop our policies and procedures. So that they don’t see differences in every bank they visit. And I asked a lot of banks and I feel the process is too different.

The lack of detailed regulatory guidance from the Central Bank of Oman (CBO) has resulted in inconsistency, making it difficult for banks to effectively manage their data. Without clear and consistent regulatory guidance, banks may struggle to standardize their practices and ensure compliance with regulatory requirements. This can lead to differing interpretations of regulations among banks, potentially resulting in varying levels of compliance and legal risks. This issue is exacerbated when policies are created but not actively followed or enforced, leading to a gap between the policy's intent and practical application. As highlighted by the vice president of information security (P30): “there are many people creating policies and procedures and all that, and eventually, it's shelved and put into a cabinet, and nobody's actually really acting upon them”.

4.2.2.3 Legacy IT Systems

Banks and legacy systems are two sides of the same coin. To date, banks and other financial institutions have been accustomed to working with old or outdated IT systems, albeit with the high maintenance costs and risks involved. Not to mention the problems associated with compatibility, data quality, data integration, data security and performance. Despite these challenges, many banks consider legacy applications to be important assets because they contain mission-critical information that has been collected and stored over a prolonged period of time. In this study, however, the problem of legacy IT systems was strongly expressed by research participants who viewed it as a major obstacle to the innovation and implementation of IG practices in the Omani banking sector. As indicated by an IT manager (P25):

> In an industry like banking, it's not that easy to implement information governance practices because banks always come with legacy [systems] … so, that is an inhibitor factor [which] holding us back from doing a lot of innovations and [digital] transformation.

Participants frequently used the terms "system" and "data" when talking about the implications of legacy systems for data management. On the other hand, they used the term "risk" to raise their concerns about various operational and compliance risks that arise from using old systems.

While several participating banks showed enthusiasm for modernising their IT applications and building scalable data infrastructures, they were unable to do so due to difficulties in obtaining details of existing data sources. In many cases, however, IT professionals reported that they face technical challenges in accessing and retrieving certain customer information as it is hosted on servers with outdated operating systems that are no longer supported by the supplier. This makes it nearly impossible for banks to gain insights into what data exist, where they are stored, who can access them and how they generate value. In this regard, one of the database administrators (P41) asserted that the lack of technical documentation prevented them from understanding the data structures and their schemas, which is a crucial requirement for any data migration project. This assertion was further supported by the internal audit manager (P35):

> We need to see what type of data we hold and what the quality of this data is. We have been operating for a long time with bad-quality data that resides on legacy systems, and correcting this amount of data and keeping it in good shape is a big effort. Data format and its structure is something that also concerns us, especially … [when] integrating this data between different systems.

Of course, having no awareness of existing data assets will not only delay the process of migrating legacy data to new systems but can also make it harder to explore the potential benefits of that data to achieve organisational goals.

Another major problem caused by using existing legacy systems is that it significantly increases the maintenance cost of IT infrastructure without providing any value or innovative services to the organisation. This is not to say that maintaining new systems is cheaper, but the data show that older IT systems are more expensive to replace or maintain. As the head of IT governance (P32) put it, "The IT equipment is an expense to the organisation not only on the day of the purchase, but the maintenance of that system goes higher when the system gets older".

The analysis of the data revealed two primary reasons why legacy systems become particularly expensive to maintain in different Omani banks. First, these systems were developed by retired or former employees using obsolete programming languages, making it increasingly difficult to find qualified employees at the bank who have experience with these languages. This means that if a bank needs to add or modify specific parameters in its legacy systems, it will require an expensive outsourced vendor.

Second, the cost of repairing or replacing the hardware of the legacy system is too high because it has reached the end of its useful life; hence, the supplier no longer sells or manufactures these products. Opinions differed as to whether banks should retain or replace their outdated IT systems. While most IT professionals agree that older systems must be replaced to reduce IT budget overhead, others believe that they still satisfy their core purpose. However, business users were concerned about the possibility of developing a new system that does not meet their needs. Of course, in the absence of technical documentation of legacy systems, developers may make changes or ignore some important business rules or functions, which may lead to compliance issues. This is because legacy data are still subject to regulatory requirements, such as record retention and archiving. As noted by an experienced compliance manager (P11) who previously worked in a regulatory bank:

> Other challenges right now will come with your rules and regulations, especially when you [they] require a new field to be implemented in the system. Of course, the business wants to maintain its profits. And it will be costly to customise your [legacy] system. Maybe it [you] will need to change the entire system, which may cost you millions. That is a challenge we all face, … but you’re talking about the data, which you cannot do [manage] manually. You cannot find another solution to mitigate its risks. So, you have to either change the entire legacy system or customise it, which will cost you a lot. So, it’s becoming costly as a compliance requirement.

Besides being a big financial burden on the organisation, integrating legacy systems with new technologies was viewed as another hindrance to the adoption of IG practices in Oman’s banking sector. This is because the technical architecture of older applications was not designed to share information with other systems or functions; as a result, many systems become isolated and their data is stuck in silos. When siloed applications are used, business units can only access their data, preventing them from extracting other relevant data that might be useful for making informed decisions. In light of this, the study found that various departments in different Omani banks are still using legacy systems for specific operational purposes, such as customer service, lending, cheque processing and AML. However, the databases of these legacy systems were accessed only by a group of business users who owned the system, making it difficult for other stakeholders to obtain a 360-degree view of the entire data. This issue was clearly highlighted by the head of big data (P16):

> The challenge that we are currently facing is [allowing] all business users across the bank to have access to their data, analyse them, get inside and make informed decisions. If you look into our bank today, there is a lot of [data] silo because each department starts with its own system, so the silo is increasing. Everyone has gotten their own initiative, and they get approval. And the other departments are lagging a little bit, and that is also a challenge.

Undoubtedly, working with siloed applications not only produces fragmented information that is difficult to combine into standardised formats but also reduces the productivity of employees since they have to seek other sources to gather the information required for a specific task. This, in turn, can lead to mistrust and a lack of collaboration among key stakeholders, which can create further challenges in communicating the benefits of information sharing across the organisation. Also, it was suggested that due to compatibility issues with the latest technology, many departments were unable to capitalise on existing data capabilities like BI that had been implemented as part of the digital transformation projects. As noted by the head of E-channels and IT core systems (P47):

> A lot of intelligent data analytical solutions are being adopted … but usually, the data is parked in different [legacy] systems. So, to make use of such new technologies, intelligent data analytics solutions must be connected to all these systems to have better decision-making.

Lastly, and most importantly, the research revealed that unintegrated legacy systems led to inconsistent and poor data quality since the same customer information is stored in different databases within the same functional unit or organisation. In this regard, some compliance professionals reported that they had to access multiple data sources, such as core banking systems and AML transaction monitoring, to collect and cross-check customer information. This implies that there is no single source of truth on which employees can rely to make accurate decisions. This was supported by the chief internal auditor (P24): "The data is scattered in different systems, but the essential data that we have to put together, we capture it from the core banking systems, and also from other key systems". However, it has been suggested that some departments have conducted regular reviews and updates of customer information without involving or communicating changes to other teams that may be impacted by these initiatives. While it seems useful to perform periodic health checks of data, they must be done in coordination with other business users who maintain similar customer data to avoid duplication and inconsistencies between databases.

4.2.2.4 Lack of Data Integration

The data integration problem is one of the biggest challenges to overcome in the banking industry due to the complexity of products offered to customers. Part of its complexity is that it creates data silos that make it harder for banks to compile and consolidate customer data from multiple sources into a unified view. However, it is important to integrate and create a single source of information so that employees at different levels can access the information they need to do their jobs. According to the results of this study, many employees spent more than half of their time searching for and collecting relevant customer information to complete a single task, such as a loan request. In some cases, customer information was found to be shared among employees in different departments through manual data collection methods such as emails, phone calls and spreadsheets. This, in turn, has reduced their productivity and slowed down the decision-making process, which could result in poor customer service. Of course, if parts of customer information are inaccessible, it will be harder for staff to understand customer preferences and needs, prompting some clients to switch to another bank.

Additionally, this study revealed that data integration challenges increased the compliance risks, especially when banks submitted incomplete or inconsistent information to authorities that rely on that information for making a strategic decision at sectoral, national or even international levels:

> We had a big problem in reporting data … to the CBO [Central Bank of Oman], or any regulator like Visa or MasterCard ... The numbers provided by finance never match the numbers provided by retail and never match the numbers provided by IT, so it was always a mess. … for example, the number of customers who are not performing well.

> Finance [department], they take it from core banking, retail, they take it from CRM [customer relationship management]; IT, they take it from a third source. So, as a decision maker or a CEO [chief executive officer] or a GM [general manager] in the bank, you could see three different numbers, and you'll never know where the truth is. So, retaining a single source of truth is challenging. (P40, digital banking and data analytics manager)

To address the above challenges, some compliance managers suggested hiring more staff and dedicating them to preparing data in accordance with regulatory requirements. Preparing data, however, is the first and most complex task in any data integration project because it requires a lot of time and resources to manually collect, analyse and standardise data.

The analysis of the data revealed three main reasons that hinder data integration efforts in most Omani banks. These include: (1) heterogeneous data sources, (2) lack of centralised data hubs at the national level and (3) lack of data warehouses. The following sections provide a detailed discussion of each subtheme that arose from the data analysis.

Omani banks adopt hundreds of systems to provide their customers with a range of products and financial services, including loans and deposits. These systems capture specific customer information related to their products and store it in decentralised databases.

For example, an IT manager (P47) from a large local bank commented:

> We have the customer data and financial data is spread in different systems. We have some data in the mobile/internet banking and we have data in the core banking system.

> And we have data in the reporting system. And we have data in the collection system. And to apply the governance in [of] each system is a challenge.

Most IT professionals stated that because different source systems use different data formats, they struggled to create a common view for mapping and integrating banking data. According to the head of the database (P39), this technical challenge was encountered because of the fact that "… the entire data [is] reside … in a heterogeneous way concerning its own systems". For IG professionals, this means that significant time and resources are needed to standardise and eliminate redundant information from each system.

Additionally, it was reported that some customer data are difficult to collect because they are stored in physical files located in different branch offices. To unlock the hidden value of information, banks must develop strategies to integrate their information assets (including both digital and physical assets) in a more efficient and usable way so that data users can take full advantage of them. For example, by combining a client's credit history with his or her returned checks over the last five years, a credit analyst can generate a more accurate credit report and rating than would be possible by itself. However, the interview data suggest that Omani banks were weak in this regard, as confirmed by the senior vice president (30): "There's no way we can achieve information governance, [because] we always have information and data scattered everywhere without having the possibility of monetising them in a proper manner". Data integration and monetisation may have the potential to increase the profits of banks, but according to the head of performance management (P17), many employees "… have a single view of information", which means that "… the multi-dimensional view of customers is not there".

There is no doubt that building a data warehouse in such a dynamic industry like banking is extremely complex, but it can be an effective tool for bankers to store and quickly access information when needed. A data warehouse can also help IG professionals in banks to access and analyse large amounts of historical data so they can predict future operations and make informed decisions accordingly. For example, banks can use historical data to predict the likelihood that a customer will default on a loan. Despite its usefulness for decision-making and business growth, some executives interviewed believed that banks should not waste their money and resources implementing data warehouses, as data is stored elsewhere in the enterprise databases. On the surface, it appears that these executives want to direct the available resources to the bank's core businesses, but in reality, they don't seem to appreciate the efforts put by employees to collect data from different source systems.

The analysis of data revealed that the majority of participating banks failed to implement a fully-fledged data warehousing system due to technical, management and resource challenges. Given that, some of these banks have built a smaller version of a data warehouse called a data mart, which contains specialised sets of information about meeting the requirements of specific business departments like compliance, sales or marketing. As indicated by the head of IT (P25), "We do not have a single data warehouse in place yet. Most of our systems are decentralised … [but] data moved to a data mart, which is useful [for] analytics and BI [business intelligence] reports".

While some business managers viewed data mart as an effective way to solve problems in their departments, others argued that data mart is not as effective as a data warehouse because it only contains information from a single or a few sources that are not relevant to other business users. However, the findings showed that creating multiple data marts for each business unit can delay data warehouse implementation and make data collection so difficult, because "…each data mart has its own database … some use SQL and others they use Oracle …so, everything has its own data format (P19, Head of IT governance). This can increase the overhead for IT professionals, especially if they do not have prior knowledge of database design and software implementation.

Additionally, data collection was identified as another challenge that hindered the implementation of a data warehouse in most interview sites. Many participants acknowledged that their management provided them with significant resources and funding, but their data warehousing efforts often "end up with a story of failure" due to the difficulty of collecting and analysing large volumes of customer data. As was evident in the data, this challenge was attributed to the lack of technical expertise in "capturing the data from the different systems" (P40, data analytics manager).

This finding can be explained by the fact that many Omani banks have outsourced complex IT projects, such as data warehousing, to external vendors. Accordingly, IT staff were assigned the responsibility of preparing the infrastructure and providing the necessary access to databases without being directly involved in a data collection activity. However, it has been argued that outsourcing data warehousing projects may distract IT professionals from performing their core responsibilities because according to the database administrator (P41), vendors "don't know where the data located within the systems. So, they come and ask [us], collect for me X Y data from different systems, put it for me in this location in this format". With this in mind, implementing the data warehouse in-house seems more ideal than outsourcing, since most of the work must be done by employees.

Omani banks do their best to overcome internal challenges to ensure successful IG implementation, but their efforts are hampered by the lack of centralised financial data at the national level. Many interviewees agreed that creating a national databank could improve the efficiency of banks by allowing them to collect and verify customer information, thereby eliminating redundant data in different databases. As a chief compliance officer (P07) asserted, "There should be one hub of information at the country level where it [we] can update customer IDs, check commercial registration validity, municipality licence, rent agreements".

Based on the interview data, the Central Bank of Oman established a centralised database of credit and financial information (a.k.a. Mala'a), enabling banks and other financial institutions to access reliable and up-to-date information derived from trusted data providers, including the Royal Omani Police, Ministry of Labour and Ministry of Commerce and Industry. While useful information about individual and corporate customers can be found in this database, compliance professionals criticised it for being too specific to credit and loan information. Evidence from data showed that compliance employees subscribed to several external databases (e.g., the Office of Foreign Assets Control) to comply with existing regulatory requirements. This finding was confirmed by a head of compliance (P03):

> A very simple example is politically exposed persons [PEPs], the law covers that which I agree we should cover it, and we should look at their transactions. But the law missed a simple part by mandating a national database for the country to capture PEPs [information]. Other jurisdictions, for example, have AML law, but they have their own

> database for PEPs … In Oman, we don’t. We use international databases that cover international PEPs and not local PEPs. So, this is one of the key issues I see, not mandating a national database.

Regardless, the results showed that some banks have been fined by the CBO for failing to determine whether a customer is a politically exposed person. Participants acknowledged that the law provided them with a list of positions that should be considered PEPs, but it did not declare their names or relatives, including spouses and children. In Middle Eastern countries, including Oman, it is culturally unacceptable to ask a client for his wife’s name because it is seen as an invasion of privacy. However, identifying PEPs could help banks reduce the risks of ML by increasing the monitoring of these customers.

It has been suggested that access to a national data hub could enable banks to better comply with AML regulations by enabling them to identify and report suspicious transactions to law enforcement. One reason for this is that a national data hub can collect and share customer data across all financial institutions. In support of this idea, a head of compliance (P10) said:

> If we have a centralised platform [database], we will be in a better position to make conclusions about customers, who are acting or attempting to commit a money-laundering transaction … So, tomorrow if we have any suspicious transactions … we can go and check that platform [if] the customer has any history of money-laundering. So, we could have our database at the country level, like [what] we have now actually a hub at the international level, OFAC lists and other lists. That’s the challenge.

Meanwhile, Omani banks submit their STRs and other supporting documents to the FIU and CBO for further investigation. However, this information was only accessible to a few employees of the respective bank, preventing other banks from obtaining the list of blacklisted or sanctioned customers needed to prevent ML activities.

4.2.2.5 Lack of IG Awareness

This sub-theme represents employees' knowledge and understanding of the existing laws, regulations, policies and technologies used to govern enterprise information. Evidently, the lack of awareness was identified by many participating banks as the second biggest barrier to IG adoption. Participants frequently used the terms 'awareness', 'data' and 'people' to emphasise the importance of training to improve employees' understanding of various aspects of data. They also used the term 'customer' to highlight the need to educate customers about the importance of providing accurate and complete information to banks.

Despite ongoing investments in training and education, this study revealed that a large number of employees across different Omani banks are unaware of the value and risks associated with data. As one IT governance professional (P31) put it, "There are very few people who necessarily understand the relevance of data … and what it means on a personal basis and on a business basis". As mentioned by those involved, most employees perceived data as a noncore business that wasted their time and effort.

As clearly indicated by the data analytics manager (P40), "Data is still seen as cosmetic … although we started to see some good results of use cases using data". This might be explained by the fact that IG is still immature in Oman's banking industry. Therefore, it may not be given the highest priority compared to other business activities (e.g., retail banking) that directly contribute to the bank’s profits. Interestingly, when asked what information governance means, the majority of respondents acknowledged that they were hearing about this concept for the first time, but they were able to provide some keywords related to IG components, such as “information handling”, “information management”, “data quality” and “information security”.

However, frontline employees (i.e., customer service representatives) in particular were found to be less familiar with existing information policies and procedures. They also have limited knowledge of regulatory requirements, which leads them to underestimate some information because they feel that it will add more work to them during the onboarding or account-opening stages. This issue was mentioned by the market risk manager (P43) from a specialised bank who stated that “… the staff are not aware of the importance of know your customer information [KYC] … they don’t know this KYC information is needed to be compliant with the laws and regulations of CBO [Central Bank of Oman]”.

One possible reason behind this problem, as the data suggests, is that frontline staff are often located in branches away from headquarters, where most awareness and committee meetings are held. Thus, they are likely to be unaware of the current issues and risks associated with the poor management of customer information. In this regard, the head of the transaction monitoring department (P12) reported that many employees are only focused on how to obtain bonuses and achieve the end target, so they “want to bring customers even if there are risks associated with those customers”. Clearly, the lack of employees’ awareness in this context was directly related to the expected benefits of managing customers’ information.

Employees at all levels of the organisation need to be trained in their roles and responsibilities, and their job descriptions must include sufficient details of key IG tasks assigned to them. Despite this, the analysis of the data revealed that IG professionals at several Omani banks were unaware of their roles and responsibilities, either due to unclear assignments or conflicting roles with other business units. One interesting finding was that employees within the same ad had a different understanding of their roles, with IT staff being more aware of their IG responsibilities than other departments. This view was supported by the database administrator (P41) from a local bank:

> The people in [our bank] don't have a high level of awareness of [their] roles and responsibilities … some of the departments such as IT are on [an] acceptable level of having specific roles and responsibilities and ownership, but others are not. People in the branches and front-office employees ... [are] even go lower in terms of the understanding, but … they are willing to implement what is being requested from them to do.

Of course, having effective IG policies and procedures without communicating with and educating staff on how to implement them in practice can lead to issues in handling customer data. Respondents generally agreed that when employees do not understand certain aspects of data, they assign a dummy input contrary to what is stated in the respective policy. This idea was best illustrated by the credit and market risk manager (P33):

> When our people input the data, there are multiple columns that need to be selected as drop-downs. And if the person does not understand a particular aspect, he usually goes and selects 'others' …[however], others are only for the ones which have not [been]

> described in the six or seven categories we have in the system. But because of a lack of awareness, the person is actually inputting invalid input for that data segment.

Another important finding of the study was that senior management employees do not appear to be fully aware of the negative impacts of information on a bank's performance and success. Interviewees agreed that when a bank faces financial difficulties (i.e., like those experienced during the COVID-19 pandemic), senior managers tend to immediately reduce costs associated with data initiatives, arguing that data is not a core business for the bank. An information security manager (P34) shared his experience in this regard:

> There is a problem with the management's understanding of DG; this problem becomes even worse when they cannot secure the necessary [budget] to protect customer data. They don't know that if customers' data are compromised, they have to pay money for them. But [with] the security, there is no turning back. If something happens, the [bank's] reputation is gone. In response to this view, the IT governance manager (P32) of an international bank asserted:
>
> > Even if you have convinced the top management to provide you with the highest budget to purchase the most expensive and state-of-the-art technology to protect your data, what's the use [of it] if people aren't aware and educated about the information systems and the data criticality

What is obvious from the above excerpts is that the success of IG is not a matter of technology or budget but rather the awareness and belief of employees at all levels about the importance of information in achieving strategic goals.

In addition to the employee awareness problem, this study revealed that the efforts of Omani banks to adopt IG practices could be hindered without support from their customers (including individuals and corporates). To provide the necessary support, customers need to be aware of the benefits of their data in improving the customer experience by analysing their historical data, which allows banks to understand and create more personalised products that meet customers' needs. Equally important is that banks must educate their customers that providing false or inaccurate information, such as customer identification documents, makes it harder for them to detect and trace suspicious or illegal activities, which in turn exposes banks to reputational and compliance risks. However, the data analysis showed that many customers were unaware of the importance of some data requirements (for example, proof of address, marital status, source of funds, etc.) that are often collected during the account-opening stage. More than half of the participants reported that they had difficulty convincing customers to provide relevant information to comply with existing KYC requirements. For example, a chief compliance officer (P03), who was concerned about this issue, said:

> When employees ask them [customers] questions like, where is this money coming from? Where do you get this money from? Where do you work? Where do you live? They'll be telling them: Why are you asking these questions? It's not your business. They don't understand the requirements behind it.

Another chief compliance officer (P07) added that some customers were reluctant to submit and update their KYC information because they thought that other banks do not ask for such details. This may be because some banks have discarded specific data requirements to attract more customers. Conversely, the results suggest that many customers were unaware of the importance of collecting customer data to comply with regulatory requirements, assuming that banks would make more profit by sharing their data with third parties, including public prosecutions and FIUs.

According to a senior vice president of performance management (P17), some clients complained that customer service representatives had blocked their accounts because they had failed to submit additional KYC information recently mandated by the central banks without being informed about its importance. Surprisingly, it was suggested that many employees, including senior managers, have struggled to explain certain regulatory requirements to their customers due to their inability to understand how to apply these requirements in practice. In support of this, several participants confirmed that they had requested more information from their customers to comply with the new regulation on politically exposed persons (PEPs), although they expressed greater concern about the regulator's directives in this regard.

Clearly, there has been strong tension between what banks want customers to be aware of and the ability of employees to understand and educate customers on how to respond to relevant regulatory requirements. In light of this notion, there seems to be an urgent need to conduct public awareness campaigns by banking institutions, regulators or both to highlight the importance of IG practices from a customer and bank perspective.

Lastly, it is worth mentioning that developing and instilling an information culture in the minds of heterogeneous groups of individuals is a challenging endeavour, as noted by one of the senior managers (P27):

> We try to educate the public through our branches, but still, they are adamant. The culture is that they will not provide what we ask them. So, it takes a lot of time and

> effort to gather this information or whatever we require under KYC and CDD [customer due diligence] guidelines.

4.2.2.6 Lack of clear roles and responsibilities

Analysis of interviews revealed that the adoption of IG practices in Omani banks was hindered by the lack of clear roles and responsibilities. Participants of this study confirmed that the role and responsibilities across different departments are often overlap with each other, leading to confusion and conflict. For example, the head of data analytics (P40) said:

> Unfortunately, we don't have clear roles and responsibilities. To be honest, that's what I told you in the beginning, that we are taking baby steps in terms of data governance, we lack a lot.... So, some of the departments already know their data ownership responsibilities, and they help out in validating this data, some of them are not

Additionally, it was reported that some employees do not understand the role of IT, as they thought that they are the owners of data. This misconception found to cause conflicts among IT and business departments regarding data ownership.

4.2.2.7 Summary

This study identified several factors inhibiting IG adoption in Omani banks. These are: (1) data quality issues; (2) lack of clear policies and procedures; (3) Legacy IT systems; (4) lack of data integration; (5) lack of IG awareness; and (6) lack of clear roles and responsibilities. In particular, data quality were identified in this study as the major challenge hindering IG adoption in the Omani banking sector. Again, it was found that these factors are interconnected and affecting each other. For example, it was found that data quality can suffer if employees are not properly trained to apply existing data quality policies in practice. Likewise, it was found that legacy IT systems were negatively impact data integration efforts.

4.3 Information Governance Practices

4.3.1 Structural Practices

4.3.1.1 Data Ownership Responsibilities

As part of the ongoing discussion to uncover the various structural practices adopted by Omani banks, participants were asked who is responsible for information management and how data ownership was assigned to different IG professionals in their respective banks. The majority of those who responded to this question agreed that everyone within the organisation is responsible for managing and protecting the information assets and that responsibility should not be held by one person or department: "Data is never a responsibility of an individual group or an individual unit or an individual division. Everybody is responsible for the confidentiality of the data" (P39, head of the database department). Another internal audit manager (P35) added that "data ownership is mainly distributed between IT, information security, risk management, compliance and other business departments".

According to the IT manager (P46), data must be owned by the respective business units because "they define how data should be maintained and kept". This means that these business units have full control over their data in terms of its retention, archiving and deletion. However, the results suggest that determining the sole data owners is not straightforward since banking data is often created and used by multiple stakeholders. In this regard, IT professionals described themselves as 'enablers' and 'data custodians' whose primary responsibility is to maintain data on IT systems in accordance with relevant policies and business needs.

> IT is the enabler, for sure. So, as the information governance function is evolving, it is IT [responsibility] to provide the right solutions to run that function. Also, IT is the one that maintains the data, stores the data, and manages the data from a technical standpoint in terms of data integrity and controls, which is on systems. (P25, head of IT)

It is clear from the excerpt above that the IT department does not own data, which means that it is not responsible for collecting data from customers or ensuring its quality. According to the chief internal auditor (P24), business departments are accountable for data quality because they gather information from customers and put it in the system. Despite this, a few respondents were still adamant that data be owned by IT.

The analysis of the data showed that Omani banks have adopted a variety of models to facilitate the assignment of data ownership to different IG stakeholder groups. The most commonly used model is called RACI (responsible, accountable, consulted and informed) or the responsibility assignment matrix, which "… delineates who's responsible for what kind of data" (P14, head of information security). As mentioned by those involved, the RACI matrix allowed banks to assign specific roles –namely responsible, accountable, consulted and informed—to each employee or function involved in executing a specific data activity. Having clear roles and responsibilities can help eliminate confusion and reduce conflicts among IG stakeholders, as key data activities are well defined in the organisation's policy.

As the head of a large local bank's information security (P29) put it:

> If the [data] ownership has not been developed rightly from the beginning, [it] may cause confusion. Anyways, I always say, those confusions would be there if we did not

> have proper governance. The governance would also include the RACI matrix, which [enables] us to know all those activities in terms of accountabilities and responsibilities.

To avoid disputes related to data ownership, many participating banks have embedded the responsibility assignment matrix (RACI) into their internal policies. In light of this notion, more than half of the respondents reported that they were referring to an information security policy because, according to the chief internal auditor (P24), it “…mandates so many tasks relating to governing [of] the data and the responsibilities [of] each person … in the bank”.

This idea was supported by another IT manager (P25):

> If you look at information security policy, there is a definition related to data ownership and responsibilities. For example, customer data are owned by the respective business unit. Analytical data related to compliance; it’s owned by the compliance. The transactional data is again related to the customers; then it’s owned by the respective business. So, data ownership is spread like that.

Although many IG professionals confirmed that they knew who was responsible for data in their respective banks, they emphasised the need to map data ownership responsibilities to the job descriptions of employees. According to the head of information security (P34), employees may not be aware that they have the responsibility for managing information assets if specific data activities or roles are not assigned to their KPIs. Therefore, it was argued that banks must clearly define the roles and responsibilities of each employee before engaging them in any IG-related tasks.

Another interesting approach widely used by Omani banks to assign data ownership responsibilities is the three-lines-of-defence model. According to the interview data, the model treats data as a risk factor, and accordingly the ownership was assigned based on the location or business's exposure to data risk – i.e., risk-taking, risk oversight or risk assurance. In this case, business departments, such as customer service and IT, that deal with data daily were held accountable for managing and ensuring the quality of banking data.

To confirm this, a chief compliance officer (P42) who had previously worked in international and local banks stated:

> The three-lines-of-defence model basically assigns [data] ownership to the first line of defence. And when I say the first line of defence, I'm talking about the businesses, and they are supported by the second line of defence … [including] compliance, risk management, finance, HR …[However] the third line of defence is the assurance and it's usually the internal audit team. So, the three lines of defence is the approach that we took to define [data] ownership and accountability.

The above excerpt suggests that the first line of defence (i.e., customer-facing staff) is responsible for ensuring that customer data meets regulatory or data user requirements.

As highlighted by an experienced interviewee (P13) who previously worked in the compliance department:

> The first line of defence is absolutely responsible for capturing the data in the first place [and] to make sure that they've got all the KYC information in line with business requirements. They're doing updating and they're capturing data. So that's their responsibility.

However, a compliance department assumes a data monitoring role by identifying any gaps or inconsistencies related to data collection or data quality. Finally, internal audit professionals reported that their primary responsibility was to ensure that banks had robust controls and policies by conducting routine reviews of all information management activities performed by both the first and second lines of defence.

4.3.1.2 Policy-Setting Procedures

In terms of policy creation, a trend was noted that the information security office (ISO) took control of developing essential IG policies and procedures (mainly information protection policy, cybersecurity policy, backup policy, identity and access management, data classification scheme, information privacy, data ownership responsibilities, data masking and risk-tolerance levels). This trend or practice was prevalent across all nine banks, except Bank H, where ISO responsibilities, including policy-setting, were assigned to risk management due to the absence of a formal structure for information security within the organisation.

> There is a general policy that has been prepared and created by the Information Security Department for all employees of the bank. And then there are portions of that policy within the HR [human resources] manuals and … employment contracts of employees… So that's generally how we implement or deal with information governance within the bank. (P48, head of legal, Bank C)

While key IG policies were centrally established within an organisation-wide framework, business users were also allowed to define their own policies and data requirements. Regarding this issue, several participants from different business functions indicated that they have created separate policies to manage customer-related information and records.

For example, the head of AML (P03) stated:

> I set the policy and procedure for them [business departments] to follow with regard to data management, especially on the AML side … I tell them what kind of KYC [know your customer] information they [need to] collect … I will tell them what transaction data should be captured. So, I will give the instructions in the policies and procedures of AML-related data, but it's their job to collect the data based on these instructions.

As such, it was argued that policy owners should be responsible for updating and informing implementers of these policies when existing data requirements, such as data retention, are changed.

For example, a head of the IT core system (P47) asserted:

> At the end, the business department owns the full data on the system and we are not deciding on any retention or any policy without informing them [business departments]. If we are maintaining the data of [a certain] system, let's say 5 years in the archival system, after that we [do] a backup. [Then], we need to know the status of that data in my live system. The head or somebody from the business might [should] be reporting to us. It is not decided by IT.

The analysis of the data revealed that IG policies were jointly developed by nominated representatives from both the IT and business functions. As the IT governance manager (P19) put it, "From each department, there will be a focal point, from IT, admin[istration], operation. This is like a committee. Each one will handle and create their own department policy". This view was echoed by another IT governance specialist (P31): "We [IT governance staff] write the policies, and then we ask for input with [form] the relevant business areas. There's no point in

[for] us writing policies in isolation …”. These findings suggest that IG policies and procedures must be reviewed and approved before they are formally created or published.

This was confirmed by the head of compliance (P11) from Bank E:

> One of the main roles of the compliance department is to review all the policies within the organisation before they have been approved by the board [of Directors]. So, any approval of a policy that has to go to the board should be reviewed by our compliance department. Of course, we have to ensure that … anything related … to the rules and regulations, where the risk is there, is covered under those policies. So, you can say that we are a part of governance within the organisation.

To ensure that relevant regulatory requirements were included, some banks involved corporate legal counsel during the review process of IG policies:

> We [the legal department] interfere at the policymaking level … when these policies are made … just to make sure that everything is compliant with the applicable laws … [or] if any decisions to be made with respect to breaches … to either vet or advise. (P48, head of legal, Bank C)

However, banking data are easily accessible and often shared with various business functions; therefore, there is a need for oversight mechanisms to ensure that information is used properly.

4.3.1.3 Oversight Mechanisms

Despite the absence of a formal IG committee, the analysis of interview data revealed an attempt by most Omani banks to share oversight and supervision of IG activities with a broad range of senior executive managers and other stakeholder groups (including boards of directors, chief risk officers, information security managers, IT steering committees, management risk committees and audit committees). Shared oversight allowed banks to identify inappropriate or illegal use of enterprise data that could lead to financial or reputational risks. It was also used to ensure that IG professionals and business departments are collecting, storing and using the information in accordance with the rules set by laws and regulations.

However, interviewees generally agreed that the oversight function lies on the shoulders of the management risk committee (MRC), which has the overall responsibility of addressing any issues related to IG and data security. For example, a chief compliance officer from Bank C said, “We report to the bank risk committee. So, whenever there are issues, we report to that committee; it is a board committee. So, any issue related to AML [anti-money laundering], whether it’s data [related] or any other aspects”.

Another information security manager (P14) from Bank A added:

> We keep the MRC [management risk committee] informed on the data security aspects …to ensure data is not compromised”. According to the interview data, the risk committee consists of “… heads of departments and AGMs [assistant general managers], [who] have an oversight to … decide whatever action to do with data issues, [and how] to act on it [them]” (P34, head of information security).

In the case of international banks, however, it was reported that decisions related to data issues must be evaluated and overseen by group boards and local committees, namely risk and compliance. It is clear from the following excerpts that Omani banks applied a top-down oversight mechanism to steer critical activities related to customer data. Being a member of IG oversight groups allowed respondents across business units to express their concerns about certain data policies or practices that could create a sense of over-governance among employees.

> Almost every quarter, we conduct a steering-committee meeting […] which will have top management involvement, a minimum of C-level executive, and we have the CEO [chief executive officer] or the deputy of CEO [to] be the chairman, and [we] bring them all … the issues or the risk[s] related to data. … So basically, we do have this communication ongoing with our senior management every quarter. (P29, head of information security, Bank C)

> From the board, every three months or every quarter they [the board of directors] are discussing what is the result of [customer data update]. Give me the summary report [showing] what you have done and what is the percentage of [what] you have done. (P45, head of branch operation support, Bank C)

In addition to relying on governance committees to oversee IG activities, some participating banks have implemented oversight mechanisms at the department level to relieve the pressure on busy managers who may not be able to respond quickly to data risks or incidents as they arise. Evidently, implementing departmental oversight mechanisms not only helps banks ensure that IG professionals in a given department adhere to existing IG policies and procedures but also minimises the need for additional oversight from other parties. Department heads, especially those who are part of oversight committees (i.e., those for compliance, risk or information security and auditing) confirmed that they became more responsive to IG issues because they received first-hand information about how their employees handled information assets, enabling them to take corrective actions promptly. Having an effective departmental mechanism, as the chief internal auditor (P44) argued, can "…ensure the data is accurate and the decisions are made based on correct data".

This is not a surprising result since part of an audit's purpose is to ensure that information is accurate and complete. This was illustrated by the chief internal auditor (P21): "Wherever we see the data is incomplete or data, which is mentioned anywhere is not accurate … then we highlight [that] in our audit observation, and it goes to various levels like … the board of directors". Lastly, department heads were obliged to escalate any issues related to non-compliance with existing policies and procedures to the governance committees, as shown in the excerpts below:

> As a risk manager[s], [we] go to these [business] departments and look … [if] their daily work [is] compliant with the policies and procedures … If they are not complying, there would be a gap that we should report it to the risk committee … (P43, operational and market risk manager, Bank H)
>
> If that [gap] has not been closed, basically, there will be an escalation process, which is also defined in our policy… it depends on the criticality of the data or [the] criticality of the matter. If it's very critical, [within] one day, it has to be closed. If it's not critical, it has to escalate to the business owner. If the business owner does not really respond, it

> should be reported to the senior management, and from there, it will go to the CEO [chief executive officer], and so on. It might also go to the board level as well. So this is how we ensure those policies should be met … in order for everyone to obey [to] policy implementations rightly. (P29, Head of information security, Bank C)

4.3.2 Procedural Practices

In terms of procedural practices, the study revealed a plethora of technical and managerial activities that Omani banks adopted to ensure the proper handling of their information assets. During the interview, participants highlighted several practices related to each stage of the information life cycle, including information classification, data access, compliance monitoring, auditing, backup and retention period. They also spoke about the effectiveness of data policies and procedures in formulating these activities in their organisations. The following section discusses these practices in more detail.

4.3.2.1 Data Policies, Standards, Processes and Procedures

Data policies and procedures are considered the cornerstone of any IG programme since they set ground rules for how information is governed across the organisation. Many organisations use data policies and procedures to promote best practices in the use of enterprise data by providing employees with detailed guidelines on how to deal with various IG activities, such as data sharing and data access. However, designing effective data policies is complex, especially when the organisation is mandated to govern or retain different types of information, such as emails or customer records.

For data policies to be effective, it is imperative to consult the right stakeholders – inside or outside the organisation—in the early stages of policy development to understand the legal and regulatory landscape surrounding IG. With data requirements in mind, the findings showed that some banks (such as Bank H and Bank F) hired external consultants to assist them in either formulating or improving their data policies and procedures.

> We have a project in the way where we are improving [developing] … a new process or new policy for managing information … The consultant[s] is [are] there in the bank; they are doing a full flag review. But for sure, there will be … some missing policies or missing procedures. That's why we brought a consultant. (P19, assistant manager of assurance and IT governance, Bank F)

The analysis of the interview data revealed some data policies created by different Omani banks to manage their information assets (both structured and unstructured data). These policies include, but are not limited to, an information security policy, data retention policy, backup policy, data classification policy, data management policy, data privacy policy, user access management policy and information sharing policy. Other policies were also identified by business users who perceived them as a quick way to inform employees on how to manage and retain customer information or records. For example, the head of compliance (P05) said, "We have a KYC [know your customer] policy … so that it determines the quality of the customer information and identification of information … then again data retention, data protection, and all other purposes [requirements]". In support of this finding, the chief compliance officer (P26), who was described by his colleagues as the father of banking laws and regulations, added: "AML [anti-money laundering] data requirements are spelt out in our [compliance] policies and procedures …in order to get what you [we] want from the customer data…".

It is clear from the analysis that none of the nine banks included in this study have a specific DG policy or strategy; rather, each department seems to have its own policies and procedures. However, most participants agreed that the information security policy is the primary document used by their organisations to manage information because it covers almost the entire information life cycle, as confirmed by the chief internal auditor (P24): “We have an information security policy, which mandates so many tasks relating to governing the data and the responsibilities [of] each person … in terms of protecting the information assets of the bank”. This result may be attributed to the lack of a formal IG function in these banks.

It was interesting to note that some participating banks have developed their data policies in line with international standards and best practices, notably the International Organisation for Standardisation (ISO). For these banks, adopting international standards enables them to meet the expectations of both internal and external regulations because, according to a head of AML (P08), these standards “…reflect [data] requirements of the law, and … the best practices set out by international organisations such as the FATF [Financial Action Task Force] and others”. Also, some IG professionals expressed how international standards helped them strengthen their corporate-wide data policies and keep them updated.

> So instead of limiting ourselves with [to] independent knowledge, we have an international organisation like ISO, who [which] has clear-cut policies with a degree level, how the data should be stored, how the backup should be taken, … how the data restoration should happen, what kind of password mechanism we should follow for storing our critical server passwords, how frequently we should be changing this

> password … at the database level … So many things are there. (P39, head of database, Bank E)

Furthermore, many department heads indicated that their policies and procedures would need to be reviewed annually or even earlier if the current requirements of statutory, regulatory or corresponding banks change. According to the same participants, the policy review practice was viewed as an opportunity to raise any concerns or propose new ideas for managing information assets since it has to be reviewed by multiple departments, primarily compliance and internal auditing, before it can be approved by the board.

4.3.2.2 Compliance Monitoring

Developing an effective IG programme requires ongoing monitoring and tracking of information-related activities to ensure that employees adhere to organisational policies, industry standards and procedures. To be sure, compliance monitoring must be integrated with an organisation's audit programme performed by internal or external auditors so that IG stakeholders can obtain regular and unbiased assessments of their data compliance. The interview data of this current study indicates that compliance monitoring has received the most attention because it directly affects the bank's reputation and financial resources. As the chief compliance officer (P07) asserted, "If you think compliance is an enemy [that's] stopping the bank business, non-compliance [will lead to] penalties, [financial] losses and … bad reputation".

Undoubtedly, employees are a key element of any compliance monitoring programme; therefore, they should be aware of acceptable behaviour when dealing with enterprise information. Equally important, employees should be informed about how to seek help if they have any concerns or inquiries regarding the implementation of IG policies or procedures.

Surprisingly, while most respondents recognised the importance of employees in achieving compliance, others believed that technology is more effective than them in enforcing data policies and procedures.

This view was articulated by a head of IT (P25):

> If you depend on people, then communication and awareness are not going to be foolproof. You cannot be micromanaging everybody, whether they are sufficiently collecting the data when they're doing the transaction, etc. because people will change [For a] foolproof model, you need to modify your systems, create [data] validations. For example, account opening in our bank is all automated …You input the customer data while [when] opening an account and the system [will] define what is mandatory or optional. So people [employees] automatically follow.

This study found that some participating banks have used automated monitoring tools to detect any data violations or risks that IG professionals may cause due to non-adherence to organisational policies and procedures. For example, information security professionals said that automated monitoring tools help prevent breaches of sensitive customer information by being alerted when an existing information security policy is violated.

As noted by the head of information security (P20):

> All classified data in the bank are monitored by a data leakage prevention system. The system prevents any unauthorised or [if] you want to send this data outside because it's classified by nature, by context. There are rules and policies that have been implemented in this system to trigger if there is any unauthorised task on this information.

Auditing is another compliance monitoring mechanism implemented by all Omani banks to assess the current state of information-handling practices and to identify anomalies or issues related to data quality and data security. Ideally, auditing is conducted periodically (e.g., monthly, semi-annual, annually) by internal audit departments and/ or external auditors depending on the size and complexity of the organisation.

Chief internal auditors and chief compliance auditors agreed that data audits are paramount for banks to identify and close any loopholes in current IG practices that might prevent them from meeting their obligations at national and international levels. As part of their audit engagement, audit professionals will interview concerned employees from each department to assess their understanding of existing information policies and procedures. They will also review and inspect various facets of information management activities, such as the encryption of cardholder data and the retention schedules of customer records, to ensure that they are implemented in accordance with relevant IG policies and procedures.

This idea was nicely articulated by the chief internal audit (P44) of Bank E:

> In each of our audit engagements, we look at compliance with the policies, compliance with the standards, compliance with the regulations ... wherever we see that the data is incomplete or data, which is mentioned anywhere is not accurate, or the data does not properly represent the actual situation or the latest regulatory requirements … then we highlight [that] in our audit observation, and it goes to various levels like … the board of directors [or] senior management … [So], it is very critical that we have proper information monitoring mechanism within each department to ensure data is accurate and decisions are made based on correct data.

The findings also showed that Omani banks were subject to external auditing by the CBO and other international bodies. For some respondents, working with external auditors was perceived as a daunting task because it required them to prepare pre-audit requirements and close all gaps to demonstrate good governance practices.

> We have an external auditor, which is seen by the ISO [the International Organisation for Standarisation]. Every year, they are coming to check that controls are maintained or followed by other departments, and they question them. We have the regulatory, CBO [Central Bank of Oman], coming every year to check … and we have a national auditor, and we have a PCI DSS [Payment Card Industry Data Security Standard] auditors. This is very tedious, and it's very annoying in a good way. This means that you are making sure that your policies are followed. (P34, head of information security, Bank D)

4.3.2.3 Information Classification

Information classification can improve the security of critical data by categorising it into meaningful classification levels so that classified information is accessed only by authorised users (e.g., senior managers). In this study, classification levels were found to vary across banks, but they typically range from "highly confidential" to "public". This variation might be attributed to the subjectivity involved in this process, as "… each bank has their own way of classifying information" (P46). However, it seems that there was a consensus among participants that information stored in critical systems, such as core banking and ATMs, should be classified as highly confidential because it contains valuable information that directly affects the bank's reputation and performance:

> We classify our data [based] on the value. There is a criterion for that, we have classification guidelines. Also, we consider the regulation part, how important of [is] this data ... So, all this is part of the [information] classification [policy]. The first [thing] is the value and [then] criticality of this information. (P20, head of information security, Bank D)

Of course, classifying information requires IG professionals to understand "what kind of data they have inside the bank" (P37) so that the right classification levels can be assigned to the data. This task was perceived by most information security professionals as a 'long journey' because it required them to visit each business unit and delve into their information systems to understand the value and criticality of that information on banking operations. For these participants, the ideal way to classify information is to appoint a representative from each business unit, as they are more familiar with their information and its value to the organisation.

For example, a head of AML (P08) who applied a similar practice in her organisation, described the role of the representative as follows:

> They [information security team] have assigned a focal point in each department and that person has prepared a list of information that is being gathered by the department and kept beside it what type of classification this information should be.

The above quotation illustrates the importance of coordination and collaboration between different IG stakeholders to ensure the success of any IG activity. It also assigns the responsibility of classifying information to business owners, challenging the commonly held view that this work must be performed by information security professionals.

This conclusion was further supported by the head of information security (P34):

> So a business owner should know the value of the[ir] data while coordinating with legal also. Not only does he have to decide if this is confidential or not, but maybe it is not confidential. It might be general, but in coordination with the information security team and the policies. They have to work together to see how to classify the information.

Another head of information security (29) added that:

> … if the data owner is facing some difficulties in classifying the data, [then] InfoSec [Information security] and IT would come in handy to help them out.

The analysis of interview data revealed that some banks in this study have implemented specialised information classification systems to control and monitor their classified information. This was particularly evident among local and Islamic banks undergoing digital transformation projects. The majority of information security professionals had a positive view of the role that classification systems play in preventing confidential information from being accessed or disclosed to unauthorised users by enforcing a set of rules and policies in both structured (e.g., databases) and unstructured data (e.g., emails). For example, the following two quotes from two information security managers illustrate how these systems helped them protect and track sensitive customer information:

> All classified data in the bank are monitored by a data leakage prevention system. The system prevents any unauthorised or [if] you want to send this data outside because it’s classified by nature; by context, there are rules and policies that have been implemented on this system to trigger any unauthorised task on this information. (P20, Bank F)

> We are already establishing [a new] application. So, what this application does once there is a mutual understanding of [data] classification. I'll give you an example. In the email, [if] you try … to write a full card number and send it to someone … the application [will] detects this information, [and] it will tell you this document is confidential …[so] it will force you to click whether it is confidential or restricted, that is mandatory. (P34, Bank D)

By contrast, few participants criticised those banks that implemented data classification systems before classifying their information. They questioned how these systems could identify and differentiate between confidential and public information without being assigned the right classification level. For example, the head of IT auditing (P37), who seemed upset when he narrated his experience in this regard, said:

> Let me tell you something about [our bank]. Here, we are not allowed to share documents containing account numbers. However, I can send the account numbers via email! That's because you are not classifying your information. If you classify a bank account as confidential information, you [can] put a policy on the DLP [Data Loss Prevention] [that forces] confidential information not [to] be emailed or printed.

This bank likely has the misconception that information can be classified with the help of new technological capabilities, such as AI and machine learning. Therefore, it is important for banks to align information classification projects with the IT strategy to map solution functionalities with business expectations.

4.3.2.4 Enforce Retention/Archiving

Data retention and archiving are at the heart of the IG programme in the banking industry. This is because banking data are subject to retention requirements by laws, regulations and other competent authorities (e.g., courts, public prosecution). According to the research participants, the Omani banking law mandated that they retain electronic and physical copies of customer records for long-term or even permanently, depending on the criticality and need for that information. As evident from the excerpt below, data retention periods are typically set by each business unit as they are more familiar with recordkeeping requirements and best practices related to their function.

> As a policy, we [have to] keep all AML-related data for a minimum of 10 years. Where there are STRs [suspicious transaction reports], for example, we must even maintain this data for longer than 10 years. At any time, there can be litigation or some investigations into these cases. To provide requisite information to agencies or to the courts, we maintain data for them for more than 10 years. (P27, anti-money laundering manager, Bank D)

The findings showed that the reason some banks may choose to retain customer information beyond the specified period is not to comply with data retention obligations per se but to avoid potential penalties or fines. To this end, it was noted that many Omani banks developed their data retention policies "…in line with the regulatory, CBO [Central Bank of Oman], legal and other security standards like PCI DSS [Payment Card Industry Data Security Standard]" (P29). Of course, IT professionals play a major role in enforcing data retention policies by automating archiving and or deletion of electronic information based on the approved retention schedule.

This was particularly evident at larger banks that had more systems and products, as indicated by the head of IT core systems (P47): “We have forced all the systems to be part of the archival [solution] with a process [that] should be signed by the business”. This view was echoed by another respondent (P41): “We have created an alert … [to] be sent to application owners…This alert will inform them about the remaining space, and it will send an alert like, you almost exceeded 40 GB, and we have to archive your data”.

While some IT staff claimed that auto-archiving helped them reduce the time needed to identify and move inactive data to long-term storage systems, others argued that it created storage issues due to the excessive retention of data by business users. With the increased number of data breaches, for example, it has become extremely important for banks to retain all information security logs for future analysis or auditing. To minimise storage costs, it was suggested to archive non-critical information to a less-expensive storage media, such as tape or an external hard drive.

4.3.2.5 Establish and Monitor Access

Several participants reported that the banks at which they work had implemented robust mechanisms and technologies to detect and prevent unauthorised access to sensitive information. This was particularly evident in local banks with large customer bases. IT professionals in this study acknowledged that data monitoring systems, such as database activity monitoring, enabled them to restrict access to classified customer information by “controlling what kind of data [to be] accessed based on the … role and responsibility of users in [that] department” (P46). This finding suggests that employees within the same business unit or group might have different data access levels depending on their privileges:

> In the system, we have privileges provided to the staff. The privileges are governed by policy, so that X person should have a privilege to see only 123 and Y person will have a privilege to see 567, but not 123, depending on the requirement of the users. So not everybody has access to all the information. This depends on the requirements of the department. Access is controlled by the information security or IT [information technology] department. (P34, head of information security, Bank E)

4.3.2.6 Apply Backup Practices

Information is the lifeblood of banks, and applying backup practices can help them ensure the availability and recovery of critical information in a disaster. But data backup does not operate in a vacuum; it requires an appropriate strategy, people and technology to achieve its intended goal. The majority of IG professionals in this study reported that they had a backup policy and business continuity plan in place, which provided them with clear guidance on how to perform data backup in practice:

> We have procedures to back up our data; we have procedure steps to do that. So, we cannot lose our data because we have a BCM [business continuity management] department. They are doing tests every month; they are educating the staff [on] how to back up the data, how to maintain it in case there is any pandemic or if there is any disaster. So, every department has a role … to participate in that process. (P34, head of information security, Bank D)

The above quote suggests that data backup assurance is the responsibility of all stakeholders (both business and IT) who may be impacted directly or indirectly by data loss. In this regard, IT professionals were [given] the responsibility of implementing backup policies to ensure the availability of backup data by adopting the right technologies that could facilitate the timely restoration of information. A head of IT (P46) confirmed this through his words: "… we implement, and we've been audited by the information security team [who] have to review how much we [IT] have adhered to that policy as a backup".

It was interesting to note that some banks included in this study aligned their backup policies and procedures with international best practices:

> We have [adopted] an international standard like ISO [International Organisation for Standardisation], which [that] has clear-cut policies … [on] how the data should be stored, how the backup should be taken … [and] how the backup could be [re]stored … (P39, head of database, Bank E)

> The IT team has got something called ISO 9001 that's quality management systems which have [been] implemented in their facility … So, ISO 9001 … has built and run. The run part is mostly on [about] the IT operations where they have backup procedures and protection strategies, and they [IT professionals] have to manage [implement] that particular bit. (P22, head of enterprise risk management, Bank B)

When asked about the types of backups their institutions use, most participants mentioned a combination of incremental and full backups. This fact was clearly illustrated by a database administrator (P41):

> Yes, we perform backups. We have two types of backup here: full backup and [incremental] or t-backup … we take incremental backup, at night, daily at 10 pm. We also take full backup for all the databases on a weekly basis.

Backups should be stored in multiple locations away from the original so that the copied files are not affected by a similar disaster. The responses obtained for this study clearly indicated that the participating banks followed a 3-2-1 backup strategy, replicating data to three different locations: two on-site (e.g., tape and disc) and one remote off-site. Furthermore, it was noted that some IG professionals, especially those working in compliance departments, tend to create additional backups by storing hard copies of transactions and customer records on their premises: “We have backup for information. We have it in hardcopy … in very secured lockers not accessible by any staff from outside the department.” (P07) Regarding off-site backups, many IT professionals consider it the most effective way to ensure the continuity of banking operations because backups are automatically created and stored in a safe place.

As a database administrator (P41) said:

> We have a DR [disaster recovery] server. This DR server is stored in Oman data park. So, it is far away from our bank, so in case both nodes are interrupted, we still have backup files in Oman data parks; we can get the data from there.

Backups can help IG professionals reduce the risks of losing critical information, but they are not foolproof unless there is regular testing and verification of backups.

This concern was expressed by the head of IT auditor (P37):

> Generally speaking, in the backup process itself, the first challenge that we face is that nobody is checking the quality of the backup itself. Okay, I take backup, and I have the backup stored in different locations. It's fine, but do you check that backup periodically or not? For high-input systems like core banking, you have to check that backup every day … another challenge in that area [is that] … we don't have a test system to restore this data and test it.

4.3.2.7 Apply Data Validation Practices

The findings of this research revealed that some IG professionals, particularly those who use data, associated data validation with data quality because it helped them to "minimise the incidents of missing information". In this study, data validation refers to the practice of verifying the integrity and accuracy of data before using it in business operations. Different types of data validation practices were reported by those involved. For compliance professionals, enforcing mandatory fields at the systems level was found to be a preferred approach to validate data since it can force employees to follow a set of predefined business rules related to the type and format of data. For instance, an executive AML manager shared his experience with how data validation enhanced the quality of data in his department:

> We created multiple fields in the onboarding [also known as "know your customer"] system, and we made them mandatory so that we should get the information that we need, for example, income level of the customer, occupation of the customer, date of birth, nationality, FATCA [Foreign Account Tax Compliance Act] related information. (P27, Bank D)

However, it was argued that banks have to train their staff on the new business rules so that they can understand what parameters or data input are expected in each field.

This was clearly illustrated by the chief internal auditor (P24):

> I think that the quality of data is very much dependent on the person who is processing the application … in the system. We can put the validations around the fields. For example, this field should be a date. Now, if that date is put wrong, that system cannot detect it… A system can detect that the date entered should not be a future date, but it cannot differentiate; it cannot capture whether the date from the past being entered in this field is correct or not.

It was interesting to note that some banks in this study had implemented a 'maker-checker' process as an additional type of data validation. Participants from these banks reported that their main reason for applying the maker-checker process was not only to correct data entry errors but also to identify employees who violated information-related policies so that appropriate disciplinary actions could be taken against them. The same participants added that because they knew the data were entered by unqualified employees, they had to verify it. For example, a head of credit and market risk (P33) who had more than 28 years of working experience in both local and international banks commented:

> Highly qualified people will not be very keen to take a data-entry job. So, practically, it will be the less qualified people who will actually be doing the data entry. So, the best avenue available to the bank is having a concept … which is maker and checker. In this case, [the one] who is inputting the data will become the maker. [And] there is [will]

> somebody who is checking the data …[to] ensure that a good part of the data that goes into the system is of optimal quality.

The above quote clearly highlights the need to assign data-related activities to competent staff who appreciate the value of data. It also illustrates the importance of strengthening the role of information management function in an organisation.

4.3.3 Relational Practices

4.3.3.1 Training/User Education

User education and training appeared repeatedly throughout the interview data. The overwhelming majority of participants from all nine banks indicated that training was one of the “key pillars” in their organisation strategy. They also reported that their management had allocated a sufficient budget for training to ensure that their employees were aware of their responsibilities regarding information management and the importance of complying with applicable laws and regulations. In most of the cases studied, training started during the probationary period (usually between three and six months), where new employees are given induction courses that “instruct [them] how to deal with the information and how to save the data and how to keep the information [secure]” (P47).

Emphasising the importance of information at an early stage of the hiring process is likely to help new employees understand acceptable and unacceptable behaviour when dealing with corporate information so that they do not circumvent or ignore established policies and procedures. To be sure all employees have access to the training they need to perform their duties, the study found that most banks included in this study have established “a dedicated function within HR [human resources] division for identifying the training requirements of staff" (P33).

The responses obtained for this research clearly indicate that all employees, including the board of directors, have attended annual mandatory courses that address various aspects of IG topics, such as cybersecurity, data quality and information classification. For example, a head of IT confirmed this through his words:

> We have two main mandatory courses that have been managed by the training department. [One] is about money laundering, and the other [is about] information security, which are mandatory to all the staff to attend … In that [these] course[s], we … assure that our employees have got enough knowledge about the data classification, DG and other aspects. (P46)

Another participant expressed a similar view to the one presented above and commented: "So, in the information security training, all the various things [elements] about the master information security policy get covered there" (P44, chief internal auditor).

Interestingly, the analysis of data showed that training programmes were linked to employees' appraisals to motivate them to stay up to date with industry standards and best practices for handling information. The following quote from a senior vice president and head of information security illustrates this point:

> As part of everybody's KPI [key performance indicator], we have the learning development centre. On an annual basis, we have a special training given on information security and business continuity, and then there's an exam …which they [employees] have to pass and the passing marks is 70% and above. And if they fail,

> basically, they have to repeat it or otherwise … it [will affect] their annual KPI appraisals. (P30, senior vice president and head of information security)

By linking training to employee's KPIs, the organisation would be able to ensure that their employees have acquired the necessary knowledge and skills to manage information. It also allows the organisation to assess the effectiveness of its training programmes and determine whether additional improvement is required. This view was further endorsed by other participants who worked closely with the learning and development departments to enhance the quality of the training materials. For example, a head of information security commented: "We also track the progress whether all users have attended this training, and completed the certification programme … [and] we might tweak it [training programme] a bit" (P14).

Analysis of the data showed that most banks in this study used multiple types of training programmes to ensure that all employees had access to the knowledge and resources needed to raise their IG awareness. Participants indicated that the training programmes in their institutions varied from "classroom, online courses, [to] one-to-one coaching" (P26). According to the interview data, this variation was influenced by the organisations' goals, culture, employees' competencies and budget allocated for training. This finding suggests that the quality of IG training can be impacted by the existence or absence of certain organisational conditions.

In this study, online training appeared to be more effective and convenient than classroom or face-to-face training. Many interviewees agreed that online training enabled them to create personalised learning experiences, enabling them to access training materials anytime without being physically present. In this regard, they shared their experiences of how online platforms like e-learning helped them to continue educating their staff on various IG issues during the COVID-19 pandemic when face-to-face training was banned by the government. This view is illustrated in the following quotation:

> We have a digital platform for the training, where we have these BCP [Business Continuity Plan] related training sessions … we have something called ‘Al Bawaba’ … to train our staff because the face-to-face training is now not very much feasible amid this COVID-19 [pandemic]. So we have digital tools to train the staff, which I think is the most effective and the most usable in this kind of situation. (P24, chief internal auditor)

4.3.3.2 Communication/ Idea Exchange

Analysis of interviews showed that effective communication improved transparency, understanding and trust among IG professionals by providing them with clear and consistent information, fostering open dialogue, collaboration and ideas exchange. In this study, the theme of communication was prevalent across all nine case studies, but it was particularly evident in local and specialised banks. Interestingly, several participants associated communication with information culture, suggesting that it could raise awareness among all employees by keeping them informed of any changes or updates about information policies and procedures. Therefore, they perceived communication as “nice stuff” because it connected different IG Groups (both IT and business) thereby ensuring everyone is working towards the goals of information governance. To be sure, most of the banks in this study employed a top-down message approach by which a senior leader and/or responsible party, such as an HY department, communicated the organisation’s goals and policy changes to all stakeholders. The following quotation, for example, reflects this point:

> There are two levels for that [communication]. The first is on a bank-wide level. HR [human resources] is doing a great job in terms of sending emails and keeping employees up to date in terms of policy changes. That’s one thing. The second thing is always at the departmental level … meaning that the head of that department or division … would [review] and send the updated policy to the team and the team has to acknowledge that, whether by email or by signing an acknowledgement … and then give it back to his line manager. (P48, head of legal, Bank C)

There are several possible explanations for this result. First, keeping all employees informed about changes or updates to IG policies and procedures demonstrates that the organisation values transparency and open communication, which in turn could improve collaboration across all business units. In this case, employees may feel more comfortable asking questions and sharing feedback with the responsible person or department, helping them improve their policies and procedures to better serve the organisation’s goals. Second, when policy changes are communicated to employees through their line managers, this means that they are accountable for ensuring their employees understand and comply with the new policies.

The majority of participants in this study reported that their organisations used a variety of communication methods to disseminate relevant IG information to their employees, including emails, posters, infographics, social media, meetings, text messaging and intranet websites. Based on the analysis of data, it was noted that these communication methods varied across banks based on their size, organisation structure, type of information being shared, culture and employees' preferences. That said, larger banks with complex organisational structures were found to rely more on emails and other digital tools (such as text messaging) for communication, while smaller banks tended to use face-to-face meetings.

Despite this variation, the participants agreed that emails were the most secure method for communicating critical and sensitive information with their employees. For some IT and information security professionals in this study, emails allowed them to encrypt and control access to sensitive information so that they could ensure that it was delivered to the intended recipients. They also added that emails provided them with 'evidence' or a record of communication that could be used in a dispute, or if an employee denied receiving specific information related to IG. For example, the following quotation from a database administrator reflects this idea:

> Basically, we are using Outlook emails. Sometimes we use Microsoft Teams, but for the critical things [information], we are using emails, because for example, if something happens, then at least we have evidence, we have an email to show to our managers … also, [if] someone says no, I did not receive it, or I didn't see [it]. In this case, we have mail evidence. (P41, Bank C)

Similarly, another participant reported that his bank used email to educate and inform IG professionals about potential cybersecurity threats by creating visuals, such as posters or infographics, and emailed them to stay cautious:

> We do these posters [and] infographic[s] … which are sent as an email to everybody [employees]. Sometimes, when we see a threat level increasing, we will send an email

> saying that you know what, you need to be careful, things are not good. This is one activity that … can protect the organisation. (P22, head of enterprise risk management, Bank B)

Despite the consensus that email provides IG professionals with an efficient and convenient means of communication, a few participants argued that it is not as effective as face to face “because we are human, and based on our culture, we’d like more interaction” (P40). This argument suggests that people, by their nature, tend to learn and understand information through social connections and interactions with each other rather than through solitary or individual learning. Indeed, the desire to interact with others can be influenced by the culture or social norms in which a person is raised and the values or beliefs emphasised in that culture. For example, the cultural and social norms of Oman place a strong emphasis on building and maintaining relationships with others, which may influence an individual’s preferences for communicating within an organisation.

This view was illustrated by a chief internal auditor:

> I am one of the strong believers in [of] the weekly meetings … where you [we] basically discuss key elements, such as information, data quality and strategic goals. Weekly meetings for me are the best approach to educating staff. But that doesn’t limit you from using internal communication channels such as emails … It doesn’t limit you from using magazines … weekly team meetings are the best way to have that information spread across and refreshed from time to time … [because] the more you talk about it [something], [the more] it sticks in their [employees] mind. (P42, Bank B)

Therefore, it is important for the banks in this study to employ a combination of communication methods to ensure that relevant IG information is received by all employees. By doing so, banks can reach employees more quickly and efficiently, which can improve their responsiveness to regulatory changes or policy updates and thereby avoid costly fines and penalties.

4.4 Consequences of Information Governance

The results of this study showed that the adoption of IG practices in Oman banks has led to various intermediate performance effects and mitigation.

In the context of this current study, intermediate performance effects refer to immediate or short-term results that can be observed immediately following the implementation of IG practices in an individual bank. These effects may have positive impacts on specific aspects of the bank's performance, such as productivity, efficiency and customer satisfaction. Conversely, risk mitigation is defined as the process of reducing potential losses or negative consequences associated with the use of information in banks. According to the results of this study, this may include a reduction of ML risks, improved assessment of credit risks and enhanced compliance with laws and regulations. Unlike intermediate performance effects, however, risk mitigation is a long-term goal and may not be visible in the early stages of IG implementation. Further discussion about these consequences is provided in the following sections.

4.4.1 Intermediate Performance Effects

The analysis of interview responses regarding the consequences of IG practices in the Omani banking industry revealed a range of intermediate performance effects that often reflected the environment or type of business in which the bank operates. When asked about the potential benefits that can be derived from the implementation of IG practices, the majority of participants from different banks reported several performance effects, as follows:

4.4.1.1 Improved Operational Efficiency

First, the findings of this study showed that effective IG practices can improve the efficiency of business operations by providing timely access to information, reducing errors and increasing employees' productivity. For example, compliance professionals spoke of how ease of access (having the right information at the right time) led to reduced time needed for collecting KYC information from different departments, which in turn reduced the workload of employees and made them more focused on the analysis and actual risks. They also talked about how accurate and relevant information helped them reduce the number of false-positive alarms by improving their monitoring system and response times to any potential issues.

In IT, information governance is associated with reduced costs of data storage by implementing data retention and archival policies, whereas in information security, IG practices are associated with better prediction of cybersecurity attacks and better business continuity planning. In a similar vein, the audit professionals in this study acknowledged that the availability and accessibility of information helped them reduce the time spent on auditing assignments, which in turn resulted in the generation of accurate and timely reports. The following quotes from different groups of IG professionals provide further evidence of how IG practices have positively impacted the performance of the Omani banks included in this study.

All of this information helps the AML [anti-money laundering] department to function better, our monitoring system will function better, and our analysis results will be up [go] to a high level. [Also] reports issued to authority like a FIU [financial intelligence unit] will be [in] high quality and contain good information about the customers …[therefore] the load of work will be less, the number of transactions we need to monitor will be reduced. [P07, chief compliance officer, Bank F]

I think we will be very highly efficient in terms of AML [anti-money laundering] by deducting all suspicious transactions because the data is under the same umbrella and everything is in one place and assessment will be very easy and it will be controlled very well. Better than if it is split into other systems. [P47, head of IT core systems, Bank A]

When we collected the data from the different systems and stored them in a single data hub, we built dashboards and reports; we could track a single transaction or a single service across different platforms. And that could help us to have better monitoring, better insights into the errors and mistakes where they may fall, and to fix the root cause… [P40, data analytics manager, Bank C]

Our audit becomes far more focused on the areas where there are problems ... So, yes, the data [governance] impact a lot on audit work. And we are changing the process of how we collect data and from which source we get the data. So, let’s say, for example, I ask for loan data from the department, whether it’s business or operations, now, I can access the data directly from the system and do my own analysis to find out which are the problem areas … so many benefits are there. We can save a lot of time in auditing if

> we get the correct data and timely for our analysis. We can do better data mining; we can do better analytics. And in the end, with less time, add more value to the organisation. [P44, chief internal auditor, Bank E]

4.4.1.2 Improved Customer Service

Second, the study found that effective IG can significantly improve customers' satisfaction by providing more personalised products that meet their needs. It was not surprising to note that most participating banks in this study attribute their success to the quality of services provided to customers since they are the main source of their profits. However, the research participants from specialised banks (namely Bank H) did not comment on the topic under discussion. This is perhaps because these banks do not provide banking services like other commercial banks but rather provide a few products tailored for specific people like entrepreneurs.

In most of the case studies, data was seen as a "gateway" to understanding and analysing customer behaviour, enabling banks to better serve customers by cross-selling and offering customised products that meet the specific needs of different customer segments. Of course, without a 360-degree view of customer data (e.g., address, income, occupation, credit score or transaction history), it would be difficult for banking institutions to deliver a consistent and excellent customer experience across all segments.

This idea was supported by an executive AML manager:

> [The] more information you are having about the customer, the better you will serve the customer … [because] if we have relevant and accurate information, we will be in a better position to serve the customers. We will be in a better position to know the

> needs and wants of the customer. So, we can design the products according to the requirements of customers. [P27, Bank D]

During the interviews, several IG professionals from different business units highlighted some evidence of how information governance enhances customer experience in their respective banks. For example, retail banking professionals in this study indicated that easy access to credit card usage allowed them to analyse and upgrade some customers to a higher-level card type, such as “premium or elite cards”, which provided cardholders with exclusive discounts and rewards, including access to airport lounges.

Another interviewee from risk management added that “we also see if the customer is eligible for a loan or a credit card based on his salary…so if he opts for this kind of credit card …he [will] get a cashback of 1% to 2% so the customer also benefited” (P14). Based on what has been presented so far, it is clear that Omani banks could improve customer service if they provide their IG professionals with accurate, complete and easy access to relevant customer data.

4.4.1.3 Improved Data-Driven Decision-Making

Third, the findings of this study revealed that implementing effective information governance practices can play a critical role in improving decision-making in banks as IG professionals were able to make informed decisions based on accurate, complete and relevant information. Among other groups of participants, compliance professionals appeared to be more impacted by the availability and quality of customer data, which caused some to view it as the “building block” for making business decisions in their departments. As a head of compliance put it, “The data is the core activity that we do. Because of data, we can make a decision. But in the absence of data, it’s not clear what decision we can take” (P09). This finding is not surprising given that compliance departments rely heavily on reliable data to make decisions related to opening accounts, filing suspicious activity reports and/or denying transactions.

Analyses of the interviews suggest that having the right information at the right time accelerated the decision-making process, enabling compliance professionals to make quick decisions about whether to close or report a suspicious transaction to a higher-level authority, such as FIU]. The following quotation illustrates this point and highlights how the adoption of some IG practices, including data validation and data cleansing, has led to improved compliance-related decisions:

> We do data cleansing, update customer information, enforce sometimes mandatory fields … All this information [practices] helps the AML [anti-money laundering] department to function better … The decision of whether to take this case or transaction to a higher-level authority becomes easy and faster. [P07, chief compliance officer, Bank F]

Despite this view, it was argued that implementing IG practices can slow down decision-making because, according to the head of IT governance, “having [information governance] means you’re adding controls, which means that you’re adding more layers for the business to take decisions” (P32). Later in the interview, however, the same participant retracted his statement and commented: “If I am the compliance chair, I would be happy to know that I have next to my door a strong DG that is creating very valuable decisions about data”. There seems to be a paradox here, which can be attributed to the following reasons.

From the technical point of view, adopting IG practices may indeed require employees to follow a set of rules, policies and procedures for accessing, using and sharing enterprise information. For some business users, these processes can be seen as time consuming and slow down their decisions. Again, the realisation of IG benefits on decision-making might not be obvious to those (e.g., IT professionals) who are responsible for ensuring the availability of information rather than using it for business decisions. It is, therefore, important for banks to communicate the potential value of IG to all employees to recognise its critical role in improving decision-making.

4.4.1.4 Improved Data Quality

Fourth, the majority of studied banks reported a significant improvement in their data quality following the implementation of IG practices, particularly data validation, compliance monitoring, auditing, oversight mechanisms and training. In their interview responses, participants used the words “reliability”, “accuracy” and “integrity” to demonstrate the positive impacts of IG on data quality. In her words, for example, a head of information security (P20) said, “Information is the hub of the organisation and governing it will not cause any issue in the bank. It’s the other way, it will benefit, it will have [the] right information, accurate information”.

Another banking surveillance manager (P38) from a regulatory bank supported the previous statement and added, “On the top of that, errors [that] take place due to manual exchanging of data will become less”. Obviously, IG professionals who work in critical business units, such as compliance and legal units, must rely on high-quality data to make informed decisions. Interestingly, some compliance professionals in this study indicated that their ability to identify suspicious transactions and/ or high-risk customers has been enhanced as a result of the increased quality of KYC data. However, the same participants highlighted the need for more efforts from branches and KYC analysts to capture accurate and complete customer information in accordance with established data quality policies and procedures.

For example, a head of transaction monitoring noted:

> If the operation staff does not state [collect] the KYC details correctly, if the branch also does not take the full details from the customer, this will impact the data quality, which in the end will lead to a violation from the CBO [Central Bank of Oman]. (P12, Bank C)

The above quotation suggests that employees play a significant role in the implementation of IG in banks, as their ability to collect and store information in line with current regulatory requirements, such as KYC and CDD, would lead to improved data quality and thereby avoid potential regulatory penalties.

4.4.2 Risk Mitigation

Additionally, the IG professionals in this study were asked about their views on the role that information governance plays in mitigating information-related risks in their respective banks. Views obtained from the interviews varied by the banks and business units in which the participants worked. Analysis showed that the impact of IG practices on risk management was evident in all nine banks, except Bank G (an international bank) where the situation appeared to be blurry due to the absence of explicit evidence. A possible explanation for this might be that Bank G has different goals or metrics, such as improving customer satisfaction and reducing costs, for measuring the success of IG implementation, which may take precedence over reporting its impact on risk management. More discussion about the effects of IG on risk mitigation is presented in the following section.

4.4.2.1 Mitigated Money-Laundering Risks

The findings of this study revealed that effective IG can play a critical role in mitigating the risks of ML in banks by improving the efficiency of AML/ compliance departments in identifying, detecting and monitoring suspicious transactions. Compliance professionals repeatedly mentioned that "data is a core component in preventing financial crimes like ML [money laundering]" (P04) because it helped them to "assign the correct risk level [i.e., high, medium, low] to the customer" (P07). The same participants believed that their ability to monitor and reject illicit transactions from high-risk customers would be enhanced if they had timely access to relevant KYC information.

This is illustrated in the following quotations by two compliance/AML participants:

> I think we will be very highly efficient in terms of AML [anti-money laundering] by deducting all suspicious transactions because your [our] data is under the same umbrella and everything is in one place and the assessment will be very easy and it will be controlled very well … So if we have one single unit of governance and everything is in one place, it will be very helpful because there will be one pool for addressing the risks. We don't need to go into each system and create rules based on each system, which makes it very difficult to deduct [detect] any suspicious transactions. [P05, head of Compliance, Bank G]

> If I have this information, I can basically reject accounts for [from] known money-laundering offenders; I can reject their accounts because I know these customers may

> try to launder money through me. So, the more information there, the better I can do my duties and protect the institution and the country as a whole. [P03, Chief Compliance Officer, Bank A]

The quotations above reveal a mixed view of how compliance professionals perceive the role of IG in increasing their capabilities in detecting ML cases. By having a centralised data repository like data warehousing, compliance and AML officers would be able to get a 'helicopter' or 'holistic' view of all customer data, enabling them to identify unusual behaviour and patterns that deviate from normal customer activity, such as depositing large sums of money or making frequent transfers to high-risk countries. However, some IG professionals argued that "without strong data capturing capabilities and strong information systems in place … it's [will be] very difficult and tedious to mitigate the compliance risks" (P24). Therefore, it is important for banks to align their data strategy with IT to ensure that the right technologies and systems are acquired to collect and analyse data.

Also, participants spoke about AML data requirements [such as customer identification records and source of funds] that banks need to collect to prevent fraudulent activities related to ML. They believed that the ability to comply with these requirements embedded in a bank's policies and procedures would significantly reduce the number of false positives by enhancing the accuracy of AML monitoring systems. This means that the compliance officers will become more focused on 'real' suspicious transactions, allowing them to put more controls and measures to avoid their risks.

For instance, a head of transaction monitoring at a large local bank stated:

> The opportunity to me is if we collected the right KYC data and take policies and procedures seriously from the frontline until the CEO [chief executive officer]. If that happened … we could fight 80%–90% of money laundering …We will reduce the risk on the bank from an AML perspective. [P12, Bank C]

Overall, an IG programme can play a vital role in mitigating the risks of ML by ensuring the integrity, accuracy and availability of customer information. When implemented properly, it can help compliance professionals to effectively detect, monitor and report suspicious transactions and thus protect the bank from financial losses or compliance risks associated with ML.

Chapter 5: Cross-Case Analyses

5.1 Introduction

This chapter presents the cross-case analyses (stage two) of this current study. It aims to synthesise and compare findings from eight banks (cases) to identify their similarities and differences in relation to their antecedents, IG practices and consequences. Each bank was thoroughly examined by analysing respective interview data and relevant documents, including annual reports, and bank's policies and procedures, to understand how different contextual factors/conditions can influence the adoption of structural, procedural, procedural and relational practices in each organisation. A detailed explanation of each case study, including its mission, products, key characteristics, organizational structure, and internal conditions, is provided in Appendix 7.

5.2 Overview of the Case Classification

To facilitate the cross-case analysis, Tallon et al.'s (2013) framework was used as a baseline to categorise banks into distinct groups based on the maturity of their IG practices—i.e., structural, procedural and relational. Each practice was qualitatively assessed using nominal codes to reflect the level of implementation. In this study, the codes 'F', 'P' and 'N' were used to signify for 'full, 'partial', and 'none' implementation of IG practices, respectively (see Table 14). For instance, a bank may be assigned a "P" code in its information classification practices if it has an information classification policy in place, but it is inconsistently applied across different departments.

To be more objective in assigning the nominal codes to IG practices, frequency counts/data prevalence were extracted from NVivo and cross-referenced with the researcher's assessments. The combination of empirical data and the researcher's judgements enhances the reliability of case classifications by providing a more transparent and evidence-based approach. The assessment of IG practices resulted in three groups: (1) advanced IG (AIG), (2) intermediate IG (IIG) and (3) basic IG (BIG). Similar groups/maturity levels were reported by Proença et al. (2016) and ARMA International (2007).

As shown in Table 14 below, the theoretical framework seems to be biased towards procedural practices as evidenced by the number of practices being emphasised as compared to structural and relational practices. This was also confirmed by the frequency counts of the procedural practices (n = 550), which accounted for more than double the total governance practices (n = 978). The emphasis on procedural practices suggests their critical role in the overall evaluation of IG practices across different banks. Therefore, the following criteria were developed to classify banks into three different groups:

- Advanced IG (AIG): Banks that have more "F" codes in their procedural practices. This group includes Case 1 and Case 7.
- Intermediate IG (IIG): Banks that have a mix of "F" and "P" codes in their procedural practices, with "F" codes being predominant but not overwhelming. This group includes Cases 2, 3, 4, 5 and 6.
- Basic IG (BIG): Banks that have a mix of "P" and "N" codes in their procedural practices, with few or no "F" codes. This group includes Case 8 only.

The AIG Group comprises banks that have fully implemented IG practices in their business processes to such an extent that compliance with an organisation's policies and legal and regulatory requirements is routine. In contrast, the IIG Group comprises banks that have met the minimum IG requirements, with some areas requiring further improvement. The BIG Group is characterised by the absence of formal IG practices, which makes banks vulnerable to high risks due to noncompliance with relevant laws and regulations.

IG Practices		Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8
Structural Practices	Data ownership responsibilities	F	F	F	P	P	P	F	P
	Policy-setting procedures	F	F	F	F	F	F	F	P
	Oversight mechanisms	F	P	P	P	P	P	F	P
Procedural Practices	Data policies, standards, processes and procedures	F	F	F	F	F	F	F	P
	Compliance monitoring	F	P	F	F	F	F	F	P
	Enforce retention and archiving	F	F	F	F	F	F	F	P
	Classify information by value	F	F	P	P	P	F	F	N
	Establish and monitor access	F	F	F	P	F	F	F	N
	Apply backups practices	F	F	F	F	F	P	F	P

	Apply data validation practices	F	F	F	F	P	F	F	N
Relational Practices	User education/training	F	F	F	F	F	F	F	P
	Communications/ ideas exchange	F	P	P	P	F	P	F	P
	Collaboration among stakeholders	F	N	F	F	P	N	F	P

Note: "F" indicates 'full' implementation of the practice, "P" represents the 'partial' implementation of a practice, and "N" indicates 'none' implementation of the practice

Table 14: Cross-Case Analysis of IG practices across eight banks

5.3 Similarities and Differences of the Cases

5.3.1 Antecedents of Information Governance

A comparison of the AIG, IIG and BIG cases enables an understanding of the antecedents that account for the differences in the IG-maturity level across the three groups. The attainment of IG maturity is preceded by a combination of internal and external factors that create an enabling or inhibiting environment for the development of IG practices in an organisation. The subsequent section provides a detailed exploration and analysis of these factors.

5.3.1.1 IG Enablers

A cross-case analysis of antecedents revealed a variety of enabling factors that facilitated the development of IG practices across the eight banks. Table 15 shows the prevalence/ frequency counts of these enabling factors.

IG Enablers	Case 1 (Local)	Case 2 (Local)	Case 3 (Local)	Case 4 (Local)	Case 5 (Local)	Case 6 (Islamic)	Case 7 (Foreign)	Case 8 (Specialised)
Regulatory compliance	13	12	20	19	8	16	13	3
Information growth rate	11	16	27	24	22	17	7	8
New information technologies	16	11	14	9	16	7	10	2
Senior management support	9	8	19	11	12	15	10	1
Organisation/ IT strategy	8	15	14	16	15	8	4	3
Customer gathering information	13	1	9	17	5	7	8	2
Information culture	8	4	12	16	11	5	5	0
Organisation/ IT structure	3	2	5	3	4	3	1	0
Funding availability	5	3	5	3	4	3	6	0
IT infrastructure	2	1	2	1	1	2	1	1
Data integration	3	2	9	0	6	3	2	0
Stakeholder engagement and support	3	3	3	2	4	2	3	0
Experienced employees on IG	2	3	3	1	3	4	5	0

Table 15: Frequency counts of IG enablers across the eight banks

As shown in the table above, AIG's cases have more enablers as compared to the IIG and BIG groups. Cases 1 and 7 demonstrated a good understanding of the internal and external factors that could enable them to achieve a high maturity of IG practices. However, IIG cases have complied with most of the enablers, but according to the interview data, they need to deal with funding, customer information gathering and senior management support to attain a higher level of IG maturity. Conversely, the BIG Group had failed to meet the expected level of IG maturity due to the absence of critical enablers necessary for IG adoption, such as funding availability, senior management support, information culture, Organisation/ IT structure, technology, data integration and IG expertise.

Despite differences in IG enablers, all groups recognised the importance of regulatory compliance in adopting IG practices within their organisations. The cross-case analysis showed that AIG cases are highly proactive in addressing relevant regulatory requirements, such as AML and KYC regulations. They see laws and regulatory requirements as critical enablers for enhancing their data collection and data management practices. As such, data-related requirements were fully integrated into their internal systems, policies and procedures. On the other hand, regulatory compliance is viewed similarly across different IIG banks. The five banks considered legal and regulatory requirements to be enablers for IG adoption, with an emphasis on their role in enhancing their IG policies and procedures. Like the AIG Group, the IIG Group used systems to ensure compliance with both national and international regulations (e.g., FATF and PCI DSS).

Conversely, the BIG Group showed a basic understanding of regulatory requirements, focusing solely on implementing the minimum requirements of local laws (such as CBO laws) without putting any effort into adhering to relevant international laws (e.g., FATF). This may be attributed to their perception that ML does not pose risks to their banks since they are dealing with a small number of customers.

5.3.1.2 IG Inhibitors

Cross-case analyses revealed several inhibitors hindering the development of IG practices across the studied banks (see Table 16). While these inhibitors are somehow similar, their impacts on IG maturity vary based on the specific conditions and capabilities of each bank. For example, the analysis showed that the AIG Group has managed to mitigate and overcome many of the challenges by leveraging its organisational capabilities to improve various IG practices. However, there are a few inhibitors that the AIG Group has not managed effectively, including data quality issues and a lack of data integration. The IIG Group, however, reported more inhibitors compared to the AIG Group, with some inhibitors particularly prevalent in this group. Examples of these inhibitors are ‘resistance to change’, ‘lack of adherence to existing policies and procedures’, ‘lack of effective IG training’ and ‘lack of communication and collaboration’. The presence of these inhibitors across the IIG’s cases can be attributed to a lack of awareness of the importance of information, coupled with insufficient support from senior management. Lastly, it was noted that the BIG Group faced a significant number of challenges, which limited its ability to develop effective IG practices. The only inhibitors that have been addressed well by the BIG Group include product complexity and mix. This can be explained by the limited number of products and services offered by the BIG banks to their customers.

IG inhibitors	**Case 1 (Local)**	**Case 2 (Local)**	**Case 3 (Local)**	**Case 4 (Local)**	**Case 5 (Local)**	**Case 6 (Islamic)**	**Case 7 (Foreign)**	**Case 8 (Specialised)**
Data quality issues	14	7	28	13	5	16	3	7
Lack of clear policies and procedures	7	8	24	8	6	19	2	9

Lack of data integration	10	5	11	8	16	12	3	4
Lack of IG awareness	7	6	24	11	5	5	2	10
Legacy IT systems	2	2	5	10	6	4	2	3
Lack of expertise in IG	1	7	11	6	6	6	1	2
Budget constraints	3	4	13	9	6	12	1	1
Lack of clear roles and responsibilities	1	1	5	3	3	5	1	2
Resistance to change	0	3	7	2	2	3	0	1
Lack of adherence to existing policies and procedures	0	1	2	2	3	4	0	5
Lack of effective IG training	0	1	3	4	1	2	0	2
Lack of effective communication / collaboration	0	2	3	1	2	1	0	2
Product complexity/ mix	3	1	4	2	1	1	0	0
Lack of senior management support	0	0	1	1	1	0	0	3

Table 16: Frequency counts of IG inhibitors across the eight banks

5.3.2 Information Governance Practices

5.3.2.1 Structural Practices

The cross-case analysis revealed different maturity levels of structural practices across the eight banks, as shown in the below table.

Structural Practices	**Case 1 (Local)**	**Case 2 (Local)**	**Case 3 (Local)**	**Case 4 (Local)**	**Case 5 (Local)**	**Case 6 (Islamic)**	**Case 7 (Foreign)**	**Case 8 (Specialised)**
Data ownership responsibilities	19	10	23	20	13	16	5	6
Policy-setting procedures	6	4	12	4	9	4	2	4
Oversight mechanisms	5	1	11	8	6	2	2	4

Table 17: Frequency counts of structural practices across the eight banks

The cross-case analysis revealed that the AIG group has demonstrated higher maturity in their structural practices as compared to other groups. Analysis of Cases 1 and 7 indicate that the advanced IG group had established clear lines of roles and responsibilities through the implementation of a new organisational structure. This organisational structure has a dedicated IG department responsible for promoting a culture of accountability across all levels by explicitly assigning data ownership responsibilities to specific employees or teams. This department is also responsible for formulating IG policies and procedures, ensuring that data ownership responsibilities are strictly followed throughout the organisation. Both cases used the responsibility matrix (RACI) and job descriptions to ensure that all employees and departments understood their IG roles and responsibilities. Additionally, a review of internal documents (namely CG and annual reports) revealed a strong responsibility culture in both banks, starting from the board of directors and cascading down to the executive management, departmental heads and employees. This can be attributed to effective corporate strategies across the AIG banks, which place accountability and responsibility at the centre of its pillars.

Moreover, the analysis showed that a clear governance structure enabled the banks of the AIG Group to strengthen their oversight mechanisms by delegating oversight responsibilities to high-level governance groups and other steering committees. Cases 1 and 7 have dedicated committees for information governance, enabling them to oversee and supervise strategic IG initiatives by reviewing and approving proposed plans, objectives and policies to ensure they are aligned with the organisation's strategy and regulatory requirements. Also, the governance structure of both cases has clearly defined the oversight responsibilities in their policies and procedures, segregating them from day-to-day governance activities.

In contrast, the IIG Group showed an intermediate level of structural practices. Evidence from the data suggests that IIG banks have used the three-lines-of-defence model to assign data ownership responsibilities. They also embedded these responsibilities in their internal policies and procedures. Despite this, a conflict among different business departments regarding data ownership responsibilities was reported by some IIG banks (e.g., Cases 2 and 3). This conflict might be attributed to the absence of a formal IG structure, which results in conflicting and overlapping roles and responsibilities.

Policy-setting procedures are also well established in the IIG Group, supported by effective collaboration among IG stakeholders. IIG banks have a dedicated department responsible for creating and reviewing policies and procedures by coordinating with different business departments. They also maintained clear policy ownership, where each department is held responsible for developing and reviewing its policies and procedures as per the relevant laws and regulations. Unlike the AIG Group, however, the IIG Group has no dedicated IG committee to oversee information-related issues; rather, oversight responsibility is distributed among different committees, including the information security committee, IT steering committee, and risk management committee. A possible explanation for the absence of a dedicated IG committee could be the lack of awareness of IG benefits, which may result in insufficient support from senior management to invest in this area.

Conversely, the cross-case analyses revealed that Case 8 in the BIG Group performed the poorest in structural practices compared to the other cases. One of the key gaps identified is the lack of clear assignment of data ownership responsibilities coupled with the absence of critical IG roles, such as information security officers. Unlike the AIG and IIG Groups, the BIG Group has no department for information security, forcing it to delegate such responsibility to nonspecialised employees, such as internal auditors and risk managers. The interview data identified three key inhibitors that contributed to this problem: (1) lack of clear roles and responsibilities, (2) budget constraints, (3) lack of senior management support and (4) lack of IG awareness.

Gaps also exist in policy-setting procedures. The interview data showed that the BIG group lacked a clear and effective mechanism for developing IG policies and procedures. This practice is hindered by the absence of some IG positions, such as ISO, which play a critical role in facilitating and overseeing the policy development process. Furthermore, conflicts and a lack of effective collaboration among employees adversely affect the development of IG policies and procedures.

Moreover, the analysis showed that Case 8 had no dedicated IG committee or oversight mechanisms. The presence of inaccurate data (and consequently, unreliable reports from information systems) indicate that the bank has failed to implement effective measures to oversee the activities of the employees. According to the interview data, the lack of senior management awareness of the importance of IG and its impact on firm performance and compliance makes them less inclined to establish and invest in such committees.

5.3.2.2 Procedural Practices

Analysis of the procedural practices across the eight cases revealed both similarities and differences in how these banks manage their information over their life cycles. As shown in Table 18 below, the frequency count of specific procedural practices, such as data policies, standards, processes, procedures, compliance monitoring and enforced data retention/ archiving, varied significantly across the cases, which suggests different levels of emphasis and IG maturity across the banks. These variations could be attributed to several factors including regulatory pressures, organisational priorities and resource allocations.

Procedural Practices	**Case 1 (Local)**	**Case 2 (Local)**	**Case 3 (Local)**	**Case 4 (Local)**	**Case 5 (Local)**	**Case 6 (Islamic)**	**Case 7 (Foreign)**	**Case 8 (Specialised)**
Data policies, standards, processes, procedures	9	12	28	20	16	15	5	5
Compliance monitoring	12	2	14	6	7	10	3	2
Classify information by value	16	9	14	4	4	9	12	0
Enforce retention/ archiving	10	4	13	6	7	7	11	2
Establish and monitor access	15	4	12	2	8	8	13	0

Apply backups practices	5	5	9	4	7	6	2	4
Apply data validation practices	4	2	8	8	1	7	1	0

Table 18: Frequency counts of procedural practices

Despite their differences in IG maturity, all eight cases demonstrated a commitment to developing effective information policies and procedures. A review of interview data and internal documents revealed that both the AIG and IIG Groups had established a comprehensive set of IG policies and procedures that adhered to industry regulations, business requirements and international best practices. These policies and procedures were collaboratively developed with several business departments (e.g., IT, information security, legal and compliance) to ensure that all data requirements were accurately captured and documented. This reflects the compliance culture and interdepartmental collaboration within the AIG and IIG Groups. However, the BIG Group emerged as lacking effective policies and procedures. The interviews revealed that the group does not currently have information security and KYC policies. The absence of these policies can be attributed to the lack of awareness of the risks associated with data breaches and AML, insufficient regulatory pressure, ineffective collaboration among key stakeholders and staff shortages who may prioritise other areas of business operations over the establishment of these policies.

Additionally, cross-case analyses showed that the AIG and IIG Groups had implemented a strong compliance monitoring system supported by advanced information technologies, experienced compliance professionals and continue oversights/ auditing. As part of their digital transformation initiative, the executive management of the two groups has allocated a significant budget and resources for improving their compliance monitoring capabilities by leveraging new technologies such as AI, machine learning and big data analytics. By leveraging new technologies, the compliance functions of these banks were equipped with real-time monitoring and alerting services, allowing them to detect any anomalies or compliance violations that deviate from predefined rules, policies and regulations. Unlike the AIG and IIG Groups, the BIG Group seems to have partially implemented compliance monitoring requirements. Evidence showed that Case 8 of the BIG Group used traditional and manual processes for detecting compliance issues by assigning this role to the operational risk manager who conducts periodic checks on departments to ensure they adhere to internal policies and regulatory requirements. This approach, while valuable, may not capture all compliance risks due to its infrequent nature and reliance on human intervention. Therefore, banks within this group would need to invest in and adopt automated monitoring tools to increase their capacity in this area.

Data retention, archiving and backups are other procedural practices that are similar across the eight cases, albeit the variations in the level of implementation. All banks included in this study recognised the importance of retaining both physical and digital copies of customer information to comply with relevant laws and regulations. Analysis of documents reveals that all banks have a data retention policy in place, with clear references indicating the duration over which data should be retained. According to the interview data, all banks store customer data for a minimum of 10 years to ensure that data are available in case the Central Bank or other regulatory authorities require it.

On the other hand, the cross-case analysis revealed some differences in procedural practices across the studied banks. Among these practices is information classification. While some banks employ detailed classification schemes that classify data based on sensitivity and regulatory requirements, others have used more simplistic classification schemes. In their information classification policies, for example, Cases 1 and 7 of the AIG Group have provided clear instructions to their employees on how to classify both structured and unstructured data into different classification levels (i.e., confidential, public, private and highly confidential). To be sure, employees within the AIG Group were assigned clear roles and responsibilities, enabling them to understand and fulfil their data classification roles. The differences in classifying information across cases might be attributed to varying levels of awareness of data security, resource availability and expertise.

5.3.2.3 Relational Practices

The AIG cases demonstrated a high level of maturity in the relational practices, particularly in the realms of training, communication, and collaboration among key stakeholders. The cross-case analysis revealed that these practices had been improved due to the presence of certain conditions or factors. These include organisational culture, senior management support, budget availability, technology, talent management, and clear roles and responsibilities. However, it should be noted that these factors are not exhaustive, as there are other factors that directly or indirectly affect the implementation of relational practices, such as the organisation's reputation, leadership styles, trust, and regulatory requirements.

In terms of training, the AIG group's management is committed to fostering an information culture throughout the organisation by conducting regular training and awareness programs for their employees in partnership with globally accredited institutions like the International Organization for Standardization (ISO), Gartner and Microsoft. A significant investment was allocated by the two banks for building a state-of-the-art learning centre equipped with the most advanced technologies and facilities to deliver specialised courses in information governance and other relevant domains, such as AML (Anti-Money Laundering), data security, and data quality. Through multiple training and awareness programs, employees at different organisational levels were informed about the values and risks of information, plus the importance of keeping customer information secure. Interestingly, protecting the organisation from reputational risks was the key factor that promoted AIG's cases to invest in employee development and training. This may maybe because their ability to acquire new customers and generate profits relies on the solid reputation they establish within their industry.

As such, employees in both banks were trained on how to maintain a good reputation and avoid information-related risks like data breaches by familiarising them with international best practices and relevant policies and procedures. In addition, the AIG group has maintained a culture of continuous learning and development through the establishment of a talent management programme, which aims to align the employees' skills and competencies with organisational goals. As a result, AIG's management offered their employees financial rewards and incentives to encourage them to acquire relevant IG certifications and experiences for achieving these goals. They also awarded and funded several academic scholarships in various disciplines, including information management and data science, to support their talented staff in pursuing their postgraduate studies at local and international universities.

On the other hand, both cases 1 and 7 have conducted regular evaluations and assessments of their training programs using various methods like self-assessment, tests, and performance metrics. For example, all employees were required to take a mandatory post-training exam to measure their level of understanding and to identify areas that need further development. The results of the exams are also analysed by the responsible training managers so that they can report any deficiencies in the current training practices to the executive management for further action. To summarise, the effectiveness of training at AIG group has been strengthened by the organisational culture and strong support from their senior management.

By contrast, IIG groups have adopted a combination of relational practices for enhancing interactions with stakeholder groups. User education is especially established. One of the key challenges identified is that customers sometimes express resistance towards the conditions that banks impose on them based on Central Bank AML regulations. However, it is observed that the banks do not identify the adoption of proactive action towards educating the employs about IG. Training only emerges to be primarily focused on AML and KYC requirements.

Communication also emerges to be well-established. Case 2 holds a meeting each quarter to communicate with the employees about policies and regulations changes. Other IIG bank cases utilize channels including email and meetings to communicate with employees. Utilizing diverse communication channels ensures that employees are aware of aspects such as policy and procedure changes. IIG case banks show an appreciation of the importance of maintaining communication with employees through a combination of channels.

Collaboration between stakeholders is an established practice in IIG cases, though some challenges are also experienced. Collaboration especially occurs with the regulators with each of the IIG banks reporting working closely with the central bank to ensure compliance with banking regulations. However, support from the senior management team emerges to be a challenge in IIGs. It is noted from case 3 that CEOs are explained as viewing data as “a waste of time and a waste of money” and are not willing to invest the resources required for effective data governance. The absence of adequate support from top-level managers imposes significant constraints on effective IG in the IIG banks. Case 4 is an exception as it is explained that the bank has created an Information Security Committee composed of executive officers and other top-level managers. The Information Security Committee has enhanced support from the CEO and the executive team because it provides an environment where effective collaboration can occur.

The BIG group has also developed a good maturity in its structural practices driven by senior management support. A key observation is the presence of strong communication between personnel and the senior managerial team. Interviews reveal that senior managers at Case 8 are supportive towards the IT department. The management team is receptive towards making the financial investments required for the creation of effective IT systems. The Head of IT reports having had the opportunity to communicate about the personnel deficiencies that should be addressed for effective IG. The presence of communication with the senior managers and support expressed towards the establishment of effective IG through the provision of required equipment creates a conducive environment for improvements to be made towards effective IG.

One of the key issues is the absence of effective communication with subordinate members of staff who are expected to directly implement the IG policies that are developed. It is observed that in Case 8 one of the issues affecting IG is the lack of awareness among personnel. It emerges that subordinate employees at the lower hierarchy levels are not aware of existing IG policies and procedures. The low level of awareness about IG among personnel hinders the effective execution of the existing policies. Low levels of awareness illustrate that Case 8 does not actively engage employees in promoting IG practices. The low levels of awareness create the opportunity for employees to violate best practices and existing guidelines absence of the knowledge of doing so. There is a risk that case 8 considers IG as a practice that is the responsibility of higher-level managers with minimal involvement required from operations-level personnel. The failure to adequately create awareness among lower-level personnel makes it challenging for the bank to effectively execute IG practices.

A further issue that emerges as hindering the adoption of effective IG is the absence of employee training. Interview data indicates concerns that the pattern of missing data and data containing errors is an outcome of employees lacking adequate training. Employee training is essential in enhancing employee competence in upholding IG (Abraham et al., 2019). Training provides employees with the competence required to address IG issues. The absence of employee education is adversely affecting the IG of the bank. In the interview, it emerges that there are only limited instances when employees are trained, with one instance being when the loan policy was changed. Employees require training on a variety of IG issues including privacy, confidentiality, security, and adherence to established policies. The failure to provide adequate training to the operational level employees exposes Case 8 to the risk of employees ignoring recommended best practices. Personnel should be one of the key approaches for enhancing IG at the operational level.

A key strength of the communication practices in Case 8 is the use of a variety of channels in some of the instances. Communication is essential in ensuring that parties are aware of expected data requirements (Alhassan et al., 2019). An example is given that when policy review changes occur every 2 years, effort is put into communicating the policy changes to employees through channels including email. Email is bound to be a communication channel that is accessible to most of the employees. Communicating policy changes through email guarantees that employees can become aware of the guidelines that should be followed. However, the use of email may be limited given the availability of other alternative channels including official face-to-face meetings that can allow for more direct communication and allow the employees to ask questions.

However, Compliance emerges to be a concern especially about AML. While the bank expresses the perspective that it is not significantly exposed to AML risk based on its operations being focused on issuing loans instead of taking deposits, case 8 expresses a commitment towards ensuring that it adopts measures that minimize the risk of customers exploiting loopholes to engage in money laundering. However, the analysis reveals that Case 8 may be placing too much reliance on government and central bank-issued laws to ensure they are in alignment. The interview reveals the perspective that Case 8's IG failures are partly attributable to the government and the central bank's failure to issue guidelines specifically aimed towards the management of data. To this end, Case 8 may expect that the government and the central bank should play a greater role in the development of IG policies and guidelines. However, this perspective is contrary to the expectation that IG is a proactive approach that organizations are expected to adopt without relying overly on government regulations.

Relational Practices	Case 1 (Local)	Case 2 (Local)	Case 3 (Local)	Case 4 (Local)	Case 5 (Local)	Case 6 (Islamic)	Case 7 (Foreign)	Case 8 (Specialised)
User education/ Training	12	7	24	11	9	9	1	7
Communication /ideas exchange	5	9	15	7	2	1	5	1
Collaboration among stakeholders	3	0	6	8	2	0	2	4

Table 19: Frequency counts of relational practices across the eight banks

5.3.3 Consequences of Information Governance

The cross-case analysis revealed that the three groups considered in this study have achieved different outcomes depending on their IG maturity level and organisational capabilities.

The AIG's cases witnessed a significant improvement in customer service underpinned by their customer-centric strategy, continuous training, innovative products, and services, as well as the use of advanced technologies. These cases utilized IG to place the customers' voice at the centre of their business strategy and tactics, and therefore they harnessed all resources and capabilities to satisfy their needs. By adopting a customer-centric strategy, the two banks were able to attract more customers and gain their loyalty and trust, which ultimately helped them build a strong brand reputation in the industry. To better serve customers, they have undergone a major digital transformation, which includes upgrading their IT infrastructure, replacing legacy systems, implementing big data analytics, and launching innovative digital services. For example, the use of big data analytics capabilities enabled employees at the AIG group to gain deep insights into customers' behaviours and preferences by analysing their historical purchase data, thereby providing them with more personalised products and services. Emphasising the importance of delivering an exceptional customer experience, AIG's management developed a set of performance metrics and KPIs, including customer satisfaction and retention scores, to assess the effectiveness of its organisation in meeting customer needs and expectations. Therefore, all employees have received continuous training on how to increase customer satisfaction by informing them about their responsibilities, customer rights, complaint handling, problem-solving techniques, and data protection measures.

In addition, the cross-case analysis revealed that the digitalisation and implementation of intelligent solutions like robotic process automation (RPA) and artificial intelligence have increased the productivity of employees in AIG's cases. This has allowed them to automate routine IG tasks while directing their efforts to core activities that require critical thinking and cognitive skills. Therefore, resulting in relatively fewer human errors and more accuracy in data, which led to increased customer satisfaction and reduced complaints.

Furthermore, the findings showed that the adoption of effective IT infrastructure with clear policies and procedures has helped the AIG group to experience a remarkable enhancement in their data quality, as they reported fewer data entry errors, non-compliance issues, fraud cases, and customer complaints.

In terms of risk mitigation, the cross-case analysis revealed several conditions and IG practices the AIG's cases have adopted to mitigate risks of money laundering. As evidenced by the data, these cases possess a strong risk culture supported by a risk management framework, senior management support, board-level oversight, risk policies, and training programs. The management in AIG group cases has actively promoted a risk mitigation culture across employees by consistently communicating the impact of associated risks on the bank's reputation.

Additionally, the findings highlighted the proactive approach by the management in the AIG group that has actively promoted a risk culture across employees by consistently communicating the impact of AML risks on the bank's reputation and encouraging them to report suspicious or illicit transactions. The group has also proposed a new oversight structure, which includes dedicated committees like the Board risk committee and financial crime committee to monitor policy implementation and ensure compliance with relevant laws and regulations. A review of their documents indicated that the group had a zero-tolerance policy against money laundering risks, which promoted the executive management to continuously enhance their AML governance, controls, and monitoring tools. These findings align with the existing literature which correspond that having high-quality KYC data can help compliance officers better detect anomalies or suspicious transactions from large datasets and respond timely to ensure that risky transactions are detected and prevented before they are executed (AlGhamdi et al., 2020). Likewise, it can be argued that ensuring compliance with laws and regulations can mitigate money laundering risks by implementing best practices for collecting, protecting, and analysing AML-related data (Al Wahshi, Foster, & Abbott, 2021; Protiviti, 2020).

5.4 Strategies for Improving IG Practices: Practical Steps for Navigating From Basic to Advanced Levels

The previous sections provide a comparison of antecedents, IG practices and consequences across eight Omani banks classified into three groups or levels (i.e., advanced, intermediate and basic). Based on the results of the cross-case analysis, it was noted that there are specific conditions that affect the maturity of structural, procedural and relational practices across different groups. This section, however, aims to provide practical steps and strategies for banks at the basic level to improve their IG practices/ capacities. These practical steps were drawn from the lessons learned from both the advanced and intermediate IG Groups.

5.4.1 Conduct comprehensive training on IG

The first step in improving IG practices is to conduct a comprehensive training programme for employees that covers the core principles of IG. This training should be mandatory for all employees at different organisational levels, from the board of directors and executive management to junior staff, such as clerks. Therefore, it is important for the organisation to tailor its training programmes to different roles and responsibilities to ensure the relevance of the content.

From the moment of joining the organisation, an employee must be made aware of the importance of data and the existing policies and procedures to be followed. Likewise, employees should be trained in how to incorporate these policies and procedures into their daily activities. For example, front-office staff may be provided with special training showing them how to accurately collect mandatory KYC information according to AML policy. To be more effective, training programmes should be conducted using different methods and formats, including classroom instructions, online learning and interactive workshops.

Of course, the choice among these methods will depend on the nature of the topic being delivered, employees' preferences and the training budget. For example, an organisation may find it more useful to conduct classroom or interactive training sessions for IG topics –such as information classification—that require hands-on or practical exercises. Regardless of the chosen method, training programmes must be followed with assessments and quizzes to measure employees' understanding of key IG topics before and after training. The results of these assessments can be analysed to identify gaps in knowledge where employees need further training and awareness. However, it is recommended that IG training programmes be linked to the KPIs of employees to ensure consistent progression in their learning and professional development in the IG domain. Lastly and most importantly, training and awareness sessions should be ongoing—at least twice per year—to stay updated and informed about recent developments and changes in IG-related issues and trends.

5.4.2 Develop clear policies and procedures

The second step in improving IG practices is to create clear policies and procedures that are free from technical jargon. These policies and procedures must be understood by all employees –regardless of their educational levels or experience—so that they can be implemented without any complications. For the policies and procedures to be clear, they must be discussed and explained to all employees using simple or plain language. To simplify the process of policy implementation, the organisation may use illustrations and visual representations, such as tables, mind views, flowcharts, checklists and templates.

Before approving these policies and procedures, it might be useful to share the drafts with different business users or stakeholders, particularly those who are required to implement them. Alternatively, each department may appoint a representative or a focal point who should be responsible for developing their own policies and procedures.

In all cases, these policies and procedures must be reviewed and validated by control functions, including compliance, legal and audit, to ensure that they are aligned with applicable laws and regulations. Lastly, banks should establish a mechanism to review their policies and procedures periodically to stay aware of recent changes and updates in IG requirements, therefore preventing them from becoming obsolete or ineffective.

5.4.3 Assign clear roles and responsibilities

The third strategy for improving IG practices entails the clear assignment of roles and responsibilities. Policies and procedures must use a responsibility matrix like RACI to outline specific IG roles and responsibilities for each employee or department. For these roles and responsibilities to be effective, they must be linked to the job descriptions of employees so that they can understand their duties in implementing specific IG policies. Furthermore, the organisation may request employees to sign an undertaken, indicating that they understand their IG roles and responsibilities and that they commit to enforcing them in accordance with relevant policies and procedures.

To be sure, regular training and awareness sessions should be conducted for all employees to ensure that everyone understands their roles and responsibilities. Likewise, employees must be clear about why they are the owner of specific data/ information in the organisation. To avoid conflicts among teams, it is recommended to use the three-lines-of-defence model, which often assigns data ownership responsibilities to the first line of defence (i.e., business). Finally, developing a culture of responsibility must be driven by top management by assuming the overall accountability of the data.

5.4.4 Leverage new information technologies

The fourth strategy for optimising the performance of IG practices is to leverage new information technologies like AI, machine learning and big data analytics to automate routine IG jobs. The results of the cross-case analysis showed that new technologies enabled AIG's banks to streamline procedural life-cycle practices (such as information classification, user access and compliance monitoring), leading to significant improvements in their operational efficiency, customer service, data quality, data security, compliance and risk mitigation.

Given that, banks at the basic level are highly recommended to invest in such technologies to increase their maturity level by establishing a clear roadmap for upgrading/or replacing their legacy IT systems. Before embarking on new technologies, it is important for banks to train their employees on the ethical standards and privacy issues pertaining to the use of these technologies to process customer information.

5.4.5 Develop an information culture

Developing an information culture is another crucial step in improving IG practices. It is considered a 'lifeblood' that connects different stakeholders through common beliefs, values and practices governing the use of information assets. Information culture must be driven by senior management by emphasising the importance of information in making the strategic decisions necessary for achieving organisational goals.

For information to be seen as a strategic asset, it must be integrated into corporate strategies and plans. Of course, this must be translated into action by establishing a bank-wide IGF duly approved by the board of directors. Additionally, employees should be encouraged to use information in their daily operations by providing them with easy access to the required information. However, it is imperative for banks to conduct regular training and awareness programmes to showcase and remind employees about the benefits of information at departmental and organisational levels.

5.4.6 Integrate data into a single repository

Finally, integrating data into a centralised repository, such as a data warehouse, is paramount for banks seeking to streamline the implementation of IG practices by enabling them to apply relevant policies and procedures in a single database. Before embarking on a data warehouse project, banks must clearly define their goals from data integration; for example, enhance regulatory compliance, reduce AML risks, enhance operational efficiency and improve customer service. Having clear and focused goals is critical because this can help banks identify the data types and sources, including core banking systems and customer relationship management systems, credit card systems and KYC data that need to be integrated.

Chapter 6: Discussion

6.1 Introduction

This current study investigated how various IG practices (structural, procedural and relational) can help Omani banks mitigate the risks of ML. The study adopted a qualitative multiple-case study approach with semi-structured interviews and document reviews used as key methods to gather the primary data (described in more detail in Chapter 3). The following sections discuss the key findings and linking them with the existing literature.

6.2 Antecedents of Information Governance

6.2.1 IG Enablers

6.2.1.1 Regulatory Compliance

The current study found that regulatory compliance is one of the key enablers of IG practices in Omani banks. The overwhelming majority of participants reported that the increased pressures from internal and external regulators, such as the CBO and the FATF, forced them to continuously update their policies and procedures to comply with evolving regulatory requirements. This finding is consistent with Alhassan et al. (2019), Karkošková (2022), Tyagi (2021) and Faria et al. (2013) who found that laws and regulatory requirements pushed banks to enhance their internal governance mechanisms, systems and controls to meet information requirements.

Similar results were observed by Kwan et al., 2022) and Shu and Jahankhani (2017) who found that data-related regulations such as GDPR enforced hospitals and health services to develop effective IG practices to ensure the confidentiality and privacy of patients' data. This similarity emphasises the critical role of regulations in accelerating the adoption of IG practices across different sectors, including banking and finance. It also supports what has been theorised by Becher and Frye (2011) who contend that regulations complement rather than substitute governance. This perspective suggests a dynamic interplay between external regulations and IG practices (Tallon et al., 2013). Therefore, it can be argued that highly regulated firms are likelier to have more mature IG practices compared to those with relaxed or weak regulations (Alhassan et al., 2019; Becher & Frye, 2011). Rather than viewing regulations as a burden or an obligation, banks may use existing regulatory requirements as a guiding framework to develop or enhance their IG policies and procedures.

6.2.1.2 Information Growth Rate

This study's findings revealed that the information growth rate is another significant driver of IG adoption in Omani banks. The majority of participants indicated that the rapid growth of information from both internal and external sources triggered their banks to develop effective IG practices to manage a large volume of customer data. Consistent with the literature, the current research identified regulatory requirements as the primary source of information growth in the banking industry (Faria et al., 2013; Tyagi, 2021).

Similar results were observed in different contexts, including the healthcare sector (e.g., Sudra, 2020; Tavakoli & Jahanbakhsh, 2013). Industry regulations, such as AML and KYC, mandate that banks collect and retain massive amounts of customer data (both physical and electronic) for specified periods or even permanently (Parameswarappa, 2022; Tyagi, 2021). This exponential increase in stored information has forced banks to optimise their storage and backup capabilities to accommodate the current and future growth of information (Serrado, Pereira, Mira, & Bianchi, 2020).

Furthermore, the current study found that data analytics is another key factor in data growth in banks. As indicated in the results chapter, the current rate of information growth is expected to double in the coming years as Omani banks have become fascinated with new technologies, such as big data analytics, to enhance their data-driven decision-making and competitive performance. These findings are in line with those of previous studies (e.g., Delgosha et al., 2021; Lis et al., 2022; Tallon et al., 2013).

In their study of IG antecedents in the railway industry, Lis et al. (2022) found that “the increasing adoption of the IoT [the Internet of Things] accelerates the volumes of generated data and forces organisations like Thales [the case study] to adopt sophisticated approaches to govern and make sense of these data assets” (p. 2,536). This suggests that the more an organisation uses big data analytics, the likelier it adopts IG practices to draw meaningful insights from large volumes of data (Mikalef, Boura, Lekakos, & Krogstie, 2020; Mikalef, Krogstie, van de Wetering, Pappas, & Giannakos, 2018). Therefore, this current study adds to existing research by empirically confirming the positive relationship between the adoption of data analytics and information growth.

6.2.1.3 Adoption of new Information Technologies

This current study showed that new information technologies, such as big data analytics and AI, played a critical role in facilitating the implementation of IG practices across different Omani banks. This finding supports previous research (Alhassan et al., 2019; Mahanti, 2021; Muhammad, Isa, Samsudin, & Miah, 2020; Smith, 2015), which highlights the role of technology in streamlining IG processes by automating repetitive or routine tasks that consume significant headcounts when performed manually. These findings contribute to the existing body of knowledge by providing empirical evidence demonstrating how banks can leverage new technologies to enhance their productivity and operational efficiency. They also extend the theory of IG (Tallon et al., 2013) by adding the factor ‘new information technologies’ to the predefined list of IG enablers. This factor has not been explicitly considered in the TRS framework, possibly because these technologies and their impacts on IG were less apparent during the development of this framework.

6.2.1.4 Senior Management Support

The results of this study showed that senior management support was one of the critical success factors for IG adoption in the Omani banking sector. Support from the executive and senior management was found to take various forms, including the provision of funds for training and IT infrastructure, resolving conflicts related to data ownership and hiring specialised personnel in IG. These results support evidence from previous research, which suggests that organisations with effective leadership are likelier to achieve successful and sustainable IG frameworks (Egan, 2011; Mahanti, 2018; Randhawa, 2019; Silic & Back, 2013; Smith, 2015).

Randhawa (2019) suggested that when senior management endorses and prioritises the implementation of IG initiatives, this perception permeates the information culture and encourages employees to embrace IG practices and integrate them into their daily operations. For example, the active involvement of senior managers in IG projects can help foster collaboration among employees and overcome resistance to change that may arise during the implementation of IG practices (Randhawa, 2019; Silic & Back, 2013). These findings reinforce the critical role of senior management support in IG adoption and extend the theory of information governance (Tallon et al., 2013) by adding this construct to IG enablers.

6.2.1.5 Organisational/IT Strategy

Consistent with the literature, this research confirms the positive impacts of organisational and IT strategies in driving IG-success across the studied banks (Alhassan et al., 2019; Mahanti, 2018; Seboka, 2015; Smith, 2015; Tallon et al., 2013). Empirical evidence shows that the strategic alignment between business and IT enables organisations to create synergies and unify their capabilities towards achieving common IG goals, which in turn leads to higher firm performance (Faria & Simpson, 2013; Mikalef et al., 2018). Alhassan et al. (2019) argued that ineffective or poor strategic planning can negatively impact IG adoption, particularly when a focused data strategy is lacking. This suggests that for an IG initiative to be visible across the entire organisation, it must be integrated with broader business goals and objectives (Bharadwaj, Omar, & Paul, 2013).

Furthermore, this study identifies data growth as a critical part of IT strategies and planning. Several IT professionals in this study stated that strategic IT alignment enabled them to implement a flexible and scalable IT infrastructure to avoid potential business interruptions arising from sudden or unexpected data growth. This finding was also reported by Tallon et al. (2013). While the majority of IG literature tends to be skewed towards organisational strategy as a key enabler for IG adoption (Lis et al., 2022; Smith, 2015), the current study sheds light on the critical role of IT strategy in shaping an organisation’s IG practices.

6.2.1.6 Customer Information Gathering

The findings showed that customer information gathering triggered Omani banks to adopt effective IG practices. Several IG professionals in this study highlighted the importance of collecting diverse information about customers to enhance customer experience, develop products, mitigate risks and achieve competitiveness. This finding aligns with Gregory (2011), who argued that customer data is a key asset for organisations that must be governed to balance the values and risks associated with holding and using customer data/ information.

In the context of the banking industry, Okunleye (2023) found that governing customer information can increase profits, reduce operational costs and enhance data security. By integrating customer data into a unified system, banks can better understand customers' behaviours and preferences, enabling them to tailor their products and services to the expectations and needs of their customers (Okunleye, 2023).

Additionally, the study's findings suggest a relationship between customer information gathering and risk mitigation, particularly in the domain of ML. Compliance professionals in this study confirmed that the more information collected about customers, the better they can detect suspicious transactions. However, this result has not been adequately described in the extant literature despite the increasing emphasis on the importance of customer data in mitigating ML risks (Al Wahshi et al., 2021; Soares, 2011). A lack of banking data can restrict access to case studies for academic investigation. Therefore, the findings of this study fill this gap by providing empirical insights into the role of customer information gathering in shaping IG practices in the banking industry. It also contributes to the theory of information governance by confirming the relationship between IG antecedents and risk management.

6.2.1.7 Information Culture

Interviews revealed that the values, norms and attitudes of the organisation played a critical role in shaping IG practices by influencing how information is used, accessed, shared and managed by employees across different Omani banks. This finding corroborates previous research that has highlighted the positive impact of information culture on overall IG effectiveness (Daneshmandnia, 2019; Lian, Wang, & Oliver, 2022; Lis et al., 2022; Svärd, 2014). For example, Svärd (2014) found that an information culture can enable an organisation to achieve a competitive advantage via the effective use of information. In the context of this current study, participants indicated that the presence of an organisational culture that promotes the use of information for making decisions and improving services served as an important vehicle for nourishing information culture by encouraging employees at all levels to leverage data/information for improving a bank's performance. These results provide further support for the argument that organisational culture and information culture are intertwined and influence each other (Choo, 2013; Oliver, 2008; Svärd, 2014).

Additionally, the study's findings emphasised the role of senior management in developing an information culture, concurring with the assertions made by Svärd (2014) and Curry and Moore (2003) who highlighted the role of leadership in fostering a culture of compliance, collaboration, accountability and trust. Respondents in the current study perceived communication from top management to be effective in making cultural changes and directing employees towards a more data-driven culture. In this regard, it has been suggested that participatory leadership that encourages information/ideas sharing between employees can help organisations overcome many challenges associated with resistance to change, facilitating them in nurturing an integrated information culture (Curry & Moore, 2003; Lian et al., 2022).

Another interesting finding is that regulatory requirements were identified as a significant factor shaping information culture in the Omani banking sector. This finding was unexpected and suggests a relationship between regulatory requirements and information culture, challenging the notion that information culture is driven by an organisation's internal values and norms (Choo, 2013; Oliver, 2008). Research has shown that the regulatory requirements put on information have an impact on information culture (Wright, 2013).

To summarise, the current study provides valuable insights into the impact of information culture on IG effectiveness, an area that has received little attention in the IG literature (Svärd, 2014). It also offers empirical evidence that both supports and extends existing IG theories. While Tallon et al.'s (2013) framework identified 'IT culture' as an enabler for IG adoption, this current research proposes replacing it with 'information culture' since the latter is found to be more prevalent and dominant across the dataset.

6.2.1.8 Funding Availability

Analyses of the interviews revealed that the availability of funding enabled the Omani banks to eliminate many obstacles to IG-success. Interviewees indicated that the allocation of adequate funds was critical to acquiring cutting-edge technologies, upgrading IT infrastructure, hiring IG professionals and conducting the training necessary for implementing and sustaining effective IG initiatives. These results reflect those of Muhammad, Miah, Isa, and Samsudin (2022) who emphasised the critical role of funding in implementing IG practices in Nigerian universities. While the importance of funding is well documented in the IT governance literature (e.g., Ismail, 2008), very little has been found in the IG literature (Bertin, 2014; Mahanti, 2018; Muhammad et al., 2022). The scarcity of focused research on IG can be attributed to difficulty in obtaining funding – especially for non-profit-organisations, such as those that provide education —due to the intangible or delayed benefits associated with IG projects (Muhammad et al., 2022).

In contrast to previous research, however, the current study showed that senior management and boards of directors are more willing to invest in IG-related activities (e.g., data cleansing and KYC updates) to comply with different data requirements. This finding suggests that profit-organisations, including banks and financial institutions, are likely to prioritise IG investment and integrate it into their strategic agenda (Faria et al., 2013; Tyagi, 2021). Arguably, without sufficient funding, banks may struggle to implement comprehensive IG practices, leaving them vulnerable to compliance issues, data breaches and other information-related risks.

Furthermore, the study's findings suggest a relationship between funding availability and training. This is particularly a useful finding as it confirms the impacts of IG antecedents in shaping various structural, procedural and relational practices. In accordance with the present results, Bertin's (2014) found that the level of IG awareness in an organisation is largely influenced by the budget assigned for training and education. Therefore, this research contributes to the existing body of knowledge by providing empirical evidence of the importance of funding in facilitating the implementation of IG practices in organisations. It also extends the theory of IG (Tallon et al., 2013) by adding the construct of funding as a critical enabling antecedent for IG adoption in banks.

6.2.2 IG Inhibitors

6.2.2.1 Data Quality Issues

Data quality issues represent a significant barrier to the effective implementation of IG practices within Omani banks. The findings from the current study underscore the prevalence of these issues, which include erroneous data entries, duplication and outdated customer information, among others. These challenges are compounded by the complexity of data systems, the variety of data being handled and the critical need for high-quality data in compliance and decision-making processes, particularly in areas concerning financial crimes and regulatory compliance.

The IG literature consistently emphasises the impact of poor data quality on operational efficiency and regulatory compliance. For instance, Dadashzade (2018) and Haug & Arlbjørn (2011) identify unintegrated systems, incorrect data entry, and the lack of a standardised approach to data management as core issues affecting data quality. These challenges hinder not only compliance efforts but also affect customer service and the bank's ability to offer personalised services.

The issues identified in Omani banks mirror those seen in broader contexts, suggesting that the barriers to effective data quality management are universally challenging, yet they also highlight specific regional challenges, such as customer reluctance to provide accurate information and the prevalence of legacy systems in long-established banks.

To address these challenges, it is imperative that banks in Oman must adopt a more integrated and standardised approach to data management. This could involve updating legacy systems, improving staff training on the importance of accurate data entry and implementing more robust DG frameworks that encourage consistency across all departments and systems. Only through such comprehensive measures can banks hope to overcome the pervasive challenge of poor data quality and realise the full potential of effective IG practices.

6.2.2.2 Lack of Clear Policies and Procedures

The interviews conducted with professionals in the Omani banking sector revealed a significant concern about the ambiguity and inconsistency of policies and procedures. Such confusion leads to inconsistent compliance practices and poses substantial regulatory risks. This situation underscores the critical gap in the effective management of IG, as discussed in the existing literature.

As highlighted by one interviewee, a lack of clearly defined and well-communicated policies resulted in varied applications across different departments, undermining the effectiveness of compliance measures. This echoes findings in broader governance literature, which suggest that clear, coherent policies are fundamental to ensuring compliance and managing organisational risks effectively (Kooper et al., 2011). Furthermore, the rapid evolution of regulatory landscapes, particularly in areas like AML, demands frequent updates to policies and procedures. This poses a specific challenge for smaller banks with limited resources, highlighting the need for regulatory frameworks that offer flexibility while maintaining comprehensiveness (Nordin et al., 2022).

This scenario calls for an integrated approach to IG that not only standardises policies across departments but also ensures that they are adaptable to fast-paced changes in regulatory requirements, thus safeguarding banks against compliance risks and enhancing overall institutional integrity.

6.2.2.3 Legacy IG Systems

The challenge of legacy IG systems in Omani banks is profound, rooted in issues of outdated technology, high maintenance costs and risks related to data quality, integration and security. These systems, while holding mission-critical information collected over many years, significantly hinder innovation and the implementation of modern IG practices due to their incompatibility with current technological standards and requirements.

As highlighted by the participants in this study, the sheer antiquity of these systems leads to operational and compliance risks, emphasising the difficulty of accessing and retrieving customer information from servers running on unsupported operating systems. This situation resonates with Aydemir's findings (2021), which suggest that the rigidity of legacy systems in the banking sector poses a significant barrier to digital transformation efforts by limiting the ability to adapt to new technologies and data standards.

The lack of detailed knowledge about existing data sources further complicates attempts to modernise IT infrastructure. As IT professionals struggle with the absence of technical documentation, they face hurdles in understanding the data structures and schemas essential for successful data migration projects. This issue is aligned with the broader challenges described by Ceruti (2004), who discusses the obstacles in data management due to legacy systems that lack scalability and interoperability, thus impeding effective information management.

Moreover, the maintenance of legacy systems imposes substantial costs without offering commensurate value, which aligns with assertions in the literature about the economic burdens of outdated IT systems (Ceruti, 2004). These systems, developed using obsolete programming languages by no longer available employees, necessitate costly outsourced maintenance and pose significant challenges in hardware repair or replacement due to their discontinued status.

Lastly, the siloed nature of legacy applications restricts data sharing and visibility across departments, leading to fragmented information and inefficiencies that undercut the potential benefits of data-driven decision-making. This issue is notably discussed by Aydemir (2021), who emphasises that legacy systems' architecture often precludes integration with newer technologies, thus perpetuating data silos and compromising the quality and consistency of data.

Overall, the persistence of legacy IG systems in the Omani banking sector exemplifies a critical barrier to adopting advanced information governance frameworks and technologies, underscoring a pressing need for strategic overhauls to mitigate the risks associated with outdated infrastructures.

6.2.2.4 Lack of Data Integration

This study's findings on the lack of data integration in Omani banks elucidate a critical challenge: data silos severely hinder the efficiency of data handling and customer service. Banks struggle with multiple uncoordinated systems, each capturing and storing distinct types of customer data, which complicates efforts to provide a unified customer view. This fragmentation not only affects productivity by increasing the time employees spend gathering data for basic tasks like loan processing but also heightens compliance risks due to discrepancies in the data reported to regulatory bodies like the CBO.

To mitigate these issues, a more integrated data management strategy is paramount. The literature supports this approach by highlighting similar challenges in various sectors where data integration has significantly enhanced operational efficiency and compliance. For instance, Wang (2019) discusses how electronic medical records integration in China faced similar hurdles due to decentralised systems, stressing the need for unified data standards and central coordination. Similarly, research on data integration in financial services suggests that establishing a centralised data hub can streamline data processing and improve decision-making, as can be seen in the case studies detailed by von Simson (2016).

Omani banks, therefore, need to adopt a centralised approach to data management. This includes the establishment of data warehouses or national data hubs, as suggested in the findings, which would allow for consistent data access and management across all banking systems. Implementing such centralised systems would not only enhance customer service and internal efficiency but also ensure that data integrity is maintained, thereby reducing compliance risks and improving the strategic use of data within the banking sector.

6.2.2.5 Lack of IG Awareness

The findings from the study underscore a significant challenge in Omani banks: the lack of awareness among employees and customers regarding IG practices aligns closely with the literature on DG in various sectors. For instance, Gutema's study (2023) on DG in higher education highlights similar challenges, where a lack of awareness impedes the effective management and utilisation of data assets.

This lack of awareness is noted as a major barrier to the adoption of IG, highlighting a disconnect between the perceived relevance of data and its actual importance for business operations and compliance, such as issues raised by Alhassan et al. (2018) who discussed the social challenges of establishing DG in educational institutions.

Employees, especially at customer-facing levels, often view data-related tasks as nonessential, thereby undermining IG efforts. This situation is compounded by the fact that information about IG policies and the importance of data compliance is not sufficiently disseminated throughout the organisation, particularly in branches distant from central offices, echoing findings by Khatri and Brown (2010) on the critical role of clear communication in effective DG.

The problem extends to customers who are unaware of how their data are used and its importance, leading to a reluctance to provide accurate and complete information. This scenario calls for a strategic shift towards enhancing IG awareness through comprehensive training and clearer communication of the critical role data plays in both compliance and service quality. Banks must prioritise ongoing education programmes for all levels of the organisation and develop initiatives to educate customers about the benefits of providing accurate data, thus fostering a more robust IG culture, aligning with the recommendations of Cheong and Chang (2007) for improving data management through better governance practices.

6.3 Relationships between the themes

This study with its analytical strength and data richness was successfully able to identify factors that shape various IG practices in the Omani banking sector. Existing literature has only focused on identifying the factors that influencing the adoption of IG practice (e.g., Abraham et al., 2019; Alhassan et al., 2019; Smith, 2015), without exploring how these factors interact with each other to shape specific IG practices–i.e., structural, procedural and relational. This study, therefore, goes beyond the theoretical framework by Tallon, Ramirez, and Short (2013) by providing 'new' insights into the relationships of different elements of the framework. To the researcher's best knoweldge, this is the first empirical study that explore these relationship on the current IG literature. Given the lack of literature in this aspect, the discussion will be based on empirical data collected in this study. The next section provides further details about the factors that shape the structural, procedural and relational practices in the Omani banking sector.

6.3.1 Factors shaping structural practices

Analysis of the structural practices revealed several factors shaping the structural practices –i.e., data ownership responsibilities, policy-setting procedures and oversight mechanisms—across different Omani banks participated in this study. These included: (1) organisational structure, (2) organisational culture, (3) clear policies and procedures, and (4) training.

6.3.1.1 Organisational structure

Organisational structure is a fundamental factor to be considered when embarking on IG initiative (Muhammad et al., 2020; Otto, 2011b). The empirical findings showed that the more precise the organisational structure, the better governance it can provide to the information. Clear organisational structure should act as a guide for organisations since it specify the roles and responsibilities of each business departments in relation to information management (Otto, 2011). It should also help in assigning the oversight responsibilities to the designated committees, thus avoiding confusion.

6.3.1.2 Clear policies and procedures

Clear policies and procedures along with clear data ownership responsibilities are two fundamental components that must be in place to ensure effective information governance in the organisation. In the context of Omani banks, the information security policy was found to be critical in outlining data ownership responsibilities of employees and business units. This policy starts from the early stage of hiring new staff, where they receive detailed instructions of the importance of data security and their roles in handling enterprise data. Additionally, each staff member is provided with clear job description that outlines their roles and responsibilities in relation to information management. To be sure, employees were required to sign an acknowledgment indicating that they have read, understood, and accepted their roles and responsibilities. They also required to acknowledge that they have read and understood the policies and procedures in place. Therefore, clear police and procedures are critical in facilitating the assignment of data ownership responsibilities.

6.3.1.3 Training

This study underscores the importance of training in shaping structural practices. Providing staff with training and awareness sessions are crucial to ensure all employees understand their roles and responsibilities in handling enterprise information. Without effective training, employees may not understand what data ownership entails. The training should cover why they are the owners, and the importance of ensuring that the data is rightly governed and secured. This will help in enhancing transparency of data ownership while making them more accountable for their actions.

6.3.1.4 Organisational Culture

On the other hand, organisational culture was found to have a positive impact in shaping structural practices, particularly data ownership responsibilities (Daneshmandnia, 2019). If the bank's culture is based on finger-pointing and blaming, data ownership are likely to be problematic. Conversely, if the culture is calm and transparent, then employees would take data ownership responsibilities very seriously. Therefore, it is essential to develop a culture where everyone feels accountable for data ownership. As a result, this will lead to the creation of conflict-free environment among employees.

6.3.1.5 Senior management support

When explaining the relationship between senior management support and structural practices, it is crucial to acknowledge the pivotal role of senior management in in fostering a culture of transparency and responsibility (Mahanti, 2018; Randhawa, 2019). Such a culture promotes employees to engage actively in IG-related activities, and foster a sense of responsibility towards data ownership. For example, when senior managers actively endorse and participate in IG activities, it can sends a strong massage throughout the organisation about the importance of maintain effective information management practices (Randhawa, 2019). In the context of the Omani banking industry, the active involvement of senior management was essential to develop structural practices by reviewing and approving IG policies and procedures.

To conclude, this study identified four critical factors shaping structural practices, including (1) organisational structure; (2) clear policies and procedures; (3) training; (4) organisational culture; and (5) senior management support. A summary findings of these factors are presented in Table below.

Factor(s) name	**Evidence from data**
Organisational structure	*"If you have the right organisational structure in place, it defines the roles or responsibilities of each employees ... it assigns accountability and ownership. It all goes to that, if policies and organisational structures are not aligned, if they do not exist, if they are not adequate, then you will find problems with [data] ownership"* (P42)
Clear policies and procedures	*"So a lot of the policies we're developing have raci [Responsible, Accountable, Consult, Informed] matrices as part of to say, clearly, who is responsible for what data" (P31)*
Training	*"The training and awareness for staff is a must, because if I will say, you are the owner of that information, how will I know I'm the owner? So we need to educate these people [as to] why they are the owner of this information. Why do they have to make sure that this data or information is available [and is] rightly and governed right, so we will not create a separate entity to govern, maybe departments themselves can govern their data, and they will be responsible for their data" (P22)*
Organisational culture	*"If the culture of the bank depends mainly on pointing fingers and blaming, I think this data ownership is in a very high rate of issues. But if the culture is calmed and everything is transparent, as I mentioned earlier, I think people would fight to own data" (P32)*
Senior management support	*"These policies are first discussed and reviewed by our senior management. And of course, with their support, then all our policies are under the custody of compliance, and they monitor whether these policies are updated and reviewed in a timely manner" (P18)*

Table 20: Summary Findings—Factors shaping structural practices

6.3.2 Factors shaping procedural practices

This study identified various factors that enabled Omani banks in developing effective procedural practices. These included (1) adherence to laws and regulatory requirements; (2) adopting industry best practices; (3) use of new information technologies; (4) clear definition of policies and procedures; (5) and clear roles and responsibilities. Further discussion of these factors is provided in the following section:

6.3.2.1 Laws and regulatory requirements

This study found that laws and regulatory requirements have played a critical role in shaping procedural practices in Omani banks. This finding is expected since banks are mandated by law to have in place certain procedural practices (such as data retention and archiving) to comply with minimum regulatory requirements. Adopting industry standards like ISO and PCI DSS was further enhanced these procedural practices by ensuring banks are up-to data and in line with international standards. This in turn protects their customers' data and instils confidence in their customers that their data is secured.

6.3.2.2 Adoption of new information technologies

The use of advanced technologies like AI and big data analytics reshape how information is managed in organisations (Mikalef et al., 2018). The findings of this study further confirm this assumption by highlighting how new technologies were used to automate various structural practices, including information classification and data validation. Omani banks, for example, have used AI capabilities to automate account opening procedures, ensuring that mandatory fields are correctly captured as per the established policies and procedures. They also implemented a data leakage prevention system to monitor classified data and prevent unauthorized access or transmission outside the bank. Daily monitoring and auditing were conducted with the support of various systems to ensure compliance both organisational and regulatory requirements. Therefore, embracing new technologies can play a positive role in improving the maturity of procedural practices by automating various IG tasks.

6.3.2.3 Training

This study emphasised the importance of ongoing training and awareness programs to keep employees informed about the latest development in regulatory requirements and industry standards, which could affect how information is managed throughout its lifecycle. Effective training is also necessary to educate employees about the best practices for handling and securing data. Evidence from data showed that Omani banks conduct regular training for IT professionals to educate them on how to apply backup practices in a way that maintain critical data safe in a case of disaster. Overall, ongoing training can provide employees with the knoweldge and skills required to manage data effectively, securely, and efficiently.

6.3.2.4 Regular auditing and monitoring

Omani Banks conduct regular audits to ensure compliance with policies, standards, and regulations. When it comes to data quality, if the data is incomplete or inaccurate, it will be highlighted in audit observations and reported to various levels, including senior management, and the board of directors. To be more effective, different types of auditing were used, including internal and external auditors. Additionally, periodic reviews of customer data are conducted to ensure the accuracy and quality of customer information. System validations and trigger-based and product reviews are also performed. Without proper auditing, banks may fail to implement effective procedural practices, which could make them vulnerable to compliance risks.

Factor(s) name	**Evidence from data**
Laws and regulatory requirements	*"All our policies and procedures reflect the requirements of the law, and any other regulations set either by regulators or the best practices set out by international organizations such as FATF [Financial Action Task Force] and others" (P08)*
Use of new information technologies	*"Our compliance [department] is empowered by smart technologies such as machine learning, AI [Artificial Intelligence], big data analytics, helping [them] to make sense of complex patterns in data, identifying risks and compliance failures" (P16)*
Training	*"We have procedures to backup our data, we have procedures steps to do that. So, we cannot lose our data, because we have a BCM [Business Continuity Management] department. They are doing tests every month, they are educating the staff [on] how to backup the data, how to maintain it in case there is any pandemic, or if there is any disaster" (P34)*
Regular auditing and monitoring	*"We do frequent audits in all levels across the bank. We note down what type of negligence or what type of shortage and controls are there to allow this bad quality data to be inputted into our systems" (P35)*

Table 21: Summary Findings—Factors shaping procedural practices

6.3.3 Factors shaping relational practices

The study's findings revealed a number of factors that played a positive role in shaping relational practices in Omani banks. These factors included (1) laws and regulatory requirements; (2) funding availability; (3) organisational culture; (4) and senior management support.

6.3.3.1 Laws and regulatory requirements

The empirical findings suggest a relationship between regulatory compliance and training. It was found that the majority of participating banks have conducted regular training and awareness programs for their employees in order to comply with both national and international regulations. The Central Bank of Oman, for example, mandates banks and other financial institutions in Oman to provide mandatory training sessions on money laundering and data security. Additionally, it is critical for banks to adhere to these regulations to protect their reputation and market position, as non-compliance can lead to regulatory risks and loss of customer trust. Therefore, organizations tend to invest heavily in training their staff to comply with these regulations.

6.3.3.2 Funding availability

The study's findings suggest that having sufficient funding can enable Omani banks to provide specialised training programs tailored specifically for IG. Evidence from data showed that Omani Banks prioritise talent management by providing their employees with regular training and professional development opportunities. Moreover, they invest in ongoing training and awareness initiatives to keep their staff up-to-date on data security, data quality, and information management. Indeed, such initiatives require sustained funding and managerial support to ensure compliance with IG requirements, and mitigate risks associated with poor information management. Thus, having enough funding allows organisations to provide proper training to employees, and ultimately ensure effective implementation of IG practices.

6.3.3.3 Senior management support

This study emphasised the role of senior management in fostering a culture of continues learning, open communication and collaboration. With management support in place, all necessary IG requirements can be enabled. Likewise, empirical evidence showed that the participation of senior managers in various training and awareness programs can encourage employees to actively engage with these programs; thereby ensuring both employees and top management have a shared understanding of fundamental IG practices.

A summary of factors shaping relational practices are provided below.

Factor(s) name	**Evidence from data**
Laws and regulatory requirements	*“I think most banks in Oman do provide enough training, especially our organization because we're governed by a lot of entities, other than just CBO [Central Bank of Oman]. We have to follow CBO regulations, we have to follow BASELL. We have to follow CMA [Capital Market Authority] regulations, we have to follow Oman labour law, and all of these are linked with our reputation as a bank, or as an organization. So as an organization, you tend to spend on your people to elevate them.” (P21)*
Funding availability	*“From the training department itself. They always have a budget for the next year. And they communicate with other departments [to ask] what type of training you need for the next year. So if I talk about operational risk management, we have a budget in place for this year, to have awareness sessions for the staff and to educate them about data management and other relevant areas” (P43)*
Senior management support	*“The most important [thing] to keep this user [employee] engaged, is the management, it's a top-down. The good thing in our bank, again, is that it is driven [by] our CEO, and delivered by the security when it comes to giving awareness and training (P20)*

Table 22: Summary Findings—Factors shaping relational practices

6.4 Consequences of information governance

This section aims to discuss the impact of IG adoption on firm performance and risk mitigation. More specifically, it aims to discuss the factors and/or IG practices that help Omani banks to achieve intermediate performance effects and ML risk mitigation. The current study has successfully identified a number of factors and IG practices that contributed to achieve these outcomes. To the researcher’s best knoweldge, this is the first study the empirically explore the relationships between antecedents, IG practices, and consequences. The following discussion will elaborate more on how these factors or IG practices contributed in achieving the said outcomes.

6.4.1 Intermediate performance effects

The study’s findings revealed that the adoption of IG practices in Omani banks has led to significant improvements in their operational efficiency, customer service, data-driven decision making, and data quality. These findings supports evidence from previous research (Karkošková, 2022; Mikalef et al., 2020; Najdanović & Tutek, 2021; Okunleye, 2023; Tallon et al., 2013; Tyagi, 2021). While previous research has only focused on the ultimate outcomes of IG, this study goes a bit further by highlighting the conditions that can help organisations to achieve various intermediate performance effects. Analysis of interviews revealed the following factors/ IG practices: (1) data integration; (2) adoption of new information technologies; (3) application of data validation practices; and (4) organisational strategy.

Data integration helps IG professionals in Omani banks to retrieve all necessary data without having to chase users from different departments. IG professionals no longer require contacting IT staff to gather necessary information to carry out their tasks. For instance, compliance departments become more efficient in detecting suspicious transactions as data integration enables them to enforce all controls and rules into a single governance unit. Additionally, data integration enabled IG professionals in Omani banks to make informed decisions through the provision of quick access to accurate information. Likewise, by having a more comprehensive understanding of customers’ data, banks are better equipped to provide more personalized products and services. Therefore, it was evident that integrating customer data can positively enhance efficiencies of various banking operations.

Additionally, the study's findings showed that the adoption of new information technologies, such as AI, machine learning and big data analytics, have increased the productivity of employees across different departments in Omani banks. These technologies allowed IG professionals to automate routine IG tasks while directing their efforts to core activities that require critical thinking and cognitive skills. Therefore, resulting in relatively fewer human errors and more accuracy in data, which led to increased customer satisfaction and reduced complaints.

Furthermore, the interview data revealed that applying data validation practices has contributed positively in enhancing data quality, which in turn help Omani banks to take informed decisions based on accurate data. By regularly updating customer data, banks can personalize their products and offer tailored solutions that foster business growth. It is therefore crucial for banks to not only capture data but also ensure its accuracy, as this helps build a comprehensive understanding of customer behaviours and preferences. Empirical evidence also suggest that applying data validation practices, including data cleansing and KYC refresh, enhance compliance with laws and regulations by submitting high-quality reports to regulatory authorities.

Moreover, empirical findings showed that organisational strategy can play a critical role in improving firm performance. Digital transformation remains one of the cornerstones of the bank's business strategy, ensuring a distinctive customer experience while bringing about operational efficiencies and process optimisation. A vital component of Omani banks' strategy is to leverage innovation as a strategic enabler to create meaningful scale in revenue-generating opportunities and efficiencies. Overall, Omani banks putting their customers at the forefront of its business to create a holistic customer-centric offering. This in turn enabled them to provide better customer service.

The following table provide a summary of the factors / IG practices led to intermediate performance effects.

Factor(s) / IG practice(s)	**Evidence from data**
Data integration	*"So, when we collected the data from the different systems and store them in a single data hub, we [can] built the dashboards and reports, we could track a single transaction or a single service across different platforms. And that could help us to have better monitoring, better insights to the errors and mistakes where it falls, and to fix the root cause and better performance and, accordingly, better customer experience" (P40)*
Adoption of new information technologies	*"The automation and use of advanced technologies like AI and RPA [Robotic Process Automation] has brought significant efficiency improvements through the reduction of processing time and elimination of human errors, while at the same time increasing customer satisfaction and reducing complaints" (P19)*
Application of data validation practices	*"Updating and validating the data of the customers will be very helpful for the bank, growing in business in terms of customising the product and sell it to the customer based on their needs" (P08)*
Organisational strategy	*"The Bank's strategy is built on the voice of the customers and providing 'best in class' support to all the business lines and other functions in the Bank to become customer-centric. Digital transformation continues to be one of the cornerstones of the Bank's business strategy, ensuring a distinctive customer experience, while also bringing about operational efficiencies and process optimization" (P22)*

Table 23: Summary Findings—Factors and/or IG practices led to intermediate performance effects

6.4.2 Risk mitigation

The findings of this study showed that implementing effective IG practices has helped Omani banks to mitigate money laundering and compliance risks. The study identified several factors that contribute to these outcomes, including (1) data integration; (2) high-quality data; (3) effective oversight mechanisms; (4) compliance monitoring; (5) use of advanced technologies; (6) and organisational culture.

Data integration has played a critical in mitigating money laundering risks by enabling employees to get quick access to relevant KYC data. It also helps in providing a holistic view of customer data and thus, enabling effective monitoring of transactions. This in turn helps AML and compliance professionals to quickly identify suspicious transactions. When integrating customer data into a single database, banks can build accurate risk profile for each customer, enabling them to easily detect anomalies or patterns that indicate ML activities. Furthermore, having a single unit of governance can helped compliance professionals to reject accounts from known money launderers, thereby protecting the bank and the country as a whole. It is therefore important for banks to consolidate customer data from different sources to ensure effective governance of AML.

Reliable data is the core of money laundering detection and prevention. Having high-quality KYC data can help compliance officers better detect anomalies or suspicious transactions from large datasets and respond timely to ensure that suspicious transactions are detected and prevented before they are executed. Likewise, reliable data can enhance the productivity of AML officers by reducing the number of false-positive alarms; thereby directing their efforts to high-risk transactions.

Furthermore, this study highlighted the importance of compliance culture in mitigating money laundering risks by consistently communicating the impact of ML risks on the bank's reputation and performance. The interview data also showed that an organisational culture that promotes employees to report suspicious or illicit transactions can help in addressing potential ML cases before they happened. An effective compliance culture should start from the top –with the board of directors, and permeates throughout the entire organization. Likewise, it is argued that ensuring compliance with laws and regulations can mitigate money laundering risks by implementing best practices for collecting, protecting, and analysing ML-related data. Significant efforts have been made to promote a risk-minded culture across the Omani banks to ensure that compliance is not just a box to check but a fundamental part of banking operations. To sum up, a strong compliance culture is not just a requirement but a vital component for achieving sustainable IG.

Additionally, effective oversight mechanisms were found to be play a crucial role in reducing money laundering risks. Analysis of interviews showed that Omani banks have dedicated committees like the Board risk committee and financial crime committee to monitor policy implementation and ensure compliance with relevant laws and regulations. A review of banks' documents indicated that banks have a zero-tolerance policy against money laundering risks, which promoted the executive management to continuously enhance their oversights and compliance monitoring systems. Additionally, the board risk committee (BRC) manages is responsible to overseeing and ensuring compliance with laws and regulations. It is specifically responsible for ensuring that there is no significant risks related to ML data/ information, and KYC requirements.

Furthermore, the study’s findings revealed that the use of advanced technologies enabled Omani banks to effectively manage and analyse transactional data associated with money laundering. These technologies are particularly useful in analysing complex data, detecting suspicious transactions and compliance issues.

Lastly, it is important to recognise the management support in mitigating money laundering risks. Their support is instrumental in promoting a culture of compliance, securing the necessary fund, and fostering a sense of responsibility towards risk mitigation through effective governance of ML data/ information. However, the leadership's tone at the top is not just a factor, but a cornerstone in setting the standard for ethical behaviour and maintaining a robust compliance culture by following established IG policies and procedures.

Overall, the acknowledged findings on consequences enrich the existing body of knowledge on information governance by providing practical insights that can successfully inform policy development, and help Omani banks to mitigate money laundering risk through effective implementation of various IG practices. Table below provide a snapshot of factors and IG practices that contributes positively in reducing ML risks in the Omani banking sector.

Factor(s) / IG practice(s)	**Evidence from data**
Data integration	*“I think we become very highly efficient in terms of AML [Anti-money Laundering] by deducting all suspicious transactions, because your data is under the same umbrella and everything is in one place and assessment become very easy and it is controlled very well. Better than if it is split in other systems” (P05)*
Data quality	*“It's very important to have good data in order to manage the ML [Money Laundering] risks. Without data, you cannot do any analysis. Without the accurate data, you cannot even detect a suspicious transaction. So it's very, very essential, very*

	important to have quality data to run a good anti money laundering function" (P26)
Organisational culture	*"A strong compliance culture is the foundation of our ability to deliver prudent, sustainable growth and to mitigate financial crimes like money laundering (P16)*
Oversight mechanisms	*"The Bank has an anti-fraud and financial crime committee to monitor the financial crime related risks and provide direction to manage these risks" (P25)*
Compliance monitoring	*"Compliance with the various indicators and laws is monitored and reported on a regular basis and exceptions, if any are escalated to enable remedial actions" (P33)*
Use of new technologies	*"In relation to the data, obviously, maintaining a history of transactions and using artificial intelligence that has been built, so that we understand whether there's any suspicious activity on the account is really key to mitigate money laundering [risks]" (P17)*
Training	*"Proper training is provided to minimise the risk of wrong data getting entered into the system and which could lead to a potential money laundering" (P33)*
Senior management support	*"Instilling a strong compliance culture is a priority for both the Board of Directors and Executive Management. This is disseminated across the bank through various initiatives such as policies and procedures, circulars, staff training, awareness sessions" (P12)*

Table 24: Summary Findings—Factors and/or IG practices led to ML risk mitigation

6.4.3 The Relationships between Intermediate Performance Effects and Risk Mitigation

The analysis revealed that intermediate performance effects and risk mitigation are interconnected and affecting each other. Specifically, the integration of customer data into a single repository and the adoption of advanced technologies such as artificial intelligence and machine learning. This integration has led to increased productivity, reduced errors, and enhanced customer satisfaction in most organizations. These improvements not only support operational excellence but also act as foundational elements for effective and efficient risk mitigation. The proactive approach to IG practices was characterized by a customer-centric strategy, continuous training, and the adoption of digital transformation initiatives, this not only boosts business performance but also reinforces risk management capabilities. The findings also underlines the essence of integrating IG practices into the organizational strategy to accomplish both operational excellence and effective risk management. By nurturing a strong risk culture, employing robust risk management frameworks, and ensuring support and oversight from senior management, banks can better response to risks associated with money laundering. Hence, the relationship between intermediate performance effects and risk mitigation in the context of the banking sector revealed a symbiotic link between effective information governance (IG) practices and the mitigation of risks like money laundering.

6.5 Final research model

In light of the empirical findings of this study, the below IG model is proposed. The proposed model is specifically developed for the Omani banking sector. However, Banks with similar conditions and characteristics may also find it useful for developing their IG capacities. For finalisation purposes, a balance between enabling and inhibiting factors was carefully considered. For example, resources can act as enabled when adequately provided and inhibitor when withheld. This dual role has been integrated into the model to ensure its applicability across varying conditions. By acknowledging this duality, the model aims to provide a robust and adaptive framework that supports the Omani banking sector, and organizations in similar contexts. It emphasizes the importance of continuously evaluating and balancing these factors to maintain alignment with IG objectives and long-term strategic goals.

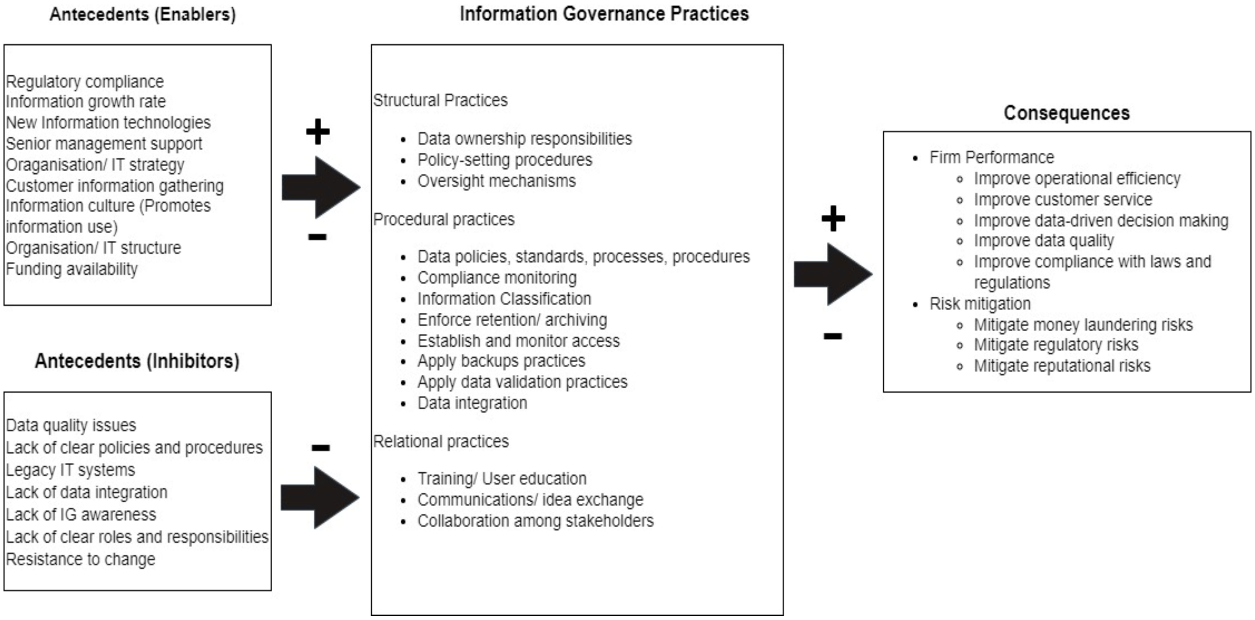

Antecedents (Enablers)
Regulatory compliance
Information growth rate
New Information technologies
Senior management support
Oraganisation/ IT strategy
Customer information gathering
Information culture (Promotes information use)
Organisation/ IT structure
Funding availability
Antecedents (Inhibitors)
Data quality issues
Lack of clear policies and procedures
Legacy IT systems
Lack of data integration
Lack of IG awareness
Lack of clear roles and responsibilities
Resistance to change
+
-
-
Information Governance Practices
Structural Practices
Data ownership responsibilities
Policy-setting procedures
Oversight mechanisms
Procedural practices
Data policies, standards, processes, procedures
Compliance monitoring
Information Classification
Enforce retention/ archiving
Establish and monitor access
Apply backups practices
Apply data validation practices
Data integration
Relational practices
Training/ User education
Communications/ idea exchange
Collaboration among stakeholders
+
-
Consequences
Firm Performance
Improve operational efficiency
Improve customer service
Improve data-driven decision making
Improve data quality
Improve compliance with laws and regulations
Risk mitigation
Mitigate money laundering risks
Mitigate regulatory risks
Mitigate reputational risks

Figure 7: Proposed Research Model

6.6 Chapter Summary

It can be concluded that the implementation of Information Governance (IG) practices in the Omani banking sector revealed a distinctive and context-specific landscape. The study identified crucial factors for mitigating money laundering risks, including compliance monitoring, data integration, adoption of new technologies, training and data quality. However, limitations, such as the specific focus on the Omani banking industry, the qualitative nature of the study, and the possibility of personal bias was acknowledged in the reporting of the findings. Despite the constraints faced in this study, the research stipulates valuable qualitative insights into IG practices, presenting a foundation for future studies and enhancing the understanding of the implementation of information governance practices in the Omani banking sector.

Chapter 7: Conclusion

7.1 Chapter Overview

The main aim of this thesis was to investigate the role of information governance practices in mitigating the risks of money laundering in the Omani banking sector. More specifically, it aimed to understand how various structural, procedural, and relational practices can aid Omani banks in improving their capacity in governing ML data/ information in a way that enable them to detect and prevent suspicious transactions associated with ML activities.

7.2 Addressing the Research Questions

This thesis sets out to answer the over-arching question: *How can various information governance practices help Omani banks in mitigating the risks of money laundering?*

In order to answer this question, the following four questions were posed.

RQ 1: What are the antecedents that enable or inhibit the adoption of IG practices in the Omani banking sector?

A) Enablers of information governance

This study identified eight factors that enabled Omani banks to adopt effective IG practices. These factors are: (1) Regulatory compliance, (2) information growth rate, (3) new information technologies, (4) senior management support, (5) Organisational/ IT strategy, (6) customer information gathering, (7) information culture, and (8) funding availability. These factors were also found to be interlinked and affected each other. Table 25 below summarise the enablers of information governance in the Omani banking sector, as identified in this study. It is worth noting that these factors are ranked based on their 'prevalence' and 'keyness'.

Enabler(s)	**Example from data**
Regulatory compliance	*"There are regulatory obligations to keep the [customer] information for a certain period of time, archive it. Now this is an ocean of work of regulations, international laws, treaties, policymakers sometimes locally sometimes outside because you're bound by certain agreements with outside banks…so, information governance is the way [to] handle that information in accordance with whatsoever rules or regulations that apply to that handling" (P48)*
Information growth rate	*"The data is in terabytes, and it's growing heavily, so soon we can be in the petabytes … from the overall growth perspective, it is a very huge growth, every month I think we are getting several terabytes of data being increased in our overall infrastructure"* (P23)
New information technologies	*"I think technology is one of the major enablers on the data, especially machine learning and big data analytics tools. That is one of the major enablers on that. When I say technology, in terms of where you're storing it, how you maintain it, retrieve it, and also on the aspect of security …" (P46)*
Senior management support	*"Our top management is well aware of the importance of data and the need for governance … So, there is a management buy-in. There is an intention, there is seriousness about the evolving and developing the data governance function [framework] …" (P25)*
Organisation/ IT strategy	*"From the IT perspective, we are aligning our IT strategy with the business to ensure that critical data is being served on a timely basis and all the security parameters that are required to ensure that data security is in place, data classification is being managed on all the different levels of applications" (P23)*
Customer information gathering	*"If you need to provide better service, better customer experience, be a market leader, you need to capture all this data about the customers" (P40)*
Information culture (Promotes information use)	*"So, from the top management, it was said that our way of designing a new product shouldn't be based on R & D [Research and Development]. It should also be based on analysis of our own data, so there*

	was a need to design better products, not based on R & D only, but more of our own data" (P27)
Funding availability	*"Necessary budget allocation is an enabler, having a proper budget allocation or budget plan with contingencies, done on an annual basis is an enabler for data governance" (P30)*

Table 25: Summary of IG enablers in the Omani banking sector

First, as shown in Table 25, regulatory compliance was identified as the biggest enabler for IG adoption in the Omani banks. The overwhelming majority of participants indicated that laws and regulatory requirements forced them to improve their current IG practices to ensure compliance with both national and international regulations, including FATF, AML, and PCI DSS. The interviews also showed that the rapid changes of regulations pushed banks to update and enhance their IG policies and procedures to ensure compliance with evolving regulatory requirements while staying competitive in the market by avoiding reputational damage associated with non-compliance. Second, the study found that the exponential growth of structured and unstructured data forced Omani banks to optimise their storage capabilities, and implement sophisticated approaches to protect and govern these information assets. Interestingly, regulatory requirements were identified as the main reason behind information growth in many interview sites. Compliance professionals of the current study reported that regulators (such as Central Bank of Oman) mandate them to collect and retain large volume of customer data for long period of time. Other internal reasons, however, were found to affect information growth in Omani banks, including (1) digitalisation, (2) expansion of digital services, (3) and increase use of big data analytics. Third, the findings of this study revealed that new technologies, particularly artificial intelligence, machine learning and big data analytics, enabled Omani banks to improve their information management capabilities by automating critical and routine IG tasks. For example, several IG professionals in this study acknowledge the role of ETL (Extract, Transform, and Load) technologies in facilitating and streamlining the collection of customer data that resides in diverse databases within the bank. They also added that new technologies helped them in enforcing different IG policies and procedures, including data retention and data classification. Fourth, this research emphasised the critical role of senior management support in driving the IG agenda in the Omani banking sector. This is not a surprising finding given that senior management has a higher level of authority and power over the organisation, which enabling them to overcome any financial, cultural, or technical obstacles that may hinder the implementation of IG practices. Interviewees frequently used the terms “lead by example”, and “governance by act” to highlight the importance of leadership involvement in various activities related to IG initiative. For those interviewees, senior management support is manifested in resolving conflicts associated with data ownership, allocating the necessary budget for training and IT infrastructure, and hiring specialised personnel in information governance. Fifth, empirical evidence showed that the alignment between IT and business strategies accelerate the implementation of IG initiative in the studied banks. Several IG professionals in this study stated that data growth is a key pillar of their IT strategy and planning, which led them to improve their IT infrastructure and storage capabilities to effectively manage current and future growth of data. Interestingly, interviews revealed that customer-centric strategy positively affects IG adoption, as banks have to rely on good quality data to provide more personalised products and services for their customers. Sixth, this research found that customer information gathering positively impacts IG adoption in Omani banks by enhancing customer service, developing new products, reducing operational costs, and ensuring compliance with regulations. Seventh, interviews revealed that information culture played a critical role in shaping IG practices by determining how information is used, accessed, shared, and managed within or outside the bank. Empirical evidence showed that data was perceived by many IG professionals as ‘new oil’ that can be leveraged to achieve their strategic goals and objectives. Additionally, the study’s findings emphasised the role of senior management in nurturing an information culture by encouraging their employees to use information for research and development and for making business decisions. Interestingly, regulatory requirements were identified as a key factor that shaping information culture in the Omani banking sector. Eighth, the current investigation found that funding availability enabled Omani banks to overcome many of roadblocks towards IG implementation. Participants reported that allocating adequate budget was critical to acquiring cutting-edge technologies, upgrading IT infrastructure, hiring IG professionals, and conducting training. Additionally, evidence from data suggests that the board of directors have provided compliance departments with a ‘blank cheque’ to invest on, and fund critical IG-activities (such as data cleansing and KYC reviews) to ensure compliance with regulatory requirements.

B) Inhibitors of information governance

On the other hand, this study identified several challenges that inhibit Omani banks to adopt IG practices. These included: (1) data quality issues, (2) lack of clear policies and procedures, (3) legacy IT systems, (4) lack of data integration, (5) lack of IG awareness, and (6) lack of clear roles and responsibilities. Similar to the enablers, it was noted that these inhibiting factors affecting each other, as a challenge in one area often exacerbates issues in others. For example, legacy IT systems can lead to data integration, which in turn results in data quality issues. A summary of these inhibitors is presented in Table 26 below.

Inhibitor(s)	**Example from data**
Data quality issues	*"The foremost important challenge is the data quality. It is common to every bank which has a long history. First banks had got the books, physical books, they switched to the core banking systems. They got certain information captured at the time and then from the legacy systems as we know that there have been multiple generations of core banking systems." (P24)*
Lack of clear policies and procedures	*"To be honest, it's the lack of policies and procedures in place. It's a big challenge. I can tell you, even if something goes wrong, you can't blame the staff. Sometimes the staff will tell you I'm not having policy and procedures in place. How would I know that I should follow this process or should not follow that process? So here it is a very big challenge" (P43)*
Legacy IT systems	*"In an industry like banking, it's not that easy to implement information governance practices because banks always come with legacy [systems] ... so, that is an inhibitor factor [which] holding us back from doing a lot of innovations and [digital] transformation" (P25)*
Lack of data integration	*"We have the customer data and financial data is spread in different systems. We have some data in the mobile/internet banking and we have data in the core banking system. And we have data in the reporting system. And we have data in the collection system. And to apply the governance in [of] each system is a challenge" (P47)*
Lack of IG awareness	*"I would put it at lack of awareness on the importance of certain aspects of data. I could give an example, when our people input the data, there are multiple columns which need to be selected as a drop down. And If the person is not understanding a particular aspect, he usually goes and selects others" (P33)*
Lack of clear roles and responsibilities	*"Unfortunately, we don't [have] clear roles and responsibilities. To be honest, that's what I told you*

	in the beginning, that we are taking baby steps in terms of data governance, we lack a lot" (P40)
Resistance to change	*"We have [data] standards. When we are implementing the standards, there is some kind of resistance among users [employees]" (14)*

Table 26: Summary of IG inhibitors in the Omani banking sector

As Table 26 suggests, data quality issues emerged as the biggest challenge that hinder IG adoption in Omani banks. Several IG professionals in this study used the phrase "garbage in, garbage out" to highlight the negative consequences of poor data quality on bank's performance. Various data quality issues were reported by participants, including wrong data entry, data inconsistences, incomplete/missing data, and outdated customer data. Evidence showed that these issues were compounded by inexperienced staff who lacked basic understanding on the importance of data, lack of data integration, lack of clear data quality procedures, and customer's reluctance to provide the necessary information. Interestingly, the competition to attract more customers has led some banks to bypass or ignore certain data quality requirements. Additionally, this study found that the lack of clear policies and procedures was another challenge hindering Omani banks to develop effective IG practices. Some participants attributed this problem to insufficient guidance on information governance from the central bank, which led to inconsistent interpretation and implementation of IG policies and procedures across Omani banks. Legacy IT systems were also identified as a barrier to IG adoption. Many IT professionals of this study reported difficulties in migrating data from these antique systems to modern IT infrastructure, due to compatibility issues, budget constraints, and lack of technical documentation. Interestingly, resistance to change and fear to adopt or learn new technologies were mentioned by some interviewees as key hurdles that prevented Omani banks to modernise or upgrade their legacy systems. However, empirical data revealed that legacy IT systems led to data silos, leading to inconsistent and poor data quality.

Likewise, the findings showed that the lack of data integration delayed many of data warehousing projects, making it challenging for Omani banks to maintain a single source of truth among disparate and unintegrated systems. Compliance professionals of this study expressed their struggles in applying consistent data policies across numerous data sources, hindering their ability to comply with relevant laws and regulations. In the same vein, the lack of IG awareness was identified as a significant barrier to IG adoption due to its association with poor data quality, data breaches, and non-compliance risks. Participants reported that employees, especially those who work in branches, often view data as a non-core business, and burden that waste their time and efforts. Evidence from data further suggest that the majority of front-office employees are unaware of the existing policies and procedures, nor their responsibilities in relation to information management. However, it was found that most of participating banks assign critical IG task such as data collection to non-specialised staff who lack basic skills and qualifications on information governance. Moreover, the findings revealed that the effectiveness of IG practices in Omani banks was hindered by a lack of clear roles and responsibilities. Various factors were found to contribute to this problem, including (1) lack of clear organisational structure, (2) lack of clear job description, (3) lack of training, (4) conflicting or overlapping responsibilities, and (5) cultural resistance (e.g., not accepting new responsibilities). For example, interviews suggest that some employees still believe that IT department are the owner of data, which lead to confusion and conflicts among different business department over data ownership. Additionally, it was noted that the organisational culture that based on blaming or finger-pointing complicates the assignment of data ownership responsibilities, as every employee feels he/or she is not the owner of the data. Lastly, resistance to change emerged as another important challenge that impedes Omani banks to embrace new technologies, or alter established practices. According to the interviews responses, this resistance often stem from a fear of losing power, comfort with current practices, lack of awareness, and cultural norms. It was interesting to note that employees with long years of experience were more hesitant to change compared to younger or inexperienced staff. This likely because older employees have greater familiarity with current systems and practices, which making them refuse to accept any changes that may disrupt their routines. For instance, some participants narrated their challenges in convincing their senior managers to use new information management tool for making decisions. However, empirical evidence suggest that Omani banks may resist to change their current practices, because "*employees are still in the early stage of understating how important data is*" (P22). Therefore, it is important for employees to be trained on the benefits of IG before embracing any changes.

RQ 2: What information governance practices have Omani banks adopted to manage their ML-related data or information?

Consistent with Tallon et al.'s (2013) framework, this study identified three different types of governance practices (structural, procedural, relational) that Omani banks have adopted to manage their information assets –including ML data/ information. These practices emerged from both inductive and deductive coding (discussed in the Methodology Chapter). Structural practices involve allocating data decision-making authority to key stakeholders; assigning data ownership responsibilities; determining reporting structure; establishing governance or oversight committees; and setting high-level groups for policy-setting and monitoring. Procedural practices concerning with how information is managed throughout its lifecycle from the moment it created or captured to its archiving or deletion. They aim to ensure that information is collected, stored, accessed, shared, and archived in a manner that is align with established organisation's policies and regulatory requirements. Relational practices, on the other hands, focus on establishing a supportive environment for IG initiative by fostering collaboration, communication, and trust among stakeholders within the organisation. They encompass (1) training; (2) communication/ ideas exchange; and (3) collaboration among stakeholders. The following sub-sections provide a summary of key findings for various IG practices being adopted by Omani banks to manage their information assets.

A) Structural practices

This study identified three structural practices that Omani banks have adopted to ensure effective management of their information assets, as summarised in Table 27 below. However, it should be acknowledge that the implementation of these structural practices may vary across different banks based on specific contextual factors, such as organisational structure, organisational culture, and senior management support. First, data ownership responsibilities seems to be well-established in Omani banks as evident in interviews data and documents review. Interviews showed that Omani banks have adopted a variety of approaches –notably the responsibility assignment matrix (RACI) and three line of defence model—to facilitate the assignment of data ownership responsibilities. Additionally, the majority of participants confirmed that they have been informed about their roles and responsibilities regarding information management during the early stage of recruitment process (i.e., orientation period). In line with the study’s findings, it was noted that data ownership is often assign to business users (e.g., compliance professionals) who engage directly with, or collect data from customers. Our review of documents further indicate that data ownership responsibilities, including data quality and data security are well-documented in the banks’ policies and procedures. Second, the study’s findings showed that Omani banks have followed a structured process to develop, implement, review, update, and approve policies and procedures related to information governance. As indicated by those involved, data policies and procedures were developed in collaboration with stakeholders from different departments, including IT, information security, legal, compliance, and internal audit. However, it was suggested that the policy owners have the sole responsibility to develop the initial draft of their policies and procedures. Additionally, empirical findings revealed that all policies and procedures are regularly reviewed and updated—typically every one to two years—to ensure they remain relevant and compliant with current regulations and organisational needs. Compliance professionals of this study acknowledged their role in this process by monitoring and overseeing policy implementation. Similarly, the board of directors and senior management were found to be actively involved in policy development process by providing the final approvals of policies, reflecting the high-level oversight of policy-setting. The results of this study revealed that Omani banks have developed robust oversight mechanisms for information governance, despite the absence of dedicated IG committees in most of the interviewed banks. Analysis of interviews showed that Omani banks have shared IG oversight with a wide range of committees, including risk management committee, information security steering committee, IT steering committee, audit committee, and board committee. Additionally, some of these banks have extended IG oversight to multiple departments—such as compliance, risk management, information security, and internal audit—to ensure the enforcement of data-related policies and procedures throughout the whole organisation. Therefore, it was clear from the interviews that Omani banks applied a top-down oversight mechanisms to oversee and monitor critical activities related to data/ information.

Structural practice(s)	**Example from data**
Data ownership responsibilities	*"The three lines of defence model basically assigns [data] ownership to the first line of defence. And when I say the first line of defence I'm talking about the businesses, and they are supported by the second line of defence … [including] compliance, risk management, finance, HR …[However] the third line of defence is the assurance and it's usually the internal audit team. So, the three lines of defence is the approach that we took to define [data] ownership and accountability" (P42)*
Policy-setting procedures	*"All our policies are under the custody of compliance, and they monitor whether these policies are updated and reviewed in a timely manner. And then these policies go to the board of directors for the review and approval. So this is basically the chain on policies development" (P44)*
Oversight mechanisms	*"The oversight mechanism is part of the group risk committee; anything which is related to the data. That's why one of the things which we say is any incident in the bank, you have to have a copy of that incident, if it is related to the data, or it is touch indirect or direct to the data. Definitely they step in and take the necessary action" (P46)*

Table 27: Summary of structural practices adopted by Omani banks

B) Procedural practices

Analysis of procedural practices revealed a plethora of activities that Omani banks have adopted to manage their information throughout different stages of information lifecycle—i.e., from creation to archival or deletion. Various procedural practices were identified by IG professionals of this study, including (1) data policies, standards, processes, procedures; (2) compliance monitoring; (3) information classification; (4) data retention/ archiving; (5) user access control; (6) backups; (7) data validation; and (8) data integration. Interestingly, these practices were frequently mentioned by participants as evident in their prevalence/ frequency counts across the dataset. This may be attributed to the complexity of money laundering data/ information, which require daily management and monitoring to ensure compliance with established policies and procedures. Table 28 below provides a summary of the procedural practices identified in this study.

Procedural practice(s)	**Evidence from data**
Data policies, standards, processes, procedures	*"We have information security policy …we have a user access control management policy. We also have a cryptography and encryption security policy … we have backup and [data] retention policy …" (P34)*
Compliance monitoring	*"In each of our audit engagements, we look at compliance with the policies, compliance with the standards, compliance with the regulations … wherever we see that the data is incomplete or not accurate, or the data does not properly represent the actual situation or the latest regulatory requirements … then we highlight [that] in our audit observation, and it goes to various levels like … the board of directors [or] senior management" (P44)*
Information classification	*"We do classify our data [based] on the value. There is a criterion for that, we have classification guidelines … Also, we consider the regulation part,*

	how important of [is] this data … So, all this is part of the [information] classification [policy]. The first [thing] is value and [then] criticality of this information" (P20)
Enforce retention/ archiving	*"As a policy, we [have to] keep all AML [Anti-money laundering] related data for 10 years minimum. Where there are STRs [Suspicious Transaction Reports], for example, we must even maintain this data longer than the 10 years" (P27)*
Establish and monitor access	*"All classified data in the bank is monitored by a data leakage prevention system. The system prevents any unauthorized or [if] you want to send this data outside, because it's classified by nature, by context, there are rules and policies that have been implemented on this system to trigger if there is any unauthorized task on this information" (P20)*
Apply backup practices	*"Yes we perform backup. We have two types of backup here: full backup and [incremental]. For full backup, we take full backup, at night, daily at 10pm … for all the databases. And [incremental] backup every one hour, for all the databases too" (P41)*
Apply data validation practices	*"We have now started the periodic reviews of customers' data and we have done the system validations … we created multiple fields in the onboarding system, and we made them mandatory so that we should be getting the information which we need, for example, income level of the customer, occupation of the customer, his date of birth, nationality, FATCA [Foreign Account Tax Compliance Act] related information" (P27)*

Table 28: Summary of procedural practices adopted by Omani banks

C) Relational practices

The study's findings showed that Omani banks have developed effective relational practices by providing continuous training for employees; using different communication methods for sharing IG-related information; and engaging key stakeholders in IG activities. To begin with, training and user education were repeatedly appeared throughout the interview data. The overwhelming majority of participants indicated that their banks conduct regular training and awareness programs, which cover areas related to information security, money laundering, and information management. They added that these training programs are mandatory for all employees including the board of directors. Interestingly, training requirements were linked to employees' key performance indicators (KPIs) to ensure that employees stay up-to-date with latest updates in industry regulations and best practices pertaining information governance. Participants reported that failure to complete these training requirements will result in mandatory retakes, and negative performance in the employee's appraisal, which in turn affect promotions and bonuses. Many Omani banks included in this study have used a variety of methods to deliver training and awareness programs, including online learning, classroom sessions, and one-to-one coaching. Additionally, this study found that Omani banks used different communication methods to keep employees informed about various aspects related to IG, such as policy updates or regulatory changes. These methods included emails, text messaging, social media, meetings, posters, infographics, and intranet websites. Interviews, however, showed that the use of these communication methods varied across banks based on their size, structure, culture and IT infrastructure. For example, it was found that larger banks with extensive employees and complex organisational structures tended to employ advanced digital communication tools—e.g., intranet websites and social media platforms, as compared to smaller banks that often use emails and face-to-face meetings. To engage staff effectively, some participants reported that their banks have used creative methods such as cartoons and visual contents to communicate complex IG policies or procedures in a more digestible manner. This study also revealed that collaboration among stakeholders have proven to be well-established in Omani banks. This collaboration was particularly evident in areas related to policy development, policy revision, information classification, compliance monitoring, and training. For instance, some information security professionals reported how different departments like IT and risk management helped them in developing real-life scenarios to evaluate employees' awareness on various aspects relate to cyber-security and data breaches. Lastly, evidence from data showed that Omani banks have adopted collaborative tools –e.g., Microsoft teams—to streamline information sharing among key stakeholders.

Relational practice(s)	**Evidence from data**
User education/ Training	*"We have two main mandatory courses which have been managed by the training department. [One] is about money laundering, and the other [is about] information security, which are mandatory to all the staff to attend … In that [these] course[s], we … assure that our employees have got enough knowledge about the data classification, data governance and other aspects" (P46)*
Communication/ idea exchange	*"We send emails, and we conduct awareness sessions in order to communicate any new policy or changes to employees. We do site visits, different methods that could assist us in making them [employees] understand" (P35)*
Collaboration among stakeholders	*"And we have to re-review all the documents and [policies] with the cooperation of the business lines [departments], not only the AML" (P18)*

Table 29: Summary of relational practices adopted by Omani banks

RQ 3: What are the consequences of adopting IG practices on firm performance and risk mitigation in the Omani banking sector?

A) Intermediate performance effects

Analysis of interview data revealed a number of intermediate performance effects that Omani banks have achieved through the implementation of various IG practices. These included (1) improved operational efficiency; (2) improved customer service; (3) improved data-driven decision making; and (4) improved data quality. However, it is worth noting that these consequences may differ across banks, due to the variation in the organisational capabilities (such as IT infrastructure, senior management support, funding), plus the maturity of IG practices. In the context of this study, for example, it was found that banks that invest in new technologies like AI and big data analytics, and integrate their customer data into a single data repository, are likely to achieve higher operational efficiencies. Table 30 provides a nutshell of the intermediate performance effects identified in this study.

First, the empirical findings showed that the adoption of IG practices in Omani banks have led to higher operational efficiencies. Respondents across various departments including AML, information security, and internal audit highlighted how the ease of accessing the information—i.e., having the right information at the right time—has improved their productivity and work performance. In the compliance departments, for example, participants spoke how the integration of customer data helped them in detecting suspicious transactions, reducing false-positive alarms, and enhancing the efficiency of risk assessment. In the information security departments, information governance was associated with better prediction of cyber security attacks. Whereas, in the internal audit departments, it enhanced the accuracy of audit findings, and reduced the time needed for audit assignments.

Second, this study found that effective IG has led to significant improvements in customer service. Several interviewees reported how accurate and complete information about customers enabled them to design more personalised products and services by better understanding customers' behaviours and needs. For example, retail professionals in this study indicated that the easy access to credit card data allowed them to upgrade eligible customers to higher credit card tiers, which provide card holders with exclusive discounts and rewards – including access to airport lounges.

Third, analysis of interviews revealed that IG adoption enabled Omani banks to make informed decisions based on accurate, complete, and relevant information. Several participants highlighted the critical role of data in making decisions related to AML, accounts opening, credit scoring, and customer segmentation. For example, compliance professionals of this study indicated that having access to complete and accurate KYC (Know-Your-Customer) data helped them to take a quick decision whether to close or report a suspicious transaction to the financial intelligence unit (FIU).

Fourth, this study found that information governance was associated with enhanced data quality by ensuring that data is effectively managed and maintained across different departments and IT systems. Participants confirmed that the continuous monitoring and auditing of customer data have positively impacts data quality by reducing data errors and enhancing compliance with data quality requirements, which in turn led to better work performance. In this study, high quality data was found to be contributed in making accurate decisions, enhancing transactions monitoring, identifying suspicious transactions, and complying with laws and regulatory requirements.

Intermediate performance effects	**Evidence from data**
Improve operational efficiency	*"Positive impacts definitely would include ease of access to the information … [therefore] back and forth between compliance and other departments or branches would be less. quicker assessments of customers" (P08)*
Improve customer service	*"[The] more information you are having about the customer [the] better you will serve the customer … [because] if we have the relevant and accurate information, we will be in a better position to serve the customers. We will be in a better position to know the needs and wants of the customer. So, we can design the products according to the requirements of customers" (P27)*
Improve data-driven decision making	*"So that data is critical to the decision making, either I accept the transaction or I reject or I send a suspicious report to FIU [Financial Intelligence Unit]" (P32)*
Improve data quality	*"Information is the hub of the organization and governing it will not cause any issue in the bank. It's the other way, it will benefit, it will have [provide] right information, accurate information …" (P20)*

Table 30: Summary of intermediate performance effects identified in this study

B) Risk mitigation

In addition to the above outcomes, this study found that the adoption of IG practices has played a positive role in mitigating the risks of money laundering in the Omani banking sector. This finding is particularly important in this context, as it provides an answer to the main research question posed in the introduction chapter. To the researcher's best knoweldge, this is the first study that empirically investigate the role of information governance in ML risk mitigation.

The majority of compliance professionals in this study emphasised the importance of data in money laundering detection and prevention. They revealed that accurate and complete KYC data were essential in detecting, preventing, and monitoring suspicious transactions associated with ML activities. High quality KYC data was also associated with enhanced transaction monitoring by accurately classifying customers into the appropriate risk categories–i.e., high, medium, low.

Additionally, interviews showed that the integration of customer data enhanced accuracy of risk assessments by allowing quick access to KYC data. In the this study, integrating KYC data was deemed necessary not only for creating accurate risk profiles, but also for enhancing the efficiency of compliance monitoring. Compliance professionals of this study reported that data integration helped them in reducing the time required for collecting customer data from desperate data sources, which had a positive impact in identifying and reporting suspicious transactions. Table 31 below provides a summary of IG impacts on risk mitigation.

Risk(s) mitigation	**Evidence from data**
Mitigate money laundering risks	*"I think we [become] very highly efficient in terms of AML [Anti-money laundering] by detecting all suspicious transactions, because data is under the same umbrella and everything is in one place and assessment will be very easy and it will be controlled very well. Better than if it is split in other systems … " (P26)* *"If we collected the right KYC data and take policies and procedures seriously from the frontline until the CEO [Chief Executive Officer]. If*

	that happened … we could fight 80%-90% of money laundering …we will reduce the risk on the bank from an AML perspective" (P12)
Mitigate compliance risks	*"Without the data, it's very difficult and tedious to mitigate the compliance risks. So only, it's with a strong data, strong information governance in place, we are able to mitigate our compliance risks" (P24)*

Table 31: Summary Findings—Consequences of IG on risks mitigation

RQ 4: What are the similarities and differences across Omani banks in relation to the antecedents, IG practices and consequences? How might these practices or the governance of ML-related data/ information be improved?

This research question was answered by conducting cross-case analysis (presented in Chapter 5).

7.3 Contributions to Knowledge

This thesis makes significant contributions to practice, theory, and methodology, as described in the following sub-sections.

7.3.1 Empirical contribution

This research has contributed empirically to the field of information governance and money laundering, filling a notable gap in the existing literature. By conducting in-depth interviews with different IG professionals from nine Omani banks, this study provides strong empirical evidence on the effectiveness of information governance in mitigating money laundering risks; thereby supporting the theoretical claims about the usefulness of IG practices in financial crimes detection and prevention (Kristian, Alfajri, Oktavia, Nofitriandi, & Teguh, 2022; Soares, 2011; Tyagi, 2021). To the best knoweldge of the researcher, this is the first empirical study that investigate this phenomenon in Oman and the Middle East region. Additionally, the current research adds to the existing knoweldge by empirically identifying a set of IG practices that contributed to ML risk mitigation in the Omani banking sector. This contribution is particularly vital for AML scholars and practitioners who seek to incorporate evidence-based IG practices into their existing AML frameworks.

This study also contributes to the existing knoweldge by empirically identifying the antecedents that enable or inhibit the adoption of IG practices in the Omani banking sector. The literature is almost silent on the factors that influence IG adoption in the banking industry (Faria, Maçada, & Kumar, 2013). The empirical findings revealed specific challenges that hinder Omani banks to develop effective IG practices. Such challenges include data quality issues, lack of data integration, legacy IT systems, product complexity, and resistance to change. Similarly, the study identified several enabling factors that facilitate the implementation of IG practices in Omani banks.

Additionally, the current research improves our understanding on the consequences of information governance on firm performance and risk management. It was argued that selling information governance to banking executives is difficult due to the lack of direct or immediate returns which often delay the project investment and approvals (Soares, 2011). The empirical data showed how effective IG practices helped Omani banks to improve their overall performance by increasing operational efficiency, enhancing data quality, ensuring compliance with regulations, and mitigating money laundering risks. Therefore, these findings contribute to the debate about the value and business opportunities of IG in the banking sector (Fernando Faria & Simpson, 2013; Okunleye, 2023; Parameswarappa, 2022; Tyagi, 2021).

Lastly, the theoretical framework of information governance (Tallon et al., 2013) was the subject of empirical contribution. By analysing from nine Omani banks, this research provides strong evidence on the applicability and relevance of the theoretical constructs outlined in Tallon et al.'s framework to the banking industry.

7.3.2 Theoretical Contribution

The study's outcomes contribute to the growing body of knoweldge on information governance and money laundering in three ways. First, it provides a 'novel' insights into the role of information governance in money laundering context, extending the IG landscape to financial crimes and risk management fields. While much of AML research focus on technology and regulatory approaches to address the money laundering problem, this research offer a unique perspective by highlighting how various IG practices can increase the efficiency of compliance officers in detecting and preventing suspicious transactions through effective governance of ML data/ information. To the researcher's knoweldge, this is the first study that empirically explore the role of information governance on ML risk mitigation. Second, this study fills a crucial gap in the IG literature by operationalising the theoretical framework of information governance (Tallon et al., 2013) into a real-world context of the Omani banking sector, uncovering various empirical findings related to antecedents, governance practices, and consequences. The banking sector is a relatively unexplored area in the existing IG literature; therefore the study's findings established a foundation for future research endeavours in this domain. Third, this study contributes to the existing knoweldge by proposing a 'new' IG model (presented in section 6.5) that tailored specifically to the Omani banking sector. The proposed model offers valuable insights for IG scholars who seek to understand the impact of local conditions (such as organisational culture, senior management support and IT infrastructure) in shaping IG practices in the Middle Eastern banking sector in general, and Sultanate Oman in particular. By doing so, the study addresses a notable gap in the IG literature, which has mainly focused on Western contexts (e.g., Faria, Maçada, & Kumar, 2013), without paying sufficient attention to Middle Eastern countries like Oman (Al Wahshi, Foster, & Abbott, 2022). This theoretical contribution is particularly valuable in this context because it provides academics and practitioners with a model supported by initial empirical evidence, which can serve as a foundation for further research. Furthermore, banks with comparable conditions and regulatory environment can use this model as a benchmark to evaluate, refine, and improve their current IG practices. For practitioners, the proposed model offers a structured and systematic framework to enhance IG practices within banking institutions. The model is designed to address sector-specific challenges such as money laundering, regulatory compliance, data security, and operational efficiency, which are paramount in a highly regulated and competitive environment like banking. For stakeholders, including regulatory bodies, policymakers, and senior management within banking institutions, the proposed model serves as a roadmap for enhancing governance of ML-related data/ information. Policymakers, for example, can use the model as a benchmark to design regulations that promote sustainable and effective governance practices across the banking sector. Overall, the proposed model equips stakeholders with the tools needed to navigate the evolving complexities of information governance and risk management banking.

Additionally, this research contributes to the theoretical framework by Tallon, Ramirez, and Short (2013) in many aspects. The empirical findings shed ‘new’ light on the relationships among different elements of the framework, demonstrating how different factors interact with each other to shape specific IG practices. For example, the findings showed how organisational structure, senior management support, and training shaped structural practices, and how regulatory requirements, IT infrastructure, new technologies, and clear roles and responsibilities shaped procedural practices. Moreover, this study goes beyond Tallon's (2013) framework by identifying which conditions and/or IG practices can led to intermediate performance effects and risk mitigation. Previous research has only focused on the direct outcomes of information governance, without sufficiently exploring the factors that precede these outcomes (Karkošková, 2022; Okunleye, 2023). The current study was able to offer a framework (see section 6.5) for mitigating ML risks by identifying a set of factors and IG practices that could help banks in mitigating such risks. By uncovering the connections among different components of the framework, the study offers important theoretical insights that can be used to enhance existing IG models.

7.3.3 Methodological Contribution

The methodological contribution of this study lies in its novel application of the collective case study approach to study information governance. Unlike previous research that used traditional approaches such as a single case study (e.g., Alhassan et al., 2019; Muhammad et al., 2022), surveys (e.g., Mikalef et al., 2018), or mixed methods (e.g., Okunleye, 2023), this study offers a significant departure from these methods by investigating IG capabilities across different types of Omani banks—including regulatory, local, Islamic, specialised, and foreign. By examining multiple banks, the research enhances our understanding not only on the similarities and differences, but also how the characteristics of each bank influence the development of these IG capabilities. Additionally, the cross-case analysis helps in enhancing the transferability of the results by producing a more compelling conclusion grounded in diverse set of empirical data. Moreover, studying multiple cases help in overcoming one-sided views of the phenomenon and thus strengthen the validity and reliability of the findings. To the researcher's best knowledge, this is the first that investigate information governance using multiple case study approach.

In line with the above contributions, this study has drawn its conclusions from a large dataset using two data collection methods: semi-structured interviews and documents review. This combination has provided a comprehensive understanding of the research problem by enabling triangulation of data sources, thus enhancing the validity and reliability of the study's findings. Conducting semi-structured interviews were helpful to explore the context and obtain deep insights into the Omani banks' experiences on IG adoption, whereas documents review was helpful to cross-validate the data obtained from the interviews.

7.4 Recommendations for practice and policy

The results of this study were obtained through in-depth interviews with key IG professionals from multiple Omani banks. These IG professionals who recruited from various departments—included IT, information security, compliance, risk management, legal, and internal audit—have provided insights into the current IG practices, enablers, inhibitors, opportunities, and suggestions for IG improvement. These insights provide various practical implications for practice and policy, which may be of interest to Omani banking institutions, compliance and AML officers, and Central Bank of Oman (CBO).

7.4.1 Omani banking institutions

7.4.1.1 Conduct comprehensive IG training

This study emphasised the importance of training in raising employees' awareness on various aspects of information governance, including its principles, goals, risks and opportunities. While training and user education were evident in Omani banks, there is a need to further develop this area. Participants from different Omani banks indicated that some employees, particularly those who work in branches and front-offices, are unaware of the importance of information, nor the policies and procedures associated with it. They added that those employees are unaware of their roles and responsibilities in relation to information management. Interestingly, evidence from data suggests that some senior managers lack understanding of information risks and their impacts on the bank's performance. Therefore, this study recommends Omani banks to conduct a comprehensive training for all employees at different organisational levels—from junior staff to the board of directors. This training should be tailored for specific roles within the bank, particularly those involved in information management and compliance. For example, customer service representatives need to be trained on how to collect the necessary KYC data as per the AML/ compliance policy. Additionally, participants highlights the need to make these training programs more engaging and interactive by using practical exercises (e.g., hands-on workshops), and real-life case studies. This engagement could be enhanced by incorporating participatory training methods such as quizzes and group discussions. Equally important, it is crucial for Omani banks to assess the level of employees' awareness on IG by conducting regular assessments and surveys. Lastly, training and awareness programs need to be frequently updated in order to ensure employees are aware of the latest changes of regulatory requirements, data threats, and IG practices.

7.4.1.2 Develop an information governance strategy

Several IG professionals of this study recognised the need to establish an information governance strategy before embarking on any IG initiatives. Despite this recognition, it was noted that the majority of Omani banks still lack a formal IG strategy or policy. It is therefore important for Omani banks to develop an effective data strategy to ensure a successful IG implementation. This strategy should clearly defined the scope of work, goals, benefits, and types of information to be collected or governed. To be more effective, it is highly recommended to align this strategy with the bank's overall business objectives. This is a critical step to recognise IG as a core strategic pillar within the organisation. Additionally, the interviews emphasised the need for management buy-in to ensure the necessary resources and support are dedicated to the strategy. Presenting the data strategy as a comprehensive business case with clear goals and benefits is the key to obtaining this support. This approach will help in obtaining the necessary approval and support from the senior management.

7.4.1.3 Establish a dedicated IG committee

The results of this study showed that the majority of Omani banks included in this study lack a formal IG committee for overseeing information-related activities and issues. Instead, IG oversight responsibilities are scattered across various committees and departments, leading to inconsistent and fragmented oversight. Therefore, it is highly recommended for Omani banks to establish a dedicated information governance committee to improve their current IG practices. This committee should comprise senior managers and key stakeholders from various departments, including IT, information security, compliance, risk management, internal audit, and legal. The involvement of key stakeholders in the committee was deemed critical to ensure that the IG decisions are made in a more transparent and responsible manner. Lastly, the IG committee must be approved by the board to lend it the necessary authority and support.

7.4.1.4 Assign clear data ownership responsibilities

This study highlighted the importance of assigning clear data ownership responsibilities to promote the transparency in managing enterprise information. However, conflicts among departments may arise when these responsibilities are not clearly defined or overlapping, leading to blaming and finger-pointing. Executive management in Omani banks can play a critical role in mitigating these issues. First, business departments should be recognised as the primary owner of data, because they are the ones who use and understand the value of their data. IT department should serve as an enabler, providing the necessary systems and infrastructure to support information governance. Second, it is imperative that every data set within the bank to be assigned to specific individuals or teams. Of course, these responsibilities should also linked to the job description of employees avoid confusion. Third, employees must be trained about their data ownership responsibilities to ensure that they fully understand what data ownership entails. Fourth, the bank's policies and procedures should include a responsibility matrix (RACI) outlining the roles and responsibilities of data owners. Finally, regular audits and compliance check are recommended to ensure that data owners are adhering to their roles and responsibilities.

7.4.1.5 Integrate data into a single data repository

The findings of this study emphasised the importance of integrating banking data into a unified database to improve IG capabilities by providing a single source of truth. While the interview data suggests that data integration can improve data quality and decision-making processes, other findings revealed that banking data is often scattered across different systems. It is therefore recommended that Omani banks, particularly those with complex products and services, to develop a comprehensive plan for data migration project. This project should begin with a comprehensive evaluation of the current situation of enterprise data, followed with a needs assessment to understand the specific bank’s data integration requirements. Next, the bank need to select the right technologies to facilitate data migration across different systems. IG professionals of this study have recommended to use extract, transform, and load (ETL) technologies to accomplish this task, as they are proven to be effective for this activity. Finally, it is important to perform data quality check to validate the integrity of data after the migration.

7.4.2 Compliance and AML professionals

- Compliance and AML professionals, as the gatekeepers of money laundering, must stay informed about emerging technologies, trends, and practices in order to effectively manage money laundering risks. This study recommends those employees to attend a comprehensive IG training to familiarise themselves with various practices, which may help them in ML risk mitigation. To be more effective, this training should be tailored to their specific needs.
- This study recommends compliance professionals to be part of the IG committee since they are the ones who responsible for ensuring compliance with laws and regulatory requirements. Being part of the committee can enable them to raise any concerns or suggest any changes for improving the current IG practices in the organisation.

- Compliance and AML professionals should maintain open communication with the regulatory bodies, such as the Central Bank of Oman, to stay updated on the latest development or changes on the information requirements pertaining money laundering.
- Compliance professionals are encouraged to read through this thesis in order to get better understanding on how various IG practices can be applied in real-world context for ML risk mitigation.

7.4.3 Central Bank of Oman

Based on the findings of this study, regulators like the Central Bank of Oman might benefit from addressing gaps in existing laws and regulations and potential areas for improvement by considering some suggestions related to the implantation of IG practices. The following suggestions are related to enhancing data governance frameworks, strengthening risk management practices, promoting digital transformation, facilitating continuous training and education, and strengthening regulatory oversight.

- First, the Central Bank of Oman (CBO) as a governing body in the country is responsible to overseeing and regulating the banking operations in Oman. While CBO puts significant efforts to combat money laundering risks, this study highlights the need for CBO to establish new regulations for information governance a part from the existing AML regulations. The new IG regulation should be flexible enough to allow banks with limited resources and capabilities to comply with its regulatory requirements.
- Second, regulators should encourage financial institutions to adopt robust data governance frameworks that address data integration, data quality, and system accessibility to support operational efficiencies, decision-making, and customer service.

Offering guidance on best practices for data governance might include data ownership, data classification, and stewardship responsibilities in the organizational systems.

- Third, regulators ought to encourage financial institutions to invest in innovative digital transformation initiatives that can advance IT infrastructure, boost data analytics capabilities, and introduce innovative digital services in their operations. The regulators can provide support and incentives to encourage the adoption of advanced technologies such as artificial intelligence, big data analytics, and robotic process automation to promote operational excellence and customer satisfaction.
- Fourth, regulators can endorse continuous training and education programs in organizations for staff members to increase awareness of information governance principles, risk management practices, and compliance requirements. This can be achieved through offering necessary resources and training opportunities to empower employees in nurturing the necessary skills and knowledge needed for effective management of information assets and risk mitigation.
- Fifth, the regulators should enhance regulatory oversight through the adoption of proactive monitoring and enforcement mechanisms to certify compliance with existing laws and regulations. This can be done by creating dedicated committees and oversight structures, such as financial crime committees and risk management boards, to monitor policy implementation, evaluate compliance levels, conduct frequent system audits, and address emerging risks. By addressing these suggestions, regulators like the Central Bank of Oman can aid in strengthening information governance practices in the Omani

financial sector, promote regulatory compliance, and boost overall stability and resilience in the implementation of IG practices across the sectors.

- Lastly, CBO may consider establishing a cross-sectoral national databank, which holds relevant financial information, including KYC records and transactional data, to facilitate information sharing across the banking sector. This centralised platform would allow banks and other financial institutions to easily access to accurate and up-to-date information necessary for customer verification, fraud detection, and risk assessment. While such a centralized system offers significant benefits, such as enhanced efficiency, improved compliance with regulatory requirements, and streamlined customer verification processes, it also introduces potential risks that must be acknowledged and mitigated.

  Centralized systems inherently concentrate vulnerabilities, making them attractive targets for cyberattacks. For instance, recent incidents like the Snowflake data breach of Santander highlight the risks of compromised credentials and misconfigurations. These risks include unauthorized access, privacy violations, operational disruptions, and potential biases in data handling. To address these risks, effective cyber security measure must be implemented. These measures should include applying advanced encryption techniques, multi-factor authentication (MFA), role-based access controls, and conducting regular vulnerability assessments and audits. The CBO may also consider to adopt international standards such as ISO/IEC 27001, which provide a structured approach to cybersecurity and risk management.

7.5 Limitations and Future Research

While this research has advanced the current understanding of the role of information governance practices in mitigating money laundering risks, there are some limitations identified which need to be acknowledged here, and worth being considered in future research.

- First, small number of case studies limits the current study. Including only nine out of nineteen Omani banks may not fully represent and capture the experiences of the whole sector. The excluded banks might have unique contextual factors or practices that are not considered in the current study. This limits the transferability of findings to other Omani banks. However, this study does not aim to generalise the findings to a wider banking sector, but rather it seeks to gain in-depth understanding of IG practice across the selected banks. In spite of this, an effort has been made to mitigate this limitation by carefully selecting representative banks from different categories, including regulatory, local, specialised, and foreign. Second, the current research focuses on the Omani banking sector, which means that the findings may not be applicable to banks in other countries. This raises a concern to the external validity of the study. Third, the COVID-19 pandemic has presented unexpected challenges to the research process. Unfortunately, the data collection stage coincided with the COVID-19 outbreak, which restricted access to important information such as policy documents and minutes of meetings. Additionally, due to social distancing measures, most interviews were shifted from face-to-face to virtual meetings, preventing the researcher from conducting focus group discussions which could provide richer data. Despite these challenges, this data was able to collect a rich dataset from a large number of participants, thereby ensuring a wide range of perspective and insights were still captured. Fourth, the qualitative nature of this study, while offering in-depth insights, may constrain the ability of the researcher to objectively measure the relationships of different components of IG framework. Using qualitative design may also lead to potential bias in interpreting and analysing data, which might impact the objectivity of the study. Fifth, the use of theoretical framework may influence how the data is collected and themes are developed. While frameworks provide valuable structure and guidance for research, they can also impose certain limitation. In particular, the analysis could be skewed towards predefined categories and constructs, which could limit the development of new or unexpected themes. To overcome this limitation, this study was adopted both inductive and deductive coding. Sixth, the dearth of empirical studies in the area of information governance and money laundering make it challenging to compare and link the study's findings with existing literature. Lastly, due to the time limit given for completing this PhD project, this study was only focused on banks, thereby excluding other financial institutions such as money exchanges and financial leasing companies

To address the above limitations, this study provides the following insights and suggestions for future research:

- Future researchers should consider including a more diverse range of banks from the same categories (i.e., local, foreign, Islamic, and specialised banks). Including a larger sample from each category could provide a more nuanced understanding of IG practices across the Omani banking sector, which could enhance the transferability of the study's findings.

- Future studies may expand the scope of this study by incorporating other financial institutions, such as money exchanges, Fintech companies, and financial leasing companies. This approach would enable an in-depth exploration of how the unique contextual factors of each institution influence the implementation of IG practices. Additionally, comparing and contrasting these factors could provide practical insights for tailoring IG practices to the specific needs of diverse financial institutions.
- More studies need to be carried out to test and validate the applicability of the proposed model (presented in section 6.6) in different banks with similar conditions.
- This study may be repeated using a mixed-method approach. Future researchers may employ quantitative methods, such as regression analysis and chi square, to test the relationships between various IG components (i.e., antecedents, IG practices, consequences) and their impact on ML risk mitigation. Likewise, statistical techniques might be used to quantify the impact of specific IG practices in mitigating M=money laundering risks.
- Another promising avenue that can be considered by future research encompasses the adoption of longitudinal studies; this would deliver a comprehensive understanding of how IG practices have advanced over time. Observing the evolution of these practices in real-world scenarios would allow researchers to discern patterns, and adaptations, and recommend sustainable solutions to rapid changes in technology, regulatory frameworks, and criminal strategies. This longitudinal approach is particularly

appropriate in the fast-paced scene of the banking sector, where the capability to adapt IG practices to emerging challenges is supreme for sustained effectiveness.

- Furthermore, future research endeavours could explore the synergies between new technologies—such as machine learning, artificial intelligence, and big data analytics, and their potential to augment IG and risk mitigation in the banking sector. Investigating how these technologies can be successfully leveraged to improve information governance practices suggests a forward-looking perspective. Understanding the integration of innovative technologies with established IG frameworks signals the potential to revolutionize risk management strategies, strengthening the banking sector's resilience against emerging threats. It also promotes service delivery in a safe and secure environment that acknowledges the need for laws and regulations to govern data privacy, data protection, and information security in financial institutions.
- Lastly, future studies may use grounded theory to develop themes from the data rather than imposing pre-existing frameworks. This can reveal new insights and patterns that might not have been considered in the current study.

7.6 Reflection on the Research Journey

This section aims to reflect on the experiences and lesson learned at different stages of the PhD journey. It also provides a critical evaluation on my personal and professional development as a researcher, highlighting some core competencies—such as critical thinking, resilience, time management, and academic writing— that were developed during this process. According to (Kolb, 2014), reflection refers to the internal process through which individuals critically assess their experiences to derive meaning and transform knowledge into actionable insights. It serves as a bridge between experience and learning, allowing individuals to conceptualize abstract ideas from concrete occurrences and apply them in future contexts (Kolb, 2014). Drawing on Kolb's definition, this section articulates how the reflective practices have allowed me to navigate the complexities of the PhD journey, overcome challenges, enhance my skills, and adapt to evolving demands of the research process.

The journey of conducting this research into information governance in the banking sector has been both transformative and instructive. Initially, the scope of the study was broad, with the aim to provide a comprehensive understanding of IG practices across the sector. However, as the research progressed, it become evident that focusing on specific problem will yield more meaningful insights. This necessitated narrowing the scope of the study to focus on the most critical aspects for the banks such information management practices, money laundering, and regulatory compliance. This practice allowed me to stay focused and concentrated on the key themes that may contribute in addressing the research questions. For instance, my initial plan was to include a wider range of banks from different categories (i.e., regulatory, local, Islamic, foreign and specialised), which then revised to focus on a more manageable sample size to ensure deeper analysis within the given time and resource constraints.

During my research journey, I noted how my belief and perspective have been changed from a student seeking knoweldge to a researcher who contribute to the body of knoweldge. I began to see myself as independent researcher who is able to critically evaluate existing theories, identifying gaps, and proposing new insights. This shift in perspective was particularly evident during the data collection and analysis phases, where the complexity of real-world banking practices challenged my initial assumptions and required me to adapt and refine my frameworks. Reviewing and synthesizing the literature has also played a critical role in shaping my research approach and understanding. It allowed me to identify gaps in existing studies, draw connections between disparate findings, and position my work within the broader academic discourse on information governance.

My ontological and epistemological stance has shaped the way in which I collected and analysed the data in this research. Ontologically, information governance is recognised as a social phenomenon that shaped by the interactions, experiences, and perceptions of different stakeholders. This influenced my decision to collect data from a wide range of participants, including regulatory bodies, IT professionals, compliance officers, internal auditors, and senior management, to investigate IG phenomenon from different perspectives within the context of the Omani banking sector. Epistemologically, my interpretivist view that IG is a reality existing within the subjective experiences of stakeholders has influenced the methodological choices of this research by adopting qualitative methods, such as semi-structured interviews and case studies.

Throughout the research process, several challenges emerged, particularly in accessing proprietary data and navigating the complexities of organizational politics. However, COVID-19 was one of the major challenges I encountered during my research journey, necessitating adaptability and resilience. The disruptions caused by the pandemic required me to reconsider and adjust my research plans, particularly in terms of data collection, stakeholder engagement, and time management. One of the most immediate challenges was the difficulty in accessing participants for data collection. Many of the stakeholders I planned to interview were either unavailable or operating under considerable pressure due to the pandemic. To mitigate these challenges and their potential impact on the research, I implemented several measures, including revising timelines, adopting flexible methodologies, leveraging digital tools for data collection, and seeking regular guidance from supervisors.

Conducting this research has been a transformative experience in my development as a researcher. The process has honed my skills in critical thinking, methodological rigor, and stakeholder engagement. Working closely with banking institutions provided valuable exposure to the practical challenges of implementing governance frameworks, enhancing my ability to bridge theoretical constructs with real-world applications. Additionally, this research has improved my communication and problem-solving skills. Collaborating with diverse stakeholders required articulating complex ideas clearly and negotiating access to sensitive data.

Establishing trust and fostering collaboration with participating banks proved to be a critical learning curve. The banks' varying levels of openness and readiness to share information highlighted the importance of adaptive communication strategies and ethical considerations in research. To address this, I prioritized clarity and transparency, ensuring that the objectives, scope, and potential benefits of the research were clearly articulated to each bank. This included emphasizing how the study aligned with their operational priorities, such as compliance, risk management, and strategic decision-making. Additionally, I adopted a flexible approach, accommodating the preferences of stakeholders in terms of meeting formats, timelines, and the level of detail provided during discussions. Through this process, I gained valuable insights into the importance of building trust and demonstrating respect for organizational cultures and constraints. This experience not only enhanced my interpersonal and negotiation skills but also underscored the critical role of ethical integrity and adaptability in conducting research within complex real-world settings like the banking sector.

Looking ahead, this research has opened avenues for further investigation into the role of IG practices in mitigating the risks of money laundering in the banking sector. These future directions will not only build upon the current study's findings but also contribute to the broader discourse on information governance in an increasingly data-driven world. In conclusion, this research journey has been a profound learning experience, offering both intellectual and practical insights.

References

Abdul Halim, N., M. Yusof, Z., & Azan M. Zin, N. (2018). The Requirement for Information Governance Policy Framework in Malaysian Public Sector. *International Journal of Engineering & Technology*, *7*(4.15), 235. https://doi.org/10.14419/ijet.v7i4.15.22996

Abdullah, A. L., Mohammad Yusof, Z., & Mokhtar, U. A. (2020). Factors influencing the implementation of electronic records and information management: A case study in military service in Malaysia. *Records Management Journal*, *30*(1), 81–99. https://doi.org/10.1108/RMJ-10-2018-0043

Abraham, R., Schneider, J., & Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*(July), 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Aguboshim, F. C., Ezeasomba, I. N., & Oko, F. P. (2019). Sustainable Information and Communication Technology (ICT) for Sustainable Data Governance in Nigeria: A Narrative Review. *Journal of Information Engineering and Applications*, (August). https://doi.org/10.7176/jiea/9-5-02

Al-Ruithe, M., & Benkhelifa, E. (2017). Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy. *Procedia Computer Science*, *113*, 223–232. https://doi.org/10.1016/j.procs.2017.08.352

Al Ghassani, A., Al Lawati, A., & Suryanarayana, A. (2017). *Banking Sector in Oman: Strategic Issues, Challenges and Future Senarios*. Muscat: College of Banking and Financial Studies.

Al Wahshi, J., Foster, J., & Abbott, P. (2021). An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector. *IConference 2021*.

Al Wahshi, J., Foster, J., & Abbott, P. (2022). An investigation into the role of data governance in improving data quality: A case study of the Omani banking sector. *ECIS 2022 Research Papers*. Retrieved from https://aisel.aisnet.org/ecis2022_rp/121

Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, *22*(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Alhassan, I., Sammon, D., & Daly, M. (2019a). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, *36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Alhassan, I., Sammon, D., & Daly, M. (2019b). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, *36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Alhassan, I., Sammon, D., & Daly, M. (2019c). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, *36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Alhojailan, M. I., & Ibrahim, M. (2012). Thematic Analysis : A Critical Review of Its Process and Evaluation. *WEI International European AcademicConference Proceedings*, *1*(2011), 8–

21.

Alldridge, P. (2003). *Money laundering law: Forfeiture, confiscation, civil recovery, criminal laundering and taxation of the proceeds of crime*. Bloomsbury Publishing.

Alldridge, P. (2008). Money laundering and globalization. *Journal of Law and Society*, *35*(4), 437–463. https://doi.org/10.1111/j.1467-6478.2008.00446.x

Aluko, A., & Bagheri, M. (2012). The impact of money laundering on economic and financial stability and on political development in developing countries: The case of Nigeria. *Journal of Money Laundering Control*, Vol. 15, pp. 442–457. https://doi.org/10.1108/13685201211266024

Antwi, S. K., & Kasim, H. (2015). Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection. *European Journal of Business and Management*, *7*(3), 217–226. Retrieved from https://www.researchgate.net/publication/295087782

Arasa, R., & Ottichilo, L. (2015). Determinants of know your customer (KYC) compliance among commercial banks in Kenya. *Journal of Economics and Behavioral Studies*, *7*(2), 162–175. Retrieved from http://ir.mksu.ac.ke/bitstream/handle/123456780/4841/574-Article Text-574-1-10-20160308.pdf?sequence=1&isAllowed=y

ARMA International. (n.d.). Information Governance. Retrieved September 1, 2023, from https://www.arma.org/page/Information_Governance#:~:text=Information Governance Defined&text=It establishes the authorities%2C supports,business requirements and risk tolerance

ARMA International. (2019). ARMA International Information Governance Implementation Model [IGIM]. Retrieved July 24, 2020, from https://www.arma.org/page/igim?&hhsearchterms=%22information+and+governance%22

Azmoodeh, A., & Dehghantanha, A. (2020). Big data and privacy: Challenges and opportunities. In *Handbook of Big Data Privacy*.

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative Research Journal*, *18*(4), 383–400. https://doi.org/10.1108/QRJ-D-18-00035

Ballard, C., Compert, C., Jesionowski, T., Milman, I., Plants, B., Rosen, B., & Smith, H. (2014). *Information Governance Principles and Practices for a Big Data Landscape*. IBM Redbooks.

Bank Muscat. (2019). *Annual Report 2019*. Retrieved from https://www.bankmuscat.com/en/investorrelations/AnnualReports/English Annual Report 2019.pdf

Barbazza, E., & Tello, J. E. (2014). A review of health governance: Definitions, dimensions and tools to govern. *Health Policy*, *116*(1), 1–11. https://doi.org/10.1016/j.healthpol.2014.01.007

Basaran-Brooks, B. (2022). Money laundering and financial stability: does adverse publicity matter? *Journal of Financial Regulation and Compliance*, *30*(2), 196–214. https://doi.org/10.1108/JFRC-09-2021-0075

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, *13*(4), 544–559.

Bazel, M., Mohammed, F., & Ahmed, M. (2021). Blockchain technology in healthcare big data management: Benefits, applications and challenges. *2021 1st International Conference* *on Emerging Smart Technologies and Applications, ESmarTA 2021*, (August). https://doi.org/10.1109/eSmarTA52612.2021.9515747

BBC News. (2012). HSBC to pay $1.9bn in US money laundering penalties. Retrieved June 28, 2020, from https://www.bbc.com/news/business-20673466

BCBC. (2020). *Sound management of risks related to money laundering and financing*. Retrieved from https://www.bis.org/bcbs/publ/d505.pdf

Beath, C., Becerra-Fernandez, I., Ross, J., & Short, J. (2012). Finding value in the information explosion. *MIT Sloan Management Review*, *53*(4), 18–20.

Becher, D., & Frye, M. (2011). Does regulation substitute or complement governance? *Journal of Banking and Finance*, *35*(3), 736–751. https://doi.org/10.1016/j.jbankfin.2010.09.003

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bennett, S. (2017). What is information governance and how does it differ from data governance? *Governance in Practice*, (September), 462–467. Retrieved from https://www.sibenco.com/information-governance-and-data-governance/

Biersteker, T., & Eckert, S. (2007). *Countering the financing of terrorism*. Routledge.

Blaikie, N. W. H. (2010). *Designing social research: the logic of anticipation* (Second edi). Cambridge: Polity.

Borgman, H., Boekamp, T., Heier, H., & Bahli, B. (2016). Dotting the I and Crossing (out) the T in IT Governance : New Challenges for Information Governance. *Hicss*, 4901–4909. https://doi.org/10.1109/HICSS.2016.608

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative*

Research Journal, *9*, 27. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Braun, V., & Clarke, V. (2013). *Successful qualitative research: a practical guide for beginners*. London: Sage.

Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. *ECIS 2015 Proceeding*, 0–18. Retrieved from http://aisel.aisnet.org/ecis2015_cr%0Ahttp://aisel.aisnet.org/ecis2015_cr/20

Brien, J. O., & Dixon, O. (2013). *The Common Link in Failures and Scandals at the World ' s Leading Banks*. 941–972.

Brinkmann, S., & Kvale, S. (2015). *Interviews: Learning the craft of qualitative research interviewing* (Third edit). Thousand Oaks: Sage.

Broek, M., & Addink, H. (2013). Prevention of money laundering and terrorist financing from a good governance perspective. In *Research Handbook on Money Laundering* (pp. 368–378). https://doi.org/10.4337/9780857934000.00039

Bruno, E., Iacoviello, G., & Lazzini, A. (2017). Data quality and data management in banking industry. Empirical evidence from small Italian banks. In *Lecture Notes in Information Systems and Organisation* (Vol. 20, pp. 21–40). https://doi.org/10.1007/978-3-319-49538-5_2

Bryman, A. (2004). *Social Research Methods* (2nd ed.). Oxford: Oxford University Press.

Buchanan, B. (2004). Money laundering - A global obstacle. *Research in International Business and Finance*, *18*(1), 115–127. https://doi.org/10.1016/j.ribaf.2004.02.001

Bureau of Counterterrorism. (2019). *Country Reports on Terrorism 2019*. https://doi.org/10.5860/choice.44-4105

Capgemini. (n.d.). *Information Governance for Financial Institutions*. Retrieved from www.capgemini.com/financialservices

Carrington, I. (2006). Protecting the financial system from abuse: Challenges to banks in implementing AML/CFT standards. *Journal of Money Laundering Control*, Vol. 9, pp. 48–61. https://doi.org/10.1108/13685200610645210

Cassella, S. (2018). Toward a new model of money laundering: Is the “placement, layering, integration” model obsolete? *Journal of Money Laundering Control*, *21*(4), 494–497. https://doi.org/10.1108/JMLC-09-2017-0045

CBO. (n.d.). Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT). Retrieved August 15, 2023, from https://cbo.gov.om/Pages/AntiMoneyLaundering.aspx

CBO. (2019). Oman Credit and Financial Information Centre (Mala’a). Retrieved August 2, 2023, from https://cbo.gov.om/Pages/Malaa.aspx

CBO. (2020). Cautionary Notice on the Use of Cryptocurrencies. Retrieved July 21, 2020, from https://cbo.gov.om/news/186

Central Bank of Oman. (2016). Promulgating the Law on Combating Money Laundering and Terrorism Financing. Retrieved from https://cbo.gov.om/Pages/AntiMoneyLaunderingLaw.aspx

Central Bank of Oman. (2019). *Annual Report 2018*. https://doi.org/10.3934/Math.2019.1.166

Central Bank of Oman. (n.d.). Anti-money Laundering and combat Financial Terrorism. Retrieved July 21, 2020, from https://cbo.gov.om/Pages/AntiMoneyLaundering.aspx

CESSDA. (2020). *Data Management Expert Guide*. Retrieved from https://www.cessda.eu/DMGuide

Choo, C. W. (2013). Information culture and organizational effectiveness. *International Journal of Information Management*, *33*(5), 775–779. https://doi.org/10.1016/j.ijinfomgt.2013.05.009

Choo, C. W., Furness, C., Paquette, S., Van Den Berg, H., Detlor, B., Bergeron, P., & Heaton, L. (2006). Working with information: Information management and culture in a professional services organization. *Journal of Information Science*, *32*(6), 491–510. https://doi.org/10.1177/0165551506068159

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, *26*.

Cohen, L., Manion, L., & Morrison, K. (2017). Research Methods in Education. In *Research Methods in Education*. https://doi.org/10.4324/9781315456539

Collis, J. (2014). *Business research: a practical guide for undergraduate & postgraduate students* (Fourth edi). Houndmills, Basingstoke, Hampshire.

Coyne, E., Coyne, J., & Walker, K. (2018). Big Data information governance by accountants. *International Journal of Accounting and Information Management*, *26*(1), 153–170. https://doi.org/10.1108/IJAIM-01-2017-0006

Creswell, J. W. (2007). Research Design: Qualitative, Quantitative and Mixed Method Aproaches. *SAGE Publications*, 203–223. https://doi.org/10.4135/9781849208956

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W., & Poth, C. (2017). *Qualitative inquiry and research design: choosing among five approaches* (4th edn). Los Angeles: SAGE Publications, Inc.

Crotty, M. (1998). *The foundations of social research : meaning and perspective in the research process*. London : London .

Dadashzade, A. (2018). Data Quality in Banking System: Case of Azerbaijan. *International Journal of Finance & Banking Studies (2147-4486)*, *7*(2), 1–8. https://doi.org/10.20525/ijfbs.v7i2.877

DAMA International. (2010). DAMA guide to the data management body of knowledge. *Technics Publications*.

Daneshmandnia, A. (2019a). The influence of organizational culture on information governance effectiveness. *Records Management Journal*, *29*(1–2), 18–41. https://doi.org/10.1108/RMJ-09-2018-0033

Daneshmandnia, A. (2019b). The influence of organizational culture on information governance effectiveness. *Records Management Journal*, *29*(1–2), 18–41. https://doi.org/10.1108/RMJ-09-2018-0033

De Abreu Faria, F., Gastaud Maçada, A. C., & Kumar, K. (2013). Information governance in the banking industry. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4436–4445. https://doi.org/10.1109/HICSS.2013.270

Deakin, H., & Wakefield, K. (2014). Skype interviewing: reflections of two PhD researchers. *Qualitative Research*, *14*(5), 603–616. https://doi.org/10.1177/1468794113488126

Delgosha, M., Hajiheydari, N., & Fahimi, S. (2021). Elucidation of big data analytics in banking: a four-stage Delphi study. *Journal of Enterprise Information Management*, *34*(6), 1577–

1596. https://doi.org/10.1108/JEIM-03-2019-0097

Demetis, D. (2010). *Technology and anti-money laundering: A systems theory and risk-based approach*. Edward Elgar Publishing.

Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE handbook of qualitative research. In *Handbook of qualitative research* (Fifth edit). Los Angeles: Sage.

Devers, K. J., & Frankel, R. M. (2000). Study design in qualitative research--2: Sampling and data collection strategies. *Education for Health*, *13*(2), 263.

Donaldson, A., & Walker, P. (2004). Information governance - A view from the NHS. *International Journal of Medical Informatics*, *73*(3), 281–284. https://doi.org/10.1016/j.ijmedinf.2003.11.009

Dyché, J., & Evan, L. (2006). *Customer data integration: Reaching a single version of the truth* (7th ed.). John Wiley & Sons.

Dyer, W. G., & Wilkins, A. L. (1991). Better Stories, Not Better Constructs, to Generate Better Theory: A Rejoinder to Eisenhardt. *The Academy of Management Review, 16*(3), 613–619.

EDRM.net. (2012). Information Governance Reference Model (IGRM). Retrieved July 24, 2020, from https://www.edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–550.

Eisenhardt, K. (2007). Theory Building from Cases: Opportunities and Challenges. *Organizational Research Methods*, *50*(1), 25–32.

https://doi.org/10.1177/0170840613495019

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Faria, Fernan, Maçada, A., & Kumar, K. (2013). Information governance in the banking industry. *The Annual Hawaii International Conference on System Sciences*, (Ketchum), 4436–4445. https://doi.org/10.1109/HICSS.2013.270

Faria, Fernando, & Simpson, G. (2013). Bridging the gap between business and it: An information governance perspective in the banking industry. *Data Governance: Creating Value from Information Assets*, 217–240. https://doi.org/10.1201/b15034

Farquhar, J. D. (2012). *Case Study Research for Business* (Vol. 7). https://doi.org/10.7748/nr2000.01.7.2.5.c6109

FATF. (2011). *Mutual Evaluation of the Sultanate of Oman*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER Oman full.pdf

FATF. (2015a). *Guidance for a risk-based approach: Virtual Currencies*. Retrieved from www.fatf-gafi.org

FATF. (2015b). *Guidance for a risk-based approach: Virtual Currencies*. Retrieved from www.fatf-gafi.org

FATF. (2017). *Consolidated FATF standards on information sharing*. Retrieved from www.fatf-gafi.org

FATF. (2022). The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. In *FATF*. Retrieved from www.fatf-gafi.org/recommendations.html

FATF. (2023). *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*. Retrieved from www.fatf-gafi.org/recommendations.html

Font, N. (2000). Debating Governance. Authority, Steering, and Democracy. In *OUP Oxford*.

Foster, J., McLeod, J., Nolin, J., R. (2018). Data work in context: Value, risks, and governance. *Journal of the Association for Information Science and Technology*, *69*(12), 1414–1427. https://doi.org/10.1002/asi.24105

Foster, J., McLeod, J., Nolin, J., & Greifeneder, E. (2018). Data work in context: Value, risks, and governance. *Journal of the Association for Information Science and Technology*, *69*(12), 1414–1427. https://doi.org/10.1002/asi.24105

Gage, nl. (1989). The Paradigm Wars and Their Aftermath A “Historical” Sketch of Research on Teaching Since 1989. *Educational Researcher*, *18*(7), 4–10. https://doi.org/10.3102/0013189X018007004

Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control*, *10*(2), 170–179. https://doi.org/10.1108/13685200710746875

Gartner. (2019). Information Governance. Retrieved February 22, 2020, from https://www.gartner.com/en/information-technology/glossary/information-governance

Gill, M., & Taylor, G. (2004). Preventing money laundering or obstructing business? Financial companies’ perspectives on ‘know your customer’procedures. *British Journal of Criminology*, *44*(4), 582–594. https://doi.org/10.1093/bjc/azh019

Gilmour, P. (2023). Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering. *Journal of Financial Crime*, *30*(1), 35–47. https://doi.org/10.1108/JFC-02-2022-0041

Given, L. (2008). *The SAGE Encyclopedia of Qualitative Research Methods*. https://doi.org/10.4135/9781412963909

Gray. (2004). *Doing research in the real world*. Sage publications.

Grembergen, W., Haes, S., & Guldentops, E. (2011). Structures, Processes and Relational Mechanisms for IT Governance. *Strategies for Information Technology Governance*, 1–36. https://doi.org/10.4018/9781591401407.ch001

Grimstad, T., & Myrseth, P. (2011). Information governance as a basis for cross-sector e-services in public administration. *2011 International Conference on E-Business and E-Government, ICEE2011 - Proceedings*, 8027–8030. https://doi.org/10.1109/ICEBEG.2011.5887109

Grix, J. (2002). Introducing Students to the Generic Terminology of Social Research. *Politics*, *22*(3), 175–186. https://doi.org/10.1111/1467-9256.00173

Grix, J. (2004). *The foundations of research*. Basingstoke: Basingstoke : Palgrave Macmillan, 2004.

Guba, E. ., & Lincoln, Y. . (1994). *Competing paradigms in qualitative research: Handbook of qualitative research* (vol. 2). Retrieved from http://steinhardtapps.es.its.nyu.edu/create/courses/3311/reading/10-guba_lincoln_94.pdf

Gubrium, J., & Holstein, J. (2012). Handbook of Interview Research. In *Handbook of Interview Research* (pp. 83–102). https://doi.org/10.4135/9781412973588

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. *Academy of Business, Engineering and Science Halmstad University, Sweden*, 1–15. https://doi.org/January 12, 2017

Hagmann, J. (2013). Information governance - beyond the buzz. *Records Management Journal*, *23*(3), 228–240. https://doi.org/10.1108/RMJ-04-2013-0008

Hammond, M. (2013). *Research methods: the key concepts*. New York, N.Y.: Routledge.

Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance*, Vol. 2, pp. 211–239. https://doi.org/10.1007/s42521-020-00023-1

Hancock, D., & Algozzine, B. (2006). *Doing case study research: A practical guide for beginning researchers*. https://doi.org/10.1039/c8dt02254b

Hesse-Biber, S. N., & Leavy, P. (2010). *The practice of qualitative research*. Sage.

Holmes, J. H. (2016). Privacy, Security, and Patient Engagement: The Changing Health Data Governance Landscape. *EGEMs (Generating Evidence & Methods to Improve Patient Outcomes)*, *4*(2), 9. https://doi.org/10.5334/egems.164

Hopton, D. (2009). *Money laundering: a concise guide for all business* (2nd editio).

Hughes, J., & Sharrock, W. (1997). *The Philosophy of Social Research* (Third edit). London.

Hulme, T. (2012). Information governance: Sharing the IBM approach. *Business Information Review*, *29*(2), 99–104. https://doi.org/10.1177/0266382112449221

IBM. (2014). *IBM Information Governance Solutions*.

IMF. (2010). Oman: Banking Sector Resilience. https://doi.org/10.5089/9781451982060.001

International Monetary Fund. (2008). The Impact of Weak AML/CFT Frameworks on Financial Stability. In *Current Developments in Monetary and Financial Law* (pp. 367–376).

Irwin, A., & Turner, A. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control*, *21*(3), 297–313. https://doi.org/10.1108/JMLC-07-2017-0031

Isa, Y., Sanusi, Z., Haniff, M., & Barnes, P. (2015). Money Laundering Risk: From the Bankers' and Regulators Perspectives. *Procedia Economics and Finance*, *28*(April), 7–13. https://doi.org/10.1016/s2212-5671(15)01075-8

Israel, M., & Hay, I. (2006). *Research Ethics for Social Scientists*. https://doi.org/http://dx.doi.org/10.4135/9781849209779

Issah, M., Antwi, S., Antwi, S. K., & Amarh, P. (2022). Anti-money laundering regulations and banking sector stability in Africa. *Cogent Economics and Finance*, *10*(1). https://doi.org/10.1080/23322039.2022.2069207

Jaffery, I., & Mughal, R. (2020). Money-laundering risk and preventive measures in Pakistan. *Journal of Money Laundering Control*, *23*(3), 699–714. https://doi.org/10.1108/JMLC-02-2020-0016

Jayasekara, S. (2020). How effective are the current global standards in combating money laundering and terrorist financing? *Journal of Money Laundering Control*, *24*(2), 255–265. https://doi.org/10.1108/JMLC-05-2020-0047

Johnson, J. (2001). In Pursuit of Dirty Money: Identifying Weaknesses in the Global Financial System. *Journal of Money Laundering Control*, *5*(2), 122–132.

https://doi.org/10.1108/eb027298

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173–186. https://doi.org/10.1108/JMLC-07-2019-0055

Kanellis, P., & Papadopoulos, T. (2009). Conducting Research in Information Systems. In *Information Systems Research Methods, Epistemology, and Applications* (pp. 1–34). https://doi.org/10.4018/978-1-60566-040-0.ch001

Karkošková, S. (2022). Data Governance Model To Enhance Data Quality In Financial Institutions. *Information Systems Management*, *00*(00), 1–21. https://doi.org/10.1080/10580530.2022.2042628

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148. https://doi.org/10.1145/1629175.1629210

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, *0*(0), 1–9. https://doi.org/10.1080/0142159X.2020.1755030

Kooiman, J. (1999). Social-Political Governance. *Public Management: An International Journal of Research and Theory*, *1*(1), 67–92. https://doi.org/10.1080/14719037800000005

Kooiman, J. (2003). *Governing as Governance*. London: Sage.

Kooiman, J. (2008). Interactive governance and governability. *Journal of Transdisciplinary Environmental Studies*, 1–11. https://doi.org/10.4337/9781783479078

Kooiman, J., & Bavinck, M. (2005). *Fish for life: Interactive governance for fisheries*. https://doi.org/10.1017/9789048505326.002

Kooper, M., Maes, R., & Lindgreen, R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, *31*(3), 195–200. https://doi.org/10.1016/j.ijinfomgt.2010.05.009

Kot, M. (2021). Money laundering as a major risk to the stability of the banking industry. *Wrocław University of Economics*, *65*(4), 77–93. https://doi.org/10.15611/pn.2021.4.05

Krauss, S. E., & Putra, U. (2005). Research Paradigms and Meaning Making : A Primer. *The Qualitative Report*, *10*(4), 758–770. https://doi.org/10.1176/appi.ajp.162.10.1985

Kristian, W., Alfajri, M., Oktavia, B., Nofitriandi, A., & Teguh, W. (2022). Risk Invalidation of Data in Banking Information System in Indonesia. *2022 International Conference on Information Management and Technology (ICIMTech)*, (August), 333–338. https://doi.org/10.1109/ICIMTech55957.2022.9915040

Kusumah, T., & Suhardi. (2014). Designing information governance in statistical organization. *2014 International Conference on Information Technology Systems and Innovation*, *9*(November), 201–205. https://doi.org/10.1109/ICITSI.2014.7048264

Kvale, S. (2011a). Conducting an interview. In *Doing Interviews* (pp. 52–66). https://doi.org/10.7748/nr2000.07.7.4.75.c6132

Kvale, S. (2011b). Introduction to Interview Research. In *Doing Interviews* (pp. 2–10). https://doi.org/10.4135/9781849208963.n1

Kvale, S. (2011c). Transcribing Interviews. In *Doing Interviews* (pp. 93–100). https://doi.org/10.4135/9781849208963.n8

Kwan, H., Riley, M., Prasad, N., & Robinson, K. (2022). An investigation of the status and maturity of hospitals' health information governance in Victoria, Australia. *Health*

Information Management Journal, *51*(2), 89–97. https://doi.org/10.1177/1833358320938309

Lajara, T., & Maçada, A. (2013). Information governance framework: The defense manufacturing case study. *Proceedings of the Nineteenth Americas Conference on Information Systems*, *3*, 1984–1993.

Lauckner, H., Paterson, M., & Krupa, T. (2012). Using constructivist case study methodology to understand community development processes: Proposed methodological questions to guide the research process. *Qualitative Report*, *17*(13), 1–22.

Lauri, L., Virkus, S., & Heidmets, M. (2021). Information cultures and strategies for coping with information overload: case of Estonian higher education institutions. *Journal of Documentation*, *77*(2), 518–541. https://doi.org/10.1108/JD-08-2020-0143

Le Khac, N., & Kechadi, T. (2010). Application of data mining for anti-money laundering detection: A case study. *IEEE International Conference on Data Mining Workshops*, 577–584. https://doi.org/10.1109/ICDMW.2010.66

Levi, Michael and Reuter, P. (2006). Money laundering. *Crime and Justice*, *34*, 289--375.

Levi, M. (2015). Money for Crime and Money from Crime: Financing Crime and Laundering Crime Proceeds. *European Journal on Criminal Policy and Research*, *21*(2), 275–297. https://doi.org/10.1007/s10610-015-9269-7

Lian, Z., Wang, N., & Oliver, G. (2022). Information culture and recordkeeping: a case of Chinese enterprises. *Journal of Documentation*, *78*(5), 973–995. https://doi.org/10.1108/JD-09-2021-0189

Lis, D., Arbter, M., Spindler, M., & Otto, B. (2022). An Investigation of Antecedents for Data

Governance Adoption in the Rail Industry: Findings From a Case Study at Thales. *IEEE Transactions on Engineering Management*, *70*(7), 2528–2545. https://doi.org/10.1109/TEM.2022.3166109

Liu, X. (2013). Full-Text Citation Analysis : A New Method to Enhance. *Journal of the American Society for Information Science and Technology*, *64*(July), 1852–1863. https://doi.org/10.1002/asi

Lokanan, M. (2022). Predicting Money Laundering Using Machine Learning and Artificial Neural Networks Algorithms in Banks. *Journal of Applied Security Research*, *0*(0), 1–25. https://doi.org/10.1080/19361610.2022.2114744

Lokanan, M., & Nasimi, N. (2020). The effectiveness of Anti-Money Laundering policies and procedures within the Banking Sector in Bahrain. *Journal of Money Laundering Control*, *23*(4), 769–781. https://doi.org/10.1108/JMLC-10-2019-0080

Lomas, E. (2020). Information Governance and Cybersecurity: Framework for Securing and Managing Information Effectively and Ethically. In Cybersecurity for Information Professionals. https://doi.org/10.1201/9781003042235-6

Malik, P. (2013). Governing Big Data: Principles and practices. *IBM Journal of Research and Development*, *57*(3/4), 1:1-1:13. https://doi.org/10.1147/jrd.2013.2241359

Masciandaro, D. (2017). *Global financial crime: terrorism, money laundering and offshore centres*. Taylor & Francis.

Mason, J. (2002). *Qualitative researching* (2nd ed). London: Thousand Oaks, Calif.: Sage Publications.

Mathes, C. (2016). Big data has unique needs for information governance and data quality.

Journal of Management Science and Business Intelligence, *1*(1), 12–20. Retrieved from https://doi.org/10.5281/zenodo.376756

Matthews, B. (2010). *Research methods: a practical guide for the social sciences*. Harlow, England: Longman.

Mclaughlin, J., & Pavelka, D. (2013). The Use of Customer Due Diligence to Combat Money Laundering. *Accountancy Business and Public Interest*, 57–84.

MENA FATF. (2013). *Money Laundering and Terrorist Financing Trends and Indicators in the Middle East and North Africa Region*. Retrieved from http://www.menafatf.org/sites/default/files/ML-TF_Trends_and_Indicators_in_the_MENA_Region_English2.pdf

Merriam, S. B. (1998). *Qualitative research and case study applications in education*. ERIC.

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation* (Rev. ed.). San Francisco: Jossey-Bass.

Michener, W. K. (2015). Ten Simple Rules for Creating a Good Data Management Plan. *PLoS Computational Biology*, *11*(10), 1–9. https://doi.org/10.1371/journal.pcbi.1004525

Mikalef, P., Krogstie, J., van de Wetering, R., Pappas, I., & Giannakos, M. (2018). Information Governance in the Big Data Era: Aligning Organizational Capabilities. *Proceedings of the 51st Hawaii International Conference on System Sciences*, *9*, 4911–4920. https://doi.org/10.24251/hicss.2018.615

Miles, M., & Huberman, M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Mills, A., Durepos, G., & Wiebe, E. (2010). Encyclopedia of Case Study Research. In *Encyclopedia of Case Study Research*. https://doi.org/10.4135/9781412957397.n26

Muhammad, J., Isa, A., Samsudin, A., & Miah, S. (2020). Critical factors for implementing effective information governance in Nigerian universities: A case study investigation. *Education and Information Technologies*. https://doi.org/10.1007/s10639-020-10206-3

Muhammad, J. S., Isa, A. M., Samsudin, A. Z. H., & Miah, S. J. (2020). Critical factors for implementing effective information governance in Nigerian universities: A case study investigation. *Education and Information Technologies*, *25*(6), 5565–5580. https://doi.org/10.1007/s10639-020-10206-3

Muhammad, J. S., Miah, S. J., Isa, A. M., & Samsudin, A. Z. H. (2022). Investigating importance and key factors for information governance implementation in Nigerian Universities. *Education and Information Technologies*, (0123456789). https://doi.org/10.1007/s10639-021-10817-4

Mullon, P. A., & Ngoepe, M. (2019). An integrated framework to elevate information governance to a national level in South Africa. *Records Management Journal*, *29*(1–2), 103–116. https://doi.org/10.1108/RMJ-09-2018-0030

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Naheem, M. A. (2016a). Money laundering: A primer for banking staff. *International Journal of Disclosure and Governance*, *13*(2), 135–156. https://doi.org/10.1057/jdg.2015.10

Naheem, M. A. (2016b). Risk of money laundering in the US: HSBC case study. *Journal of Money Laundering Control*, *19*(3), 225–237. https://doi.org/10.1108/JMLC-01-2015-0003

Naheem, M. A. (2016c). Risk of money laundering in the US: HSBC case study. *Journal of Money*

Laundering Control, *19*(3), 225–237. https://doi.org/10.1108/JMLC-01-2015-0003

Naheem, M. A. (2018). Illicit financial flows: HSBC case study. *Journal of Money Laundering Control*, *21*(2), 231–246. https://doi.org/10.1108/JMLC-08-2015-0036

Najdanović, Z., & Tutek, N. (2021). The Impact of Information Management in developing New Products in Bank – AN Empirical Analysis. *Informatologia*, *54*, 3–4.

National Archives of Australia. (2013). Information governance. Retrieved January 31, 2020, from https://www.naa.gov.au/information-management/information-governance

NCFI. (2019). *Annual report of the National Centre for Financial Information 2019*. Retrieved from https://fiu.gov.om/files/English/English2018.pdf%0D

NCFI. (2021). *NCFI ANUUAL REPORT 2021*. Retrieved from https://www.fiu.gov.om/files/AnnualReaport2021.pdf

Neuman, W. L. (William L. (2014). *Social research methods: qualitative and quantitative approaches* (Seventh ed). Harlow, Essex: Pearson.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847

O’Gorman, K., & MacIntosh, R. (2016). *Research methods for business & management : A guide to writing your dissertation* (2nd ed). https://doi.org/10.13140/RG.2.1.1419.3126

O’Reilly, K. (2012). Inductive and Deductive. In *Key Concepts in Ethnography* (pp. 104–109). Sage.

Ofoeda, I., Agbloyor, E., Abor, J., & Osei, K. (2022). Anti-money laundering regulations and financial sector development. *International Journal of Finance and Economics*, *27*(4), 4085–4104. https://doi.org/10.1002/ijfe.2360

Okunleye, O. J. (2023). *Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector*. *23*(18), 22–35. https://doi.org/10.9734/AJEBA/2023/v23i181055

Olaitan, O., Herselman, M., & Wayi, N. (2016). *Taxonomy of literature to justify data governance as a pre-requisite for information governance*. 586–605.

Oliver, G. (2008). Information culture: Exploration of differing values and attitudes to information in organisations. *Journal of Documentation*, *64*(3), 363–385. https://doi.org/10.1108/00220410810867588

Oman Observer. (2023, June 21). *CBO issues guidlines for digital onboarding and e-KYC*. Retrieved from https://www.omanobserver.om/article/1139077/business/banking/cbo-issues-guidelines-for-digital-onboarding-and-e-kyc

Onwuegbuzie, A. J., & Leech, N. L. (2005). Taking the “q” out of research: Teaching research methodology courses without the divide between quantitative and qualitative paradigms. *Quality and Quantity*, *39*(3), 267–295. https://doi.org/10.1007/s11135-004-1670-0

Otto, B. (2011). *Organizing Data Governance : Findings from the Telecommunications Industry and Consequences for Large Service Providers Organizing Data Governance : Findings from the Telecommunications Industry and Consequences for Large Service Providers Motivation Orga*. *29*(August), 45–66.

Oxford English Dictionary. (2023). Oxford University Press. Retrieved August 7, 2023, from https://www.oxfordlearnersdictionaries.com/

Parameswarappa, P. (2022). Importance of Information Governance &amp; Implementation in

Banking Industry. *SSRN Electronic Journal*, 1–27. https://doi.org/10.2139/ssrn.4190576

Patton, M. (2002). *Qualitative evaluation and research methods* (3rd editio). Newbury Park, Calif: Sage.

Pechlaner, H., Ruhanen, L., Scott, N., Ritchie, B., & Tkaczynski, A. (2010). Governance: a review and synthesis of the literature. *Tourism Review*, *65*(4), 4–16. https://doi.org/10.1108/16605371011093836

Peppard, J. (1999). A governance framework for information management in the global enterprise. *Euro*, 77–94. Retrieved from http://hdl.handle.net/1826/459

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, *21*(4), 7–22. https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2

Pettigrew, A. M. (1988). Longitudinal field research on change: Theory and practic. *Organization Science*, *1*(3), 267–292.

Pomeranz, E., & Stedman, R. (2020). Measuring good governance: piloting an instrument for evaluating good governance principles. *Journal of Environmental Policy and Planning*, *22*(3), 428–440. https://doi.org/10.1080/1523908X.2020.1753181

Pramod, V., Li, J., & Gao, P. (2012). A framework for preventing money laundering in banks. *Information Management and Computer Security*, *20*(3), 170–183. https://doi.org/10.1108/09685221211247280

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Randhawa, T. S. (2019). *Incorporating Data Governance Frameworks in the Financial Industry*. 2–193. Retrieved from https://scholarworks.waldenu.edu/dissertations

Rehman, A. A., & Alharthi, K. (2016). An introduction to research paradigms. *International Journal of Educational Investigations*, *3*(October), 51–59.

Renny, B., & Miru, A. (2019). Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes. *Journal of Law, Policy and Globalization*, *81*(2), 23–27. https://doi.org/10.7176/JLPG

Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, 652–667.

Rhodes, R. A. W. (2007). Understanding governance: Ten years on. *Organization Studies*, *28*(8), 1243–1264. https://doi.org/10.1177/0170840607076586

Riccardi, M., & Levi, M. (2018). Cash, Crime and Anti-Money Laundering. In *The Palgrave handbook of criminal and terrorism financing law*.

Richards, K. (2003). *Qualitative inquiry in TESOL*. Springer.

Ritchie, Jane and Lewis, Jane and Elam, G. (2003). *Designing and selecting samples*. London: Sage.

Rose-Ackerman, S. (2017). What Does “Governance” Mean? *Governance*, *30*(1), 23–27. https://doi.org/10.1111/gove.12212

Roulston, K. (2014). Doing Interview Research. *Reflective Interviewing: A Guide to Theory and Practice*, 96–114. https://doi.org/10.4135/9781446288009.n6

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, *35*(3–4), 260–271. https://doi.org/10.1108/01409171211210154

Rubin, H., & Rubin, I. (2012). *Qualitative Interviewing: The Art of Hearing Data*. https://doi.org/10.4135/9781452226651.n2

Safar, M., & Al-Najjar, A. (2006). Data growth in banking sector. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 667–674. https://doi.org/10.1109/dexa.2006.46

Saldana, J. (2011). *Fundementals of Qulaitative Research*. Oxford University Press.

Saldaña, J. (2013). The coding manual for qualitative researchers. In *International Journal* (2nd editio). https://doi.org/10.1017/CBO9781107415324.004

Sarigul, H. (2013). Money laundering and abuse of the financial system. *International Journal of Business and Management Studies*, *2*(1), 287–301.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (Seventh ed). Pearson.

Schoch, T. (2016). EU privacy regulations' impact on information governance. *Information Management*. https://doi.org/10.1201/9781315385488-20

Seawnght, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly*, *61*(2), 294–308. https://doi.org/10.1177/1065912907313077

Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, *22*(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

ARMA International. (2019). ARMA International Information Governance Implementation Model [IGIM]. Retrieved July 24, 2020, from https://www.arma.org/page/igim?&hhsearchterms=%22information+and+governance%22

Bennett, S. (2017). What is information governance and how does it differ from data governance? *Governance in Practice*, (September), 462–467. Retrieved from https://www.sibenco.com/information-governance-and-data-governance/

Berger, P., & Luckmann, T. (1968). *The social construction of reality: A Treatise in the Sociology of Knowledge*. Anchor Books.

Berger, R. (2015). Now I see it, now I don’t: researcher’s position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219–234. https://doi.org/10.1177/1468794112468475

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2013). *Successful qualitative research: a practical guide for beginners*. London: Sage.

Braun, V., & Clarke, V. (2021). To saturate or not to saturate ? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201–216. https://doi.org/10.1080/2159676X.2019.1704846

Bryman, A. (2004). *Social Research Methods* (2nd ed.). Oxford: Oxford University Press.

Creswell, J. W., & Poth, C. (2017). *Qualitative inquiry and research design: choosing among five approaches* (4th edn). Los Angeles: SAGE Publications, Inc.

De Abreu Faria, F., Gastaud Maçada, A. C., & Kumar, K. (2013). Information governance in the banking industry. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4436–4445. https://doi.org/10.1109/HICSS.2013.270

Devers, K. J., & Frankel, R. M. (2000). Study design in qualitative research--2: Sampling and data collection strategies. *Education for Health*, *13*(2), 263.

Donaldson, A., & Walker, P. (2004). Information governance - A view from the NHS. *International Journal of Medical Informatics*, *73*(3), 281–284. https://doi.org/10.1016/j.ijmedinf.2003.11.009

EDRM.net. (2012). Information Governance Reference Model (IGRM). Retrieved May 29, 2016, from https://www.edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

Faria, F., Maçada, A., Kumar, K., De Abreu Faria, F., Gastaud Maçada, A. C., Kumar, K., … Kumar, K. (2013). Information governance in the banking industry. *Proceedings of the Annual Hawaii International Conference on System Sciences*, (Ketchum), 4436–4445. https://doi.org/10.1109/HICSS.2013.270

Healy, M., & Perry, C. (2009). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *An International Journal Iss Qualitative Research Journal European Journal of Marketing Qualitative Market Research An International Journal*, *310*(2), 118–126. Retrieved from http://dx.doi.org/10.1108/13522750010333861%5Cnhttp://%5Cnhttp://dx.doi.org/10.1108/03090569810232237%5Cnhttp://dx.doi.org/10.1108/13522750010322089

Hulme, T. (2012). Information governance: Sharing the IBM approach. *Business Information Review*, *29*(2), 99–104. https://doi.org/10.1177/0266382112449221

IBM. (2014). *IBM Information Governance Solutions*.

Israel, M., & Hay, I. (2006). Research Ethics for Social Scientists. In *Research Ethics for Social Scientists*. https://doi.org/10.4135/9781849209779

Joppe. (2000). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, 30–37.

Jullum, M., Løland, A., & Huseby, R. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173–186. https://doi.org/10.1108/JMLC-07-2019-0055

Kolb, D. (2014). *Experiential Learning: Experience as the Source of Learning and Development*. FT press.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Lajara, T., & Maçada, A. (2013). Information governance framework: The defense manufacturing case study. *Proceedings of the Nineteenth Americas Conference on Information Systems*, *3*, 1984–1993.

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. Beverly Hills, Calif.: Beverly Hills, Calif.

Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*, *20*(2), 182–198. https://doi.org/10.1108/09565691011064322

Lomas, E., Shabou, B., & Grazhenskaya, A. (2019). Information governance and ethics - information opportunities and challenges in a shifting world: setting the scene. *Records*

Management Journal, 2–4.

Merriam, S. B. (1998). *Qualitative research and case study applications in education*. ERIC.

Merriam, S. B. (2015). Qualitative research: A guide to design and implementation. In *Progress in Electromagnetics Research Symposium* (Rev. ed.). San Francisco: John Wiley \& Sons.

Miles, M., & Huberman, M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Mullon, P. A., & Ngoepe, M. (2019). An integrated framework to elevate information governance to a national level in South Africa. *Records Management Journal*, *29*(1–2), 103–116. https://doi.org/10.1108/RMJ-09-2018-0030

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35. https://doi.org/10.1136/eb-2015-102054

Patton, M. (2014). *Qualitative Research and Evaluation Methods* (4th editio). Sage publications.

Rolfe, G. (2006). Validity, trustworthiness and rigour: Quality and the idea of qualitative research. *Journal of Advanced Nursing*, *53*(3), 304–310. https://doi.org/10.1111/j.1365-2648.2006.03727.x

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (Seventh ed). Pearson.

Scott, J. (2014). *A matter of record: Documentary sources in social research*. John Wiley & Sons.

Shleifer, A., & Vishny, R. (2007). A survey of corporate governance. *Corporate Governance and Corporate Finance: A European Perspective*, *LII*(2), 52–90. https://doi.org/10.4324/9780203940136

Singh, K., & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*, 100418.

https://doi.org/10.1016/j.accinf.2019.06.001

Stake, R. (1995). *The art of case study research*. London: Sage publications.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Sage publications.

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, *30*(3), 141–177. https://doi.org/10.2753/MIS0742-1222300306

Tracy, S. (2010). Qualitative quality: Eight a"big-tent" criteria for excellent qualitative research. *Qualitative Inquiry*, *16*(10), 837–851. https://doi.org/10.1177/1077800410383121

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

Young, R., & Collin, A. (2004). Introduction: Constructivism and social constructionism in the career field. *Journal of Vocational Behavior*, *64*(3), 373–388. https://doi.org/10.1016/j.jvb.2003.12.005

Shahin, W. (2013). Compliance with international regulation on AML/CFT: the case of banks in Lebanon. *Journal of Money Laundering Control*, *16*(2), 109–118. https://doi.org/10.1108/13685201311318467

Shepherd, E., Stevenson, A., & Flinn, A. (2010). Information governance, records management, and freedom of information: A study of local government authorities in England. *Government Information Quarterly*, *27*(4), 337–345.

https://doi.org/10.1016/j.giq.2010.02.008

Shleifer, A., & Vishny, R. (2007). A survey of corporate governance. *Corporate Governance and Corporate Finance: A European Perspective*, *LII*(2), 52–90. https://doi.org/10.4324/9780203940136

Shu, I., & Jahankhani, H. (2017). The Impact of the new European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England. *2017 Cybersecurity and Cyberforensics Conference*, 31–37. https://doi.org/10.1109/CCC.2017.16

Silic, M., & Back, A. (2013). Factors impacting information governance in the mobile device dual-use context. *Records Management Journal*, *23*(2), 73–89. https://doi.org/10.1108/RMJ-11-2012-0033

Silverman, D. (2013). *Doing qualitative research: A practical handbook* (3rd ed). London: Sage publications.

Simonova, A. (2011). The risk-based approach to anti-money laundering: problems and solutions. *Journal of Money Laundering Control*, *14*(4), 346–358. https://doi.org/10.1108/13685201111173820

Simwayi, M., & Guohua, W. (2011). The role of commercial banks in combating money laundering. *Journal of Money Laundering Control*, *14*(4), 324–333. https://doi.org/10.1108/13685201111173802

Singh, K., & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*, 100418. https://doi.org/10.1016/j.accinf.2019.06.001

Slevitch, L. (2011). Qualitative and quantitative methodologies compared: Ontological and epistemological perspectives. *Journal of Quality Assurance in Hospitality and Tourism*, *12*(1), 73–81. https://doi.org/10.1080/1528008X.2011.541810

Sloan, P. (2014). The Compliance Case for Information Governance. *Richmond Journal of Law and Technology*, *20*(2), 4.

Smallwood, R. (2014). *Information governance: concepts, strategies, and best practices*.

Smallwood, R. (2019). *Information governance: concepts, strategies and best practices*. Retrieved from http://repositorio.unan.edu.ni/2986/1/5624.pdf

Soares, S. (2011). Selling Information Governance to the Business: Best Practices by Industry and Job Function. *MC Press*.

Soares, Sunil. (2011). Banking and Financial Markets. In *Selling Information Governance to the Business: Best Practices by Industry and Job Function*. MC Press.

Social Research Association. (2003). Ethical guidelines. https://doi.org/10.1080/00031305.1984.10483191

Stake, R. (1995). *The art of case study research*. London: Sage publications.

Stoker, G. (1998). Governance as theory: five propositions. *International Social Science Journal*, 17–28. https://doi.org/10.1111/issj.12189

Strauss, A., & Corbin, J. (2007). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (3d ed). Sage publications.

Subbotina, N. (2009). Challenges that Russian banks face implementing the AML regulations. *Journal of Money Laundering Control*, *12*(1), 19–32. https://doi.org/10.1108/13685200910922624

Sudra, R. (2020). Legal Certainty Regarding Electronic Medical Record Retention Period. *International Proceedings the 2nd International Scientific Meeting on Health Information Management (ISMoHIM)*, *5*, 48–54.

Sultan, N., & Mohamed, N. (2022a). The money laundering typologies and the applicability of placement-layering-integration model in undocumented South Asian economies: a case of Pakistan. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-08-2022-0116

Sultan, N., & Mohamed, N. (2022b). The role of information sharing in combating money laundering: the importance and challenges of mutual legal assistance for developing jurisdictions like Pakistan. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2022-0128

Svärd, P. (2014). The impact of information culture on information/records management: A case study of a municipality in Belgium. *Records Management Journal*, *24*(1), 5–21. https://doi.org/10.1108/RMJ-04-2013-0007

Tallon, P., Ramirez, R., & Short, J. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, *30*(3), 141–177. https://doi.org/10.2753/MIS0742-1222300306

Tallon, P., Short, J., & Harkins, M. (2013). The evolution of information governance at intel. *MIS Quarterly Executive*, *12*(4), 189–198.

Tavakoli, N., & Jahanbakhsh, M. (2013). Investigation of retention and destruction process of medical records in the hospitals and codifying appropriate guidelines. *Journal of Education and Health Promotion*, *2*(1), 17. https://doi.org/10.4103/2277-9531.112687

The University of Sheffield. (n.d.-a). IT Services - The University of Sheffield. Retrieved May 31, 2020, from https://www.sheffield.ac.uk/it-services

The University of Sheffield. (n.d.-b). POLICY ON GOOD RESEARCH AND INNOVATION PRACTICES. Retrieved July 13, 2020, from https://www.sheffield.ac.uk/polopoly_fs/1.671066!/file/GRIPPolicy.pdf

The University of Sheffield. (2020). Ethics Policy Governing Research Involving Human Participants Personal Data and Human Tissue: General Principles and Statements. Retrieved June 12, 2020, from https://www.sheffield.ac.uk/polopoly_fs/1.755691!/file/Ethics_Policy_Senate_Approved.pdf

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, *5*, 147–158.

Traulsen, S., & Tröbs, M. (2011). Implementing Data Governance within a Financial Institution. *NFORMATIK 2011*, 195–210. Retrieved from http://informatik2011.de/519.html

Trochim, W. (2006). *Research methods knowledge base*.

Tyagi, A. (2021). Information Governance Program: Implementation and Strategies in Banking Sector. *SSRN Electronic Journal*, 1–31.

Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity*, *2011*, 1–12. https://doi.org/10.5171/2011.726196

Unger, B., & Busuioc, M. (2007). *The scale and impacts of money laundering*. Edward Elgar Publishing.

UNODC. (n.d.). Money-Laundering and Globalization. Retrieved June 24, 2020, from https://www.unodc.org/unodc/en/money-laundering/globalization.html

UNODC. (1988). *United Nations Convention against illicit drugs and psychotropic substances*. https://doi.org/10.1080/07488008908408885

UNODC. (2009). *Model Provisions on Money Laundering , Terrorist Financing , Preventive Measures and Proceeds of Crime*. Retrieved from https://www.unodc.org/documents/money-laundering/Model_Provisions_Final.pdf

UNODC. (2023). Money Laundering. Retrieved August 27, 2023, from https://www.unodc.org/unodc/en/money-laundering/overview.html

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*. https://doi.org/10.1109/HICSS.2006.322

Viritha, B., Mariappan, V., & Venkatachalapathy, V. (2015). Combating money laundering by the banks in India: compliance and challenges. *Journal of Investment Compliance*, *16*(4), 78–95. https://doi.org/10.1108/joic-07-2015-0044

Vugec, D., Spremić, M., & Bach, M. (2017). IT governance adoption in banking and insurance sector: Longitudinal case study of cobit use. *International Journal for Quality Research*, *11*(3), 691–716. https://doi.org/10.18421/IJQR11.03-13

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Weber, K., Otto, B., & Osterle, H. (2009). One Size Does Not Fit All—A Contingency Approach to Data Governance. *ACM Journal of Data and Information Quality*, *1*, 1–27. https://doi.org/10.1080/17415349.2006.11013494

Wegberg, R., Oerlemans, J.-J., & Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067

Weill, P., & Ross, J. (2004a). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Weill, P., & Ross, J. (2004b). IT Governance on One Page. *MIT Sloan Management Review*, 18. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=664612

Weiss, T. (2012). Governance, Good Governance, and Global Governance: Conceptual and actual challenges. *Thinking about Global Governance: Why People and Ideas Matter*, *21*(5), 168–189. https://doi.org/10.4324/9780203807057-19

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *Information Society*, *35*(1), 36–51. https://doi.org/10.1080/01972243.2018.1542648

World Bank. (1997). *World development report 1997: The state in a changing world*.

Wright, T. (2013). Information culture in a government organization: Examining records management training and self-perceived competencies in compliance with a records management program. *Records Management Journal*, *23*(1), 14–36. https://doi.org/10.1108/09565691311325004

Wronka, C. (2022). “Cyber-laundering”: the change of money laundering in the digital age.

Journal of Money Laundering Control, *25*(2), 330–344. https://doi.org/10.1108/JMLC-04-2021-0035

Wynn, D., & Williams, C. K. (2012). Principles for Conducting Critical Realist Case Study Research in Information Systems. In *Source: MIS Quarterly* (Vol. 36).

Yasaka, N. (2017). Data mining in anti-money laundering field. *Journal of Money Laundering Control*, *20*(3), 301–310. https://doi.org/10.1108/JMLC-09-2015-0041

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*. https://doi.org/10.22347/2175-2753v8i22.1038

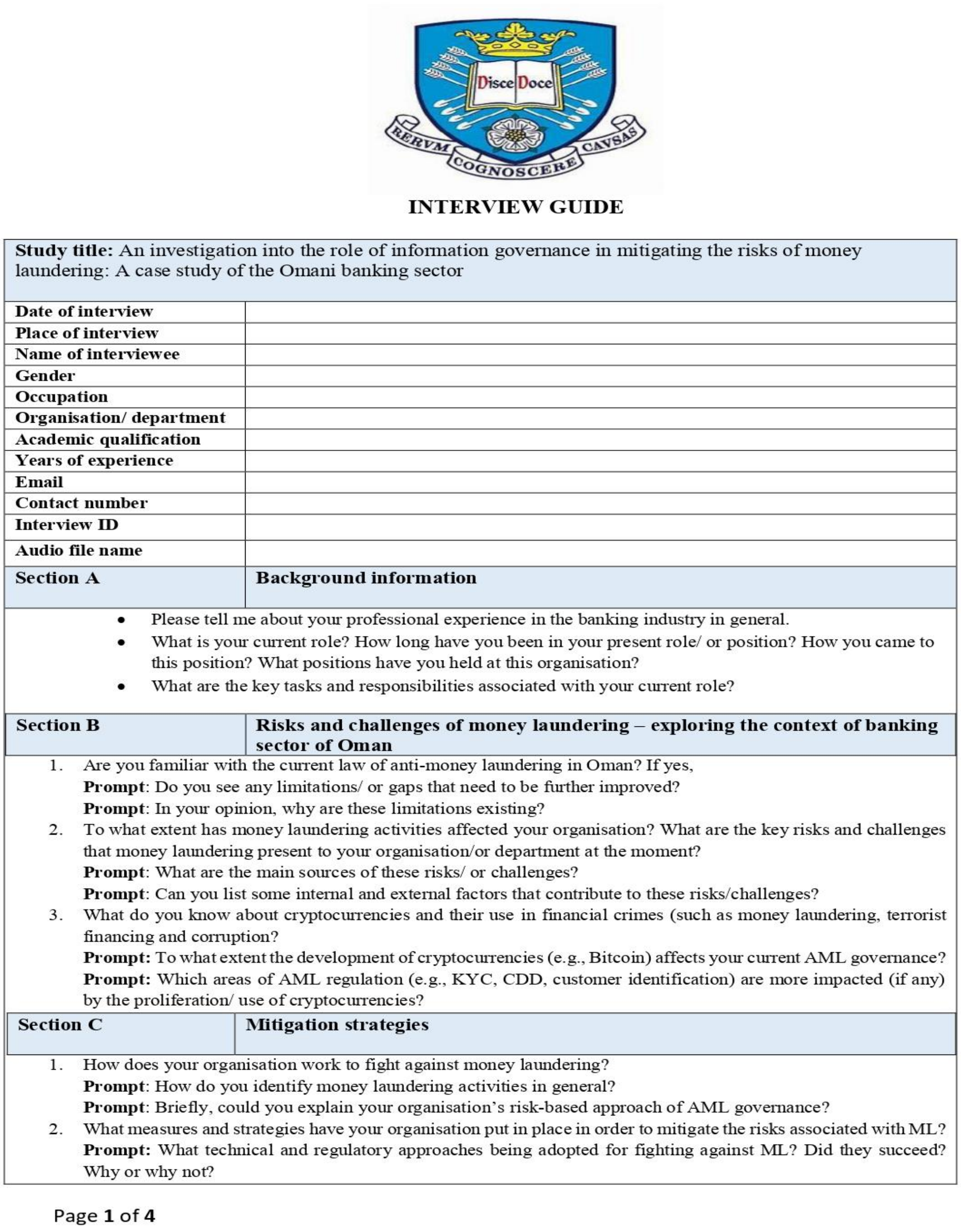
Yeoh, P. (2019). Banks' vulnerabilities to money laundering activities. *Journal of Money Laundering Control*, *23*(1), 122–135. https://doi.org/10.1108/JMLC-05-2019-0040

Yin, R. (2014). *Case study research: Design and methods* (Fifth edit). Los Angeles: Sage.

Zaman, Q., Aish, K., Akhter, W., & Zaidi, S. (2020). Exploring the role of corruption and money laundering (ML) on banking profitability and stability: a study of Pakistan and Malaysia. *Journal of Money Laundering Control*, *24*(3), 525–543. https://doi.org/10.1108/JMLC-07-2020-0082

Appendices

Appendix 1: Interviews Guide



INTERVIEW GUIDE

Study title: An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

Date of interview	
Place of interview	
Name of interviewee	
Gender	
Occupation	
Organisation/ department	
Academic qualification	
Years of experience	
Email	
Contact number	
Interview ID	
Audio file name	

Section A **Background information**

- Please tell me about your professional experience in the banking industry in general.
- What is your current role? How long have you been in your present role/ or position? How you came to this position? What positions have you held at this organisation?
- What are the key tasks and responsibilities associated with your current role?

Section B **Risks and challenges of money laundering – exploring the context of banking sector of Oman**

1. Are you familiar with the current law of anti-money laundering in Oman? If yes,
   Prompt: Do you see any limitations/ or gaps that need to be further improved?
   Prompt: In your opinion, why are these limitations existing?
2. To what extent has money laundering activities affected your organisation? What are the key risks and challenges that money laundering present to your organisation/or department at the moment?
   Prompt: What are the main sources of these risks/ or challenges?
   Prompt: Can you list some internal and external factors that contribute to these risks/challenges?
3. What do you know about cryptocurrencies and their use in financial crimes (such as money laundering, terrorist financing and corruption?
   Prompt: To what extent the development of cryptocurrencies (e.g., Bitcoin) affects your current AML governance?
   Prompt: Which areas of AML regulation (e.g., KYC, CDD, customer identification) are more impacted (if any) by the proliferation/ use of cryptocurrencies?

Section C **Mitigation strategies**

1. How does your organisation work to fight against money laundering?
   Prompt: How do you identify money laundering activities in general?
   Prompt: Briefly, could you explain your organisation's risk-based approach of AML governance?
2. What measures and strategies have your organisation put in place in order to mitigate the risks associated with ML?
   Prompt: What technical and regulatory approaches being adopted for fighting against ML? Did they succeed? Why or why not?

Page **1** of **4**

INTERVIEW GUIDE

3. What role does modern technology (e.g., machine learning, data mining, and business intelligence) play in detecting suspicious activity or transactions related to ML?
   Prompt: What technology/or tool does your department is currently adopting for AML purpose?
   Prompt: Can you share your experience about the use of technology for fighting against ML?

Section D	**Contextualisation of information needs**

Nowadays, many organisations, including financial institutions, consider information as a strategic resource, or valuable asset for achieving their organisational objectives.

1. What are the key critical success factors for your AML department/ organisation to succeed?
2. How important is information in preventing fraudulent/or criminal activities associated with money laundering?
3. What information do you need to acquire from various stakeholders in order to make operational decisions (e.g., freezing accounts, filing suspicious transaction) related to ML?
4. What plans or strategies do you put in place in order to satisfy your information needs for AML purpose?
5. What information sources or channels (e.g., human or technological context) are available for you in order to seek or obtain the needed information? Which of these sources are the most useful source of information, and why?
   Prompt: What formal systems do AML officers/ or managers use to obtain the needed information?
   Prompt: How do you obtain information that is not available or accessible within your organisation?
   Prompt: Have you ever use other alternatives such as email, fax or phone in order to obtain information related to ML? If yes, why did you choose these methods to acquire the needed information?
6. What role does a central repository or data-warehouse (if any) have in satisfying your information needs in AML context?
7. How does your information needs for AML change over time? How are these needs affected by external factors (such as changes in AML regulations or laws)?
8. What do you see as the best strategy for improving the process of satisfying the information needs in your organisation/ department?

Section E	**Antecedent factors**

Part 1: External factors

1. Are there any legislative or regulatory requirements from the national or international level imposed on your organisation to implement effective management of ML data/ information? How have these regulatory requirements affected your strategy of handling ML data/ information in your organisation/ or department?
   Prompt: I understand from the national AML law that there is a requirement to retain all customer records, documents, information and data for at least ten years after a transaction is carried out. What practice did your organisation/ department follow in order to make this information available immediately upon request to law enforcement authorities (e.g., Central bank of Oman)?
   Prompt: Can you explain the process of how you keep customer records and retrieve them within a timeframe acceptable to law enforcement agencies?
2. In which ways does the use of advanced payment systems (e.g., peer-to-peer payments) used by money launderers influence your organisation /department to rethink its processes for managing ML information?

Part 2: Internal factors

1. What are the key challenges facing your organisation in relation to the management of ML data/ or information?
2. Is your organisation/ department experiencing growth in the volume of ML data/information? What is driving this growth?
3. Have information growth of ML and its value exploitation become an essential part of your organisation or IT

strategy and plans? How the established organisational strategy enables/ or inhibits your department to implement best practices for handling ML data/ information?

4. Does your organisation promote the protection and strategic use of information assets in general, and ML information in particular? What did your senior management offer in order to promote information use across different departments in the organisation?
5. What kind of support (e.g., financial support) did you receive from your senior management to the activities/ or initiatives associated with the management of ML data/ information?
6. Is ML information managed centrally or what other structures have you put in place?
7. To what level can the existing IT infrastructure accommodate the growth of ML data/ information? Have you ever encounter a business interruption due to insufficient storage?

Section F — Data integration, organisational scope, data scope and domain scope

1. Does your organisation/or department have information/ or data strategy in place? What strategies have your organisation followed in order to integrate ML related data residing in different sources (including both internal and external sources)?
   Prompt: Do you have in place a centralised data repository where all stakeholders, including branches, AML compliance officers and regulators, can access to relevant ML data/or information? If no, why not? What factors did inhibit your organisation from integrating ML data?
2. Do you collaborate with internal or external partners (e.g., industry peers, vendors, or public-sector organisations) in order to integrate all relevant data/information about ML?
   Prompt: In the case of inter-collaboration (or inter-organisational scope), where the shared data repository is hosted, and how the access to relevant ML data is granted/ or assigned?
3. Does your organisation's policy allow you to share ML data/ information with other financial institutions in the industry? If no, why not?
   Prompt: Is there any legal or regulatory restrictions which impede the sharing of ML data with external entities in the banking industry?
   Prompt: What do you see as the key issues and benefits associated with sharing ML data/ information with other financial institutions?
   Prompt: In your opinion, what mechanisms and safeguards need to be implemented to avoid potential issues associated with sharing ML data/ information with other financial institutions?
4. Which types of data (e.g., transaction data, machine-generated data) do you collect and analyse in order to make sense of ML cases?
   Prompt: Can you describe your ML data in terms of its volume, variety (e.g., structured, semi-structured, or unstructured), and speed?
5. Which data domains (e.g., data quality, data security, data lifecycle) are more critical for your organisation/ department to develop effective AML governance, and why?

Section G — Governance practices

1. Who is responsible for ensuring that the AML regulations and procedures are followed?
   Prompt: Who is responsible for managing ML data/information and its related activities in your organisation (e.g., IT department or business users)?
   Prompt: Who is ultimately responsible for ensuring the quality of ML data/information?

Prompt: Does your organisation's top management involve in the locus of decision rights or responsibility? If yes, could you please explain how the decision rights are assigned?

2. What policies have you enacted to manage ML data/ information?

   Prompt: Who sets and monitor these policies?

   Prompt: Do you have specific data retention and backup policies?

   Prompt: Do you have any policies or procedures in place for sharing ML information internally (i.e., within your bank) or externally across different financial institutions in Oman? Do you have data sharing agreements or service level agreements in place?

   Prompt: Do you have any policies to measure and monitor the quality of ML data?

   Prompt: How do you classify ML data over its useful economic life?

3. Is ML information managed centrally or what other structures have you put in place? How are these structures changing over time?

4. Are there any processes for interaction and collaboration between the key stakeholders within or outside your organisation boundary?

   Prompt: How the relevant ML information is currently communicated to the stakeholders? Is there any communication plan in place?

   Prompt: In your opinion, what could enable the collaboration and create forms of supportive environment between different business departments within your institution?

5. How important is user education/ or training in implementing effective AML governance in your organisation/ department?

   Prompt: Does your organisation invest in the development of employees' skills? What practices are followed to ensure that sufficient education/ or training is provided to the concerned employees who engage directly or indirectly with AML activities?

   Prompt: Did board members or senior management participate in relevant AML training?

   Prompt: How frequency does the relevant AML training conducted every year?

   Prompt: Are there minimum requirements (e.g., educational qualifications, knowledge and experience) for the recruitment of AML staff? Can you please elaborate on these requirements (if any)?

6. Does the institution have the policy to ensure that management and staff do not have a criminal record?

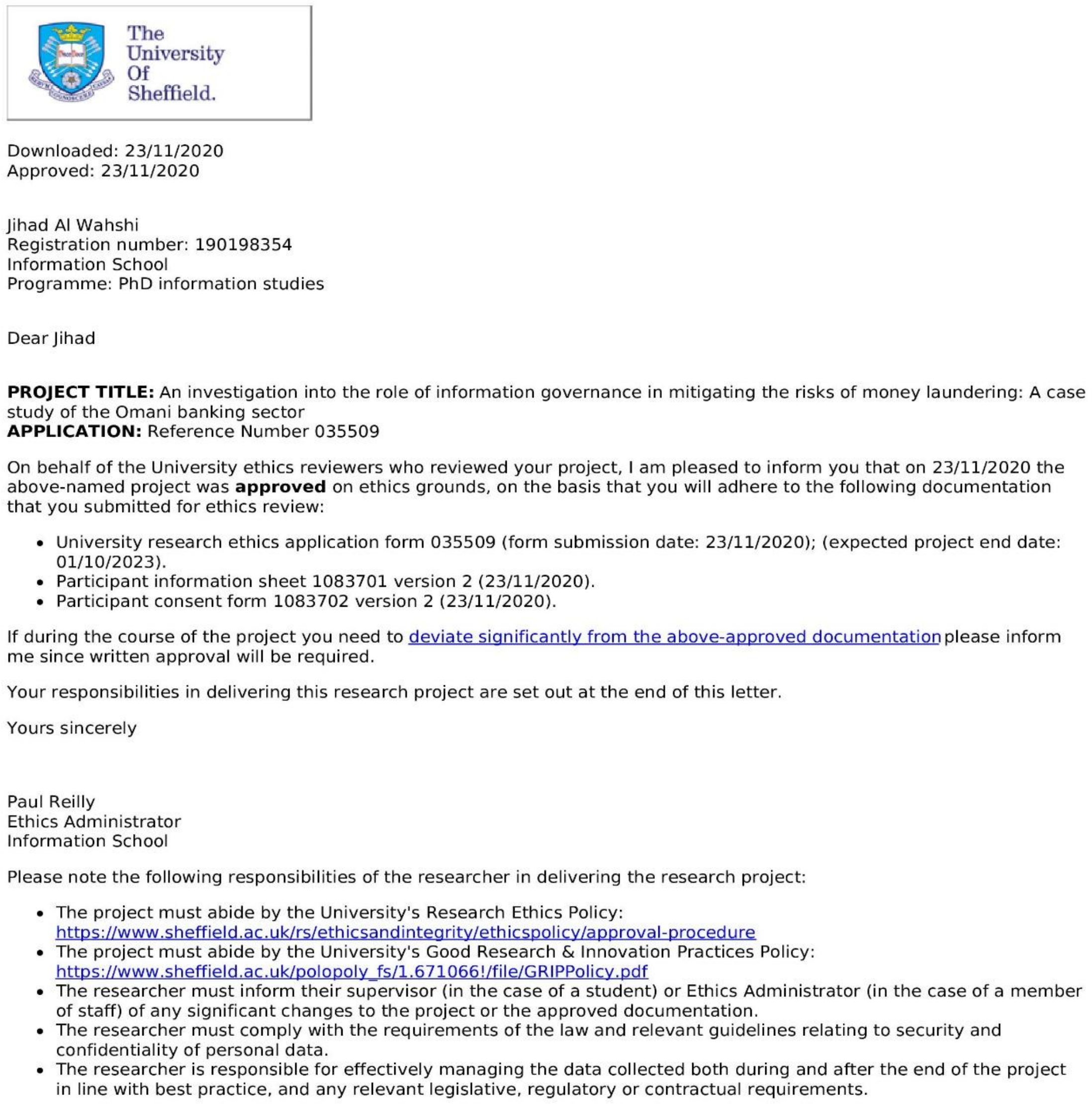
Section H	**Consequences of IG adoption in the ML context**

1. What consequences/ or impacts do you anticipate from the management of ML data/ or information? Can you list both the positive and negative impacts you anticipate?

   Prompt: What do you see as possible benefits/ outcomes emerged from the management of ML data/ information on the departmental (i.e., AML department) and organisational level?

2. In your opinion, how can the performance of the AML department impacted by the adoption of procedures and practices in managing ML data/ information?

Appendix 2: Ethical Approval



The University Of Sheffield.

Downloaded: 23/11/2020
Approved: 23/11/2020

Jihad Al Wahshi
Registration number: 190198354
Information School
Programme: PhD information studies

Dear Jihad

PROJECT TITLE: An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector
APPLICATION: Reference Number 035509

On behalf of the University ethics reviewers who reviewed your project, I am pleased to inform you that on 23/11/2020 the above-named project was **approved** on ethics grounds, on the basis that you will adhere to the following documentation that you submitted for ethics review:

- University research ethics application form 035509 (form submission date: 23/11/2020); (expected project end date: 01/10/2023).
- Participant information sheet 1083701 version 2 (23/11/2020).
- Participant consent form 1083702 version 2 (23/11/2020).

If during the course of the project you need to deviate significantly from the above-approved documentation please inform me since written approval will be required.

Your responsibilities in delivering this research project are set out at the end of this letter.

Yours sincerely

Paul Reilly
Ethics Administrator
Information School

Please note the following responsibilities of the researcher in delivering the research project:

- The project must abide by the University's Research Ethics Policy: https://www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/approval-procedure
- The project must abide by the University's Good Research & Innovation Practices Policy: https://www.sheffield.ac.uk/polopoly_fs/1.671066!/file/GRIPPolicy.pdf
- The researcher must inform their supervisor (in the case of a student) or Ethics Administrator (in the case of a member of staff) of any significant changes to the project or the approved documentation.
- The researcher must comply with the requirements of the law and relevant guidelines relating to security and confidentiality of personal data.
- The researcher is responsible for effectively managing the data collected both during and after the end of the project in line with best practice, and any relevant legislative, regulatory or contractual requirements.

Appendix 2: Information Sheet

Participant Information Sheet

Research Project Title: An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

About the research team

The principal researcher of this study is Jihad Al Wahshi, who is a second year PhD student in the information school, Information Knowledge and Innovation Management (IKIM) research group at the University of Sheffield. The study is supervised by Dr Jonathan Foster and Dr Pamela Abbott who are lecturers in the information school, University of Sheffield. The researcher has completed his master degree in Data Science in 2016 from the University of Sheffield. He has been a senior specialist of business analysis at the Central Bank of Oman with a total experience of 10 years in the banking industry. His interest lies in the areas of information/ data governance, data science, business intelligence, analytics, project management, and big data.

Further information about the research team can be found at:

Jihad Al Wahshi: https://www.sheffield.ac.uk/is/people/phd-researchers/jihad-al-wahshi

Dr Jonathan Foster: https://www.sheffield.ac.uk/is/people/academic/jonathan-foster

Dr Pamela Abbott: https://www.sheffield.ac.uk/is/people/academic/pamela-abbott

1. An invitation to participate

You are being invited to take part in this PhD research study. Before you decide whether or not to participate, it is important for you to understand why the research is being done and what it will involve. Please take some time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you wish to take part. Thank you for reading this information.

2. The purpose of the study

The aim of this study is to investigate the role of information governance (IG) programme in mitigating the risks of money laundering by integrating relevant ML data obtained from various banking institutions in Oman into a central data gathering centre (or data warehouse). More specifically, this study seeks to gain a better understanding of how to integrate and then share information about money-laundering activities within the Omani banking sector, and ii) how an information governance programme can aid banks in increasing their capacity for governing this information, so as to be able to mitigate the risks of money-laundering.

3. Why have I been chosen?

You have been chosen to take part in this study because you match the established inclusion criteria (given below) which used for identifying and recruiting potential participants. Given your professional experience in information governance or money laundering, your views, opinions and perceptions are

Participant Information Sheet

invaluable as part of this research. In particular, we are inviting banking professionals who have the following characteristics to participate in this study:

- Participants must be Omani nationality.
- Participants should work as a full-time employee.
- Participants must hold bachelor's degree from an accredited university or college OR equivalent work experience with a minimum 5 years of practical experience in the banking industry, preferably in the domains of AML, compliance or information/computer science.
- Participants should have one of the following job titles, including Chief information officer, head of compliance/ AML, Anti-money laundering officer, transaction monitoring manager, head of financial crimes, information governance manager, risk manager, or quality/data analysts.

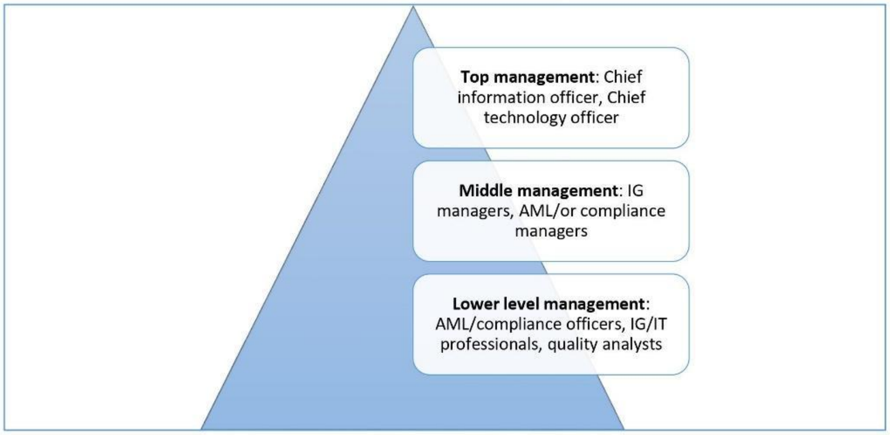
However, individual may not be able to take part in this study if any of the following exclusion criteria are present:

- The participant does not hold Omani nationality.
- The participant works as a part-time contract.
- The participant has a job title which is different than the ones mentioned in the inclusion criteria.
- The participant has an academic qualification which is below or not equivalent to the bachelor degree.
- The participant lacks of a practical experience in AML related activities such as monitoring and reporting suspicious transactions, management and analysis of ML related data or information.

4. Intended participants

In this study, different groups of participants who are working in one of the banks mentioned above will be invited to take part. The below diagram shows the potential participants of the study organised hierarchically into different organisational groups.

Participant Information Sheet


Top management: Chief information officer, Chief technology officer
Middle management: IG managers, AML/or compliance managers
Lower level management: AML/compliance officers, IG/IT professionals, quality analysts

5. Do I have to take part?

Participation in this research project is entirely voluntary. It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep (and be asked to sign a consent form) and you can still withdraw at any time*. You do not have to give a reason. If you wish to withdraw from the research, please contact the researcher, Jihad Al Wahshi, at: jralwahshi1@sheffield.ac.uk

*Please note that it will not possible for a participant's data to be withdrawn from the research once data have been analysed and included within a large dataset. To be specific, you can no longer request to withdraw your data after **1st June 2021** where data analysis phase is started. Likewise, it will not possible to remove your data if it has been already published.

It is important to note that by choosing to participate in this research, this will not create a legally binding agreement, nor is it intended to create an employment relationship between you and the University of Sheffield.

6. What will happen to me if I take part? What do I have to do?

If you are happy to take part and are satisfied with the information and explanations mentioned in this sheet, you will be asked to confirm your participation by signing a consent form. You will be then invited to participate either in a one-to-one interview or be part of a focus group where you will be interviewed as a group. The one-to-one interview will take place at a convenient time/place for you, such as your place of work or over the internet (e.g., Skype or Google meet platforms). However, the focus group interview will take place at the researcher's workplace, namely the Central Bank of Oman. The interview, in general, will involve questions about the risks and challenges that money laundering present to your bank; current practices being adopted to govern ML-related data/ or information; and the consequences of these practices in reducing the risks of ML. Further details about the key themes and interview questions will be sent to you prior to the interview date via the email. Since the interview questions may discuss sensitive topics like money laundering, you can refuse to answer any question that could cause you anxiety/or distress without giving any reason. The interview should take approximately 60 minutes to 90 minutes. As part of consenting to taking part in this study, interviews will be recorded, and then transcribed into text by the researcher. The interview recoding will not be labelled with any personal information such as your name or date of birth, and it will be listened by only the researcher and his supervisors. All interview recordings and the transcripts will be destroyed a year after the submission date of thesis (i.e., October 2023).

If you agree to take part, you would participate in the study for 6 to 12 months during the data collection phase of the project. The research study is funded for 4 years in total (i.e., from October 2019 up to October 2023).

7. What are the possible disadvantages and risks of taking part?

Given the sensitivity of money laundering topic, the information that will be collected and revealed as part of this research might be of a sensitive nature. Therefore, there is a potential psychological harm/or distress associated with your participation in this study. There is a risk of damage to your professional reputation if you accidentally breach customer confidentiality, or disclose sensitive information (e.g., illegal activities) that, if being made public, it could negatively affect the reputation of your bank. During the interview it may be possible that you feel unwilling to share some 'private' or 'sensitive' information that could cause anxiety or discomfort to you.

If this happens you may opt to not answer, and ask the researcher to move on to the next questions. Or alternatively, you are free at any time to withdraw from the interview without given any reason. However, you will be assured the confidentiality of information and protection of any possible disadvantages associated with your taking part in this study. Your personal identities will be anonymised and pseudonyms will assign immediately after the interview. Identities and any distinguishing characteristics indicated in the interview will be omitted from the interview transcript to ensure that participants cannot be identified from the text. Moreover, you will be protected through the signed informed consent form which will allow you to raise any compliant/or concern about the research if you feel that your personal data is compromised or made public without formally obtaining the necessary permission.

Furthermore, you may feel unsecure/ or discomfort to share sensitive information (such as suspicious transaction reports, funds transfers, or number of registered ML cases) through a specific virtual platform like Skype. If this applicable to your case, then you can choose the preferred virtual platform, or alternatively you may ask for the interview to be conducted through a face-to-face format at your

Participant Information Sheet

workplace (i.e., bank). Likewise, your anxiety to share specific information might be increased because that the researcher is representing the Central Bank of Oman. It is important to note that this research is strictly adhere to the ethics policy of the University of Sheffield, and therefore no data will be shared to any external entity or third party including the Central Bank of Oman without obtaining your informed consent or written permission.

8. What are the possible benefits of taking part?

It is hoped that this work will help practitioners within the banking industry of Oman to improve their internal anti-money laundering (AML) policies and procedures by providing them with a rich description of information governance (IG) practices that can lead to possible reduction of ML risks. Regulators such as central banks can also employ the research outcomes to improve the capacity of banks in sharing relevant ML information by, for example, enacting new policies that enable inter-collaboration between financial institutions without impairing the confidentiality and privacy of customer information.

9. Will my taking part in this project be kept confidential?

All the information that we collect about you during the course of the research will be kept strictly confidential and will only be accessible to members of the research team. You will not be able to be identified in any reports or publications unless you have given your explicit consent for this. If you agree to us sharing the information you provide with other researchers (e.g. by making it available in a data archive) then your personal details will not be included unless you explicitly request this. Data collected will be stored securely in a manner consistent with the General Data Protection Regulations (GDPR). All research data collected in this research will be stored on the University of Sheffield password encrypted drive. Printed documents will be stored in a locked cabinet, and they will be only accessed by the researcher.

The audio recordings will be used only for analysis purpose. No other use will be made of them without obtaining your written permission, and no one outside the study will be allowed to get access to the original recordings. The interviewer will take notes on the discussion but any information you give during the interview will be fully anonymised and combined with the views and experiences of other participants who agree to take part.

10. What is the legal basis for processing my personal data?

According to data protection legislation, we are required to inform you that the legal basis we are applying in order to process your personal data is that 'processing is necessary for the performance of a task carried out in the public interest' (Article 6(1)(e)). Further information can be found in the University's Privacy Notice https://www.sheffield.ac.uk/govern/data-protection/privacy/general.

Participant Information Sheet

11. What will happen to the data collected, and the results of the research project?

Due to the unique nature of this research it is very likely that other researchers may find the data collected to be useful in answering future research questions. We will ask for your explicit consent for your data to be shared in this way. The results of this study will be used for the purpose of the Doctoral degree thesis in information studies. However, they might additionally be disseminated at conferences or published in peer reviewed publications (such as academic journals, conference papers, book chapters, etc.), and/or for subsequent research.

If you are interested in receiving a copy of the final report with the results, please contact the researcher at jralwahshi1@sheffield.ac.uk, and it will be sent to you.

Data collected from the interview will be analysed independently by the researcher. Anonymization, including your personal data, will proceed immediately after the interview.

12. Who is organising and funding the research?

This research is funded by the Ministry of Higher Education, Research and Innovation –Oman.

13. Who is the Data Controller?

The University of Sheffield will act as the Data Controller for this study. This means that the University of Sheffield is responsible for looking after your information and using it properly.

14. Who has ethically reviewed the project?

This project has been ethically approved via the University of Sheffield's Ethics Review Procedure, as administered by information department. The University's Research Ethics Committee monitors the application and delivery of the University's Ethics Review Procedure across the University.

15. What if something goes wrong and I wish to complain about the research?

If you feel that your personal data has not dealt correctly as per the information provided in this sheet, or wish to raise any concern/ or complaint about the research, you should first discuss this with the principal investigator or his supervisors. Should you feel still not satisfied, then you can raise your complaint/or concern to the Head of department, Prof. Val Gillet at: v.gillet@sheffield.ac.uk, who will then escalate the compliant through the appropriate channels.

16. Contact for further information

In case you wish to obtain further information about this study, please contact the following people:

Researcher: Jihad Al Wahshi, PhD researcher, University of Sheffield, Information School, email: jralwahshi1@sheffield.ac.uk, or call +968 96400209 / +447307191333

Participant Information Sheet

Researcher's first supervisor: Dr Jonathan Foster, Lecturer in Information Management, email: j.j.foster@sheffield.ac.uk, or call +44 (0)114 222 2633

Researcher's second supervisor: Dr Pamela Abbott, Senior Lecturer in Information Systems, email: p.y.abbott@sheffield.ac.uk, or call +44(0)114 222 2669

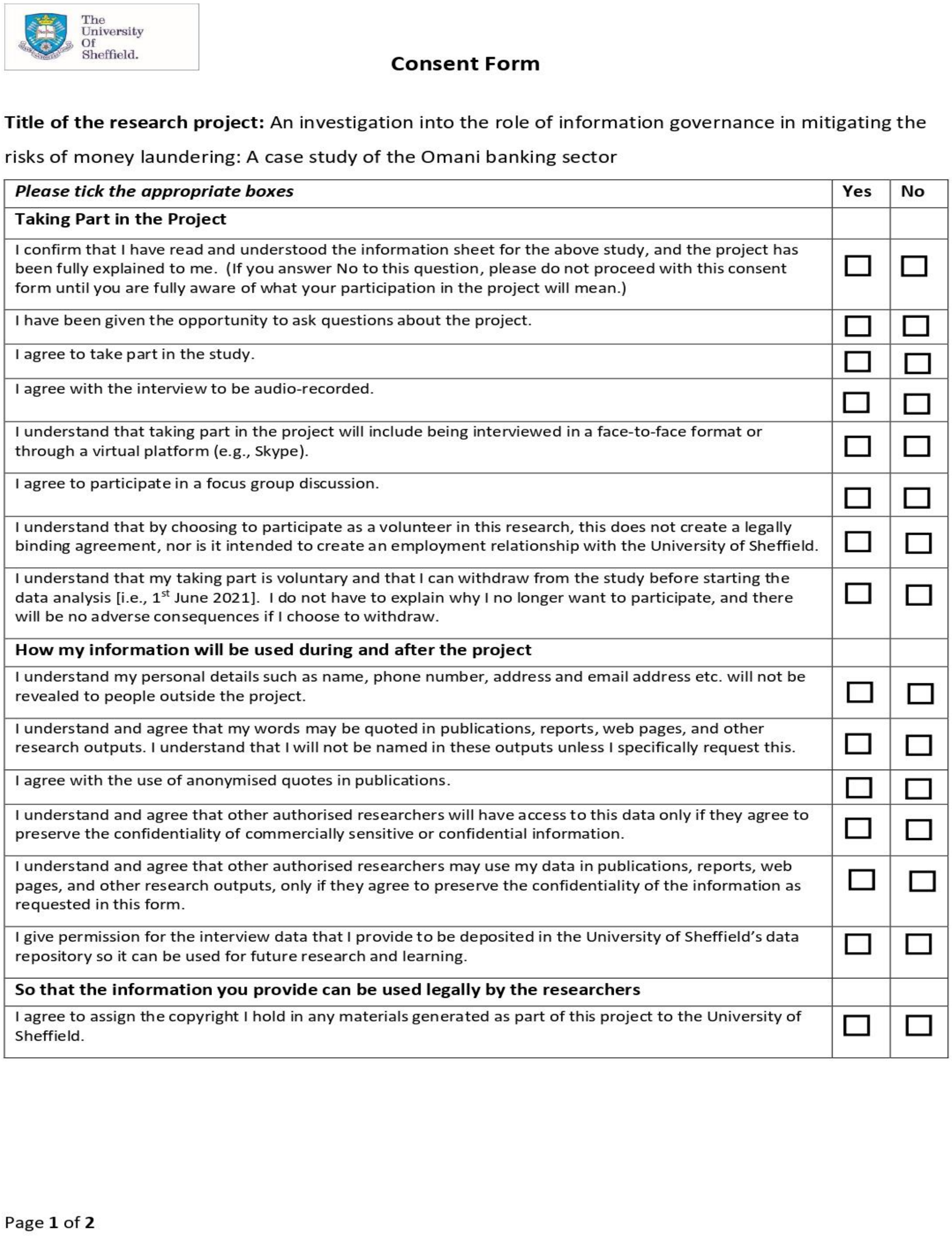
Contact for complaints and questions about the conduct of this research:

Professor Val Gillet, Head of Information School, email: v.gillet@sheffield.ac.uk

Thank you for reading this information sheet and for considering taking part in this research

NOTE: Participants will be given a copy of the information sheet and, if appropriate, a signed consent form to keep.

Appendix 3: Informed Consent



The University Of Sheffield.

Consent Form

Title of the research project: An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

Please tick the appropriate boxes	**Yes**	**No**
Taking Part in the Project		
I confirm that I have read and understood the information sheet for the above study, and the project has been fully explained to me. (If you answer No to this question, please do not proceed with this consent form until you are fully aware of what your participation in the project will mean.)	□	□
I have been given the opportunity to ask questions about the project.	□	□
I agree to take part in the study.	□	□
I agree with the interview to be audio-recorded.	□	□
I understand that taking part in the project will include being interviewed in a face-to-face format or through a virtual platform (e.g., Skype).	□	□
I agree to participate in a focus group discussion.	□	□
I understand that by choosing to participate as a volunteer in this research, this does not create a legally binding agreement, nor is it intended to create an employment relationship with the University of Sheffield.	□	□
I understand that my taking part is voluntary and that I can withdraw from the study before starting the data analysis [i.e., 1st June 2021]. I do not have to explain why I no longer want to participate, and there will be no adverse consequences if I choose to withdraw.	□	□
How my information will be used during and after the project		
I understand my personal details such as name, phone number, address and email address etc. will not be revealed to people outside the project.	□	□
I understand and agree that my words may be quoted in publications, reports, web pages, and other research outputs. I understand that I will not be named in these outputs unless I specifically request this.	□	□
I agree with the use of anonymised quotes in publications.	□	□
I understand and agree that other authorised researchers will have access to this data only if they agree to preserve the confidentiality of commercially sensitive or confidential information.	□	□
I understand and agree that other authorised researchers may use my data in publications, reports, web pages, and other research outputs, only if they agree to preserve the confidentiality of the information as requested in this form.	□	□
I give permission for the interview data that I provide to be deposited in the University of Sheffield's data repository so it can be used for future research and learning.	□	□
So that the information you provide can be used legally by the researchers		
I agree to assign the copyright I hold in any materials generated as part of this project to the University of Sheffield.	□	□

Page **1** of **2**

The University Of Sheffield.

Consent Form

Name of participant   Date   Signature

Jihad Al Wahshi (researcher)   Date   Signature

Project contact details for further information:

1. **Researcher:** Jihad Al Wahshi
   PhD researcher, Information School, University of Sheffield

   Email: jralwahshi1@sheffield.ac.uk

   Telephone number: +968 96400209 / or +44 7307191333

2. **First supervisor:** Dr Jonathan Foster
   Lecturer in Information Management, Information School, University of Sheffield

   Email: j.j.foster@sheffield.ac.uk

   Telephone number: +44 (0)114 222 2633

3. **Second supervisor:** Dr Pamela Abbott
   Senior Lecturer in Information Systems, Information School, University of Sheffield

   Email: p.y.abbott@sheffield.ac.uk

   Telephone number: +44 (0)114 222 2669

4. Professor Val Gillet
   Head of Information School, University of Sheffield

   Email: v.gillet@sheffield.ac.uk

Appendix 4: Participant Profile

Participant ID	Gender	Educational level	Job title	Years of experience	Bank name
P01	Female	Master degree	Senior banking development Analyst	11	Regulatory Bank 1
P02	Male	Diploma	Head of compliance	17	Local Bank 3
P03	Male	Master degree	Head of compliance	14	Local Bank 1
P04	Male	Master degree	Head of compliance	15	Local Bank 2
P05	Male	Master degree	Head of compliance	11	Foreign Bank 7
P06	Female	Master degree	Senior banking examiner	9	Regulatory Bank 9
P07	Male	Bachelor degree	Chief compliance officer	17	Islamic Bank 6
P08	Female	Bachelor degree	Head of Compliance	8	Local Bank 3
P09	Male	Master degree	Chief Compliance officer	22	Local Bank 4
P10	Male	Bachelor degree	Chief compliance officer	11	Islamic Bank 6
P11	Male	Bachelor degree	Chief compliance officer	23	Local Bank 5
P12	Male	Bachelor degree	Head of transactions monitoring	7	Local Bank 3
P13	Male	Master degree	Chief internal audit	25	Local Bank 1
P14	Male	Bachelor degree	Head of information security	18	Local Bank 1
P15	Male	Master degree	Head of big data	20	Local Bank 1
P16	Male	Master degree	Head of business intelligence	15	Local Bank 2

P17	Male	Master degree	VP, Head of performance management and business intelligence	25	Local Bank 5
P18	Male	Bachelor degree	Compliance officer	20	Specialized Bank 8
P19	Female	Master degree	Head of IT governance	12	Islamic Bank 6
P20	Female	Bachelor degree	Head of information security and data governance	16	Islamic Bank 6
P21	Male	Master degree	Chief internal auditor	26	Islamic Bank 6
P22	Male	Master degree	Head of information security and business continuity	20	Local Bank 2
P23	Male	Master degree	Head of IT core systems and business intelligence	10	Local Bank 2
P24	Male	Master degree	Deputy head of internal audit	11	Local Bank 4
P25	Male	Bachelor degree	Head of IT	33	Local Bank 4
P26	Male	Master degree	Chief compliance officer	31	Local Bank 3
P27	Male	Master degree	Compliance officer	20	Local Bank 4
P28	Male	Master degree	Head of IT	40	Specialized Bank 8
P29	Male	Master degree	Head of information Security	20	Local Bank 3
P30	Male	Master degree	VP, Head of information security and business continuity	16	Local Bank 5
P31	Male	Bachelor degree	Information security officer	22	Local Bank 3
P32	Male	Master degree	VP, Head of IT governance	15	Foreign Bank 7

P33	Male	Master degree	Head of credit and market risk	28	Local Bank 3
P34	Male	Master degree	Assistant manager, information security	10	Local Bank 4
P35	Male	Diploma	Deputy head of internal audit	25	Local Bank 3
P36	Male	Master degree	Executive banking examiner	22	Regulatory Bank 1
P37	Male	Bachelor degree	Head of IT auditor	20	Islamic Bank 6
P38	Female	Master degree	Assistant manager, banking surveillance department	14	Regulatory Bank 9
P39	Male	Bachelor degree	Database administrator	6	Local Bank 5
P40	Male	Bachelor degree	Head of database and data backups	14	Local Bank 3
P41	Male	Bachelor degree	Head of digital banking and data analytics	16	Local Bank 3
P42	Female	Bachelor degree	Database Administrator	5	Local Bank 3
P43	Male	Bachelor degree	Chief internal auditor	17	Local Bank 2
P44	Female	Master degree	Operational and market risk Manager	13	Specialized Bank 8
P45	Male	Master degree	Chief internal auditor	16	Local Bank 5
P46	Male	Bachelor degree	Head of data quality support and monitoring	26	Local Bank 3
P47	Male	Master degree	Head of IT	23	Local Bank 5
P48	Male	Master degree	Head of IT core systems and big data	10	Local Bank 1
P49	Male	Master degree	Head of legal	13	Local Bank 3

P50	Male	Master degree	Head IT infrastructure	17	Islamic Bank 6

Appendix 5: Coding Framework

a) IG Enablers

Category	Description	Example Quote(s)
Regulatory Compliance	This code refers to the laws, regulations, and standards that govern the collection, storage, management, and retention of information in the banking industry. This including AML, PCI DSS and Basel	“There are regulatory obligations to keep the [customer] information for a certain period of time, archive it. Now this is an ocean of work of regulations, international laws, treaties, policymakers sometimes locally sometimes outside because you're bound by certain agreements with outside banks…so, information governance is the way [to] handle that information in accordance

		with whatsoever rules or regulations that apply to that handling" (P48).
Information growth rate	The actual rate of increase in retained information; growth rate historical rates of information growth; structured versus unstructured data	"The data is in terabytes, and it's growing heavily, so soon we can be in the petabytes … from the overall growth perspective, it is a very huge growth, every month I think we are getting several terabytes of data being increased in our overall infrastructure" (P23)
Adoption of new technologies	This code captures the integration of advanced technologies such as artificial intelligence, big data analytics, blockchain, and cloud computing to enhance information governance practices. It highlights how these technologies facilitate the automation of repetitive tasks, improve data management efficiency, and enable compliance with regulatory requirements	"I think technology is one of the major enablers on the data, especially machine learning and big data analytics tools. That is one of the major enablers on that. When I say technology, in terms of where you're storing it, how you maintain it, retrieve it, and also on the aspect of security …" (P46)
Senior management support	Senior management support It reflects the commitment, leadership, and strategic direction provided by senior executives to prioritize information governance initiatives.	"Our top management is well aware of the importance of data and the need for governance … So, there is a management buy-in. There is an intention, there is seriousness about the evolving and developing the data governance function [framework] …" (P25)
Organisational/ IT strategy	This code captures the alignment of IT strategy with business objectives to ensure that critical data is delivered promptly and securely. It emphasizes the role of IT in enabling effective IG and competitive opportunities.	"From the IT perspective, we are aligning our IT strategy with the business to ensure that critical data is being served on a timely basis and all the security parameters that are required to ensure that data security is in place, data classification is being managed on all the different levels of applications" (P23)

Customer information gathering	This code refers to the processes and practices involved in collecting accurate and complete data about the customers. It highlights the importance of gathering customer information to support compliance with regulatory requirements, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols.	"If you need to provide better service, better customer experience, be a market leader, you need to capture all this data about the customers" (P40)
Information culture	Reliance on information for key decision-making; Knowledge of IG principles; openness to apply best practices in the daily operations.	"What we're seeing is people [employees] are open to hear what are the regulatory requirements, they're open to understand more about GDPR [General Data Protection Regulation]. They're more interested to understand privacy, they're more interested to understand what data governance is. [So] I think that the culture of knowing more improved our knowledge on data and its importance for the business" (P14)
Funding availability	The provision of financial resources necessary to support the implementation and sustainability of information governance initiatives; investments in technology, training, and compliance measures.	"Necessary budget allocation is an enabler, having a proper budget allocation or budget plan with contingencies, done on an annual basis is an enabler for data governance" (P30)

b) IG Inhibitors

Category	Description	Example Quote(s)
Data quality issues	This code refers to challenges related to inconsistences, inaccuracies, or incomplete data. It highlights how poor data quality can hinder effective information	"The foremost important challenge is the data quality. It is common to every bank which has a long history. First banks had got the books, physical books, they switched to the core banking

	governance, impair decision-making, and increase ML risks due to misclassification of customer profiles.	systems. They got certain information captured at the time and then from the legacy systems as we know that there have been multiple generations of core banking systems.” (P24)
Lack of clear policies and procedures	This code refers to the absence or ambiguity of formal guidelines and processes governing information assets in the Omani banking sector. It highlights how this gap creates confusion among staff, leading to inconsistent implementation of various IG practices across different departments.	“To be honest, it’s the lack of policies and procedures in place. It’s a big challenge. I can tell you, even if something goes wrong, you can't blame the staff. Sometimes the staff will tell you I'm not having policy and procedures in place. How would I know that I should follow this process or should not follow that process? So here it is a very big challenge” (P43)
Legacy IT systems	Application silos; outdated IT infrastructure; unintegrated systems; decentralised IT structure	“In an industry like banking, it's not that easy to implement information governance practices because banks always come with legacy [systems] … so, that is an inhibitor factor [which] holding us back from doing a lot of innovations and [digital] transformation” (P25)
Lack of data integration	This code refers to the fragmentation of customer and financial data across multiple systems, including core banking, mobile banking, reporting, and collection systems. It also highlights the challenges faced by banks to consolidate customer data into a unified view.	“We have the customer data and financial data is spread in different systems. We have some data in the mobile/internet banking and we have data in the core banking system. And we have data in the reporting system. And we have data in the collection system. And to apply the governance in [of] each system is a challenge” (P47)
Lack of IG awareness	The limited understanding among employees and stakeholders about the principles, importance, and	“I would put it at lack of awareness on the importance of certain aspects of data. I could give an example, when our people input the data,

	value of information governance within the Omani banking sector.	there are multiple columns which need to be selected as a drop down. And If the person is not understanding a particular aspect, he usually goes and selects others" (P33)
Lack of clear roles and responsibilities	This code refers to the absence of well-defined roles and responsibilities for information governance within the Omani banking sector. It highlights how this ambiguity can lead to confusion among staff, duplication of efforts, and gaps in accountability.	"Unfortunately, we don't [have] clear roles and responsibilities. To be honest, that's what I told you in the beginning, that we are taking baby steps in terms of data governance, we lack a lot" (P40)
Resistance to change	The reluctance or opposition of employees or stakeholders to adopt new information governance practices, technologies, or processes. It highlights how this resistance can stem from fear of disruption, lack of understanding, or discomfort with new systems.	"We have [data] standards. When we are implementing the standards, there is some kind of resistance among employees" (14)

c) IG practices

Structural Practices		
Category	**Description**	**Example Quote(s)**
Data ownership responsibilities	The allocation of data ownership/stewardship rights and responsibilities to specific individuals or roles.	"The business department owns the full data on the system and we are [IT department] not deciding any retention or any policy without informing them [business departments]" (P47)
Policy-setting procedures	The formal processes established within the Omani banking sector for developing, approving, and implementing information governance	"All our policies are under the custody of compliance, and they monitor whether these policies are updated and reviewed in a timely manner.

	policies. It includes user involvement in policy setting; shared oversight of policy setting, monitoring, and revision.	And then these policies go to the board of directors for the review and approval. So this is basically the chain on policies development" (P44)
Oversight mechanisms	The establishment of dedicated committees or governance bodies to oversee, monitor, evaluate, and ensure effective implementation of IG practices in the bank.	"The oversight mechanism is part of the group risk committee; anything which is related to the data. That's why one of the things which we say is any incident in the bank, you should have a copy of that incident. If it is related to the data … Definitely they step in and take the necessary action" (P46)
Procedural practices		
Data Policies, Standards, Processes and Procedures	This code refers to the set of policies and procedures that Omani banks developed to govern their data. This including data security policy, KYC policy, backup/data retention policy, compliance policy, and data classification.	"We have information security policy …we have a user access control management policy. We also have a cryptography and encryption security policy … we have backup and [data] retention policy …" (P34)
Compliance monitoring	This code refers to the processes and mechanisms that Omani banks used to ensure adherence to regulatory requirements and organisational policies related to information governance. It includes the supervision of data professionals, routine audits, and periodic reviews.	"In each of our audit engagements, we look at compliance with the policies, compliance with the standards, compliance with the regulations … wherever we see that the data is incomplete or not accurate, or the data does not properly represent the actual situation or the latest regulatory requirements … then we highlight [that] in our audit observation, and it goes to various levels like … the board of directors [or] senior management" (P44)

Information classification	The process of classifying data according to its criticality and value. It involves assigning levels of classification, such as public, confidential, or restricted, to ensure that information is handled appropriately in line with regulatory requirements and organizational policies.	“We do classify our data [based] on the value. There is a criterion for that, we have classification guidelines … Also, we consider the regulation part, how important of [is] this data ... So, all this is part of the [information] classification [policy]. The first [thing] is value and [then] criticality of this information” (P20)
Enforce retention/archiving	Enact retention policies/possible auto-deletion or archiving of AML-related data.	“As a policy, we [have to] keep all AML [Anti-money laundering] related data for 10 years minimum. Where there are STRs [Suspicious Transaction Reports], for example, we must even maintain this data longer than the 10 years” (P27)
Establish and monitor access	This code refers to the implementation of robust controls to regulate, oversee, and restrict access to sensitive data. These practices involve defining user roles, granting permissions based on necessity, and continuously monitoring access to ensure compliance with governance policies and prevent unauthorized data sharing or usage.	“All classified data in the bank is monitored by a data leakage prevention system. The system prevents any unauthorized or [if] you want to send this data outside, because it's classified by nature, by context, there are rules and policies that have been implemented on this system to trigger if there is any unauthorized task on this information” (P20)
Apply backup practices	Implementing backup policies according to RPO/RTO criteria; adopting the right technologies to ensure the timely restoration of critical data; business continuity plan; disaster recovery;	“Yes we perform backup. We have two types of backup here: full backup and [incremental]. For full backup, we take full backup, at night, daily at 10pm … for all the databases. And [incremental] backup every one hour, for all the databases too” (P41)

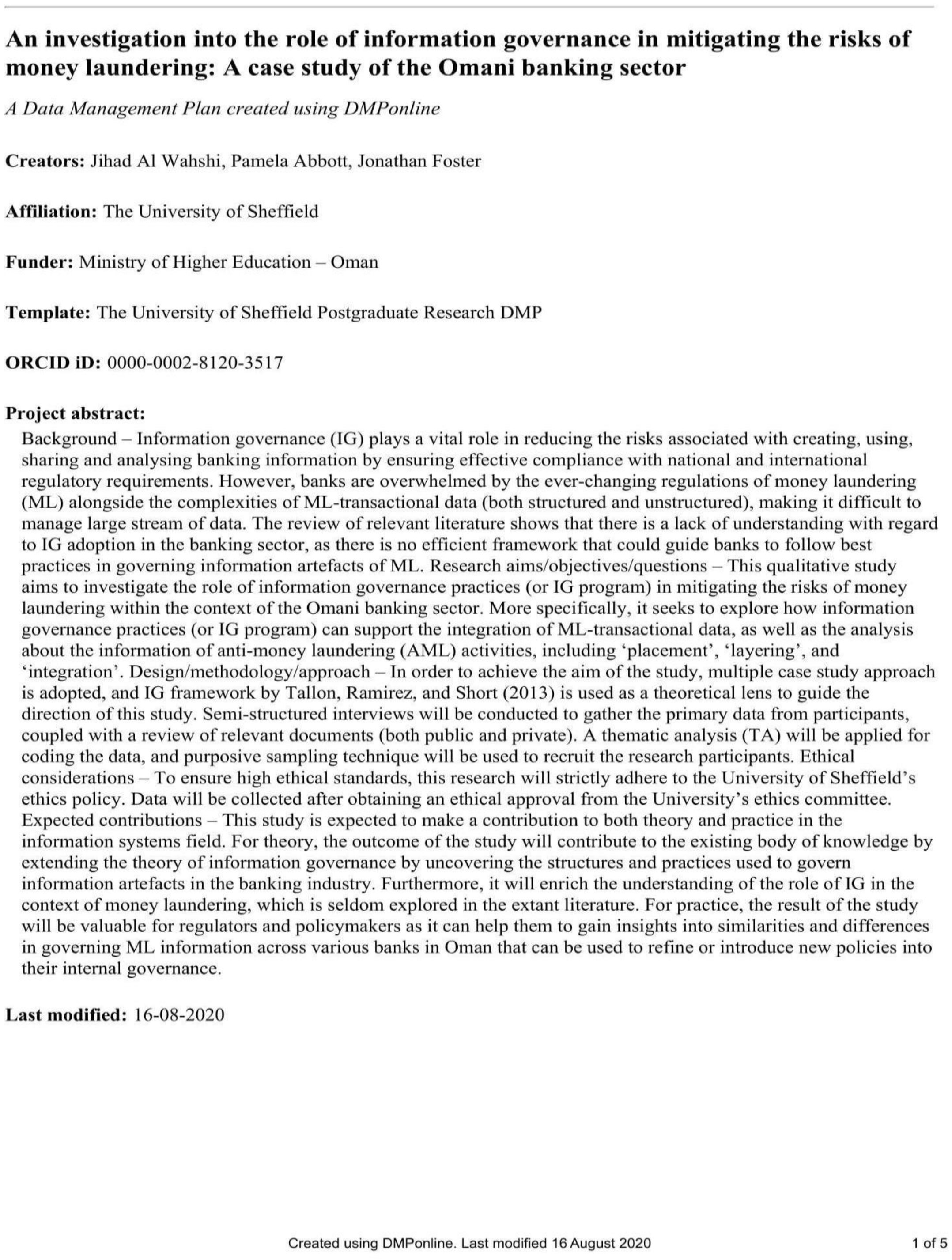
Apply data validation practices	This code refers to the processes implemented within the Omani banking sector to ensure the accuracy, consistency, and reliability of AML-related data. These practices involve verifying data during collection, entry, and processing to identify and correct errors or inconsistencies.	"We have now started the periodic reviews of customers' data and we have done the system validations … we created multiple fields in the onboarding system, and we made them mandatory so that we should be getting the information which we need, for example, income level of the customer, occupation of the customer, his date of birth, nationality, FATCA [Foreign Account Tax Compliance Act] related information" (P27)
Relational practices		
Training/ User education	This code refers to the initiatives undertaken by Omani banks to educate employees on various aspects related to information management and compliance requirements. These efforts include providing tailored training sessions, workshops, and awareness programs.	"We have two main mandatory courses which have been managed by the training department. [One] is about money laundering, and the other [is about] information security, which are mandatory to all the staff to attend … In that [these] course[s], we … assure that our employees have got enough knowledge about the data classification, data governance and other aspects" (P46)
Communication/ ideas exchange	This refers to the mechanisms established to facilitate open communication and the sharing of ideas among employees and stakeholders regarding information governance practices. These mechanisms involve regular meetings, collaborative platforms (e.g., emails, Google meet) and other tools.	"We send emails, and we conduct awareness sessions in order to communicate any new policy or changes to employees. We do site visits, different methods that could assist us in making them [employees] understand" (P35)

d) Consequences

Intermediate performance effects		
Category	**Description**	**Example Quote(s)**
Improve operational efficiency	This code demonstrates how the implementation of effective IG practices improve the productivity of AML/ compliance professionals by providing timely access to information.	“Positive impacts definitely would include ease of access to the information … [therefore] back and forth between compliance and other departments or branches would be less. quicker assessments of customers” (P08)
Improve customer service	This code highlights how the implementation of effective IG enhance customer service by facilitating access to relevant and accurate customer data. It provides examples on how banks were able to personalise their products and services to meet customer needs.	“[The] more information you have about the customer [the] better you will serve the customer … [because] if we have the relevant and accurate information, we will be in a better position to serve the customers. You will be in a better position to know the needs and wants of the customer. So, we can design the products according to the requirements of customers” (P27)
Improve data-driven decision making	This code emphasises the critical role that IG play in enhancing data-driven decision-making. It provides examples on how accurate, complete, and relevant information enabled compliance professionals to make informed decisions related opening accounts, filing suspicious activity reports and/or denying transactions.	“So that data is critical to the decision making, either I accept the transaction or I reject or I send a suspicious report to FIU [Financial Intelligence Unit]” (P32) “The data is the core activity that we do. Because of data, we can make a decision. But in the absence of data, it’s not clear what decision we can take” (P09)
Improve data quality	This code demonstrates the positive impacts of IG on data quality, particularly in areas related to customer profiling	“Information is the hub for the organization and governing it will not cause any issue in the bank. It’s the other way, it will benefit, it will provide right,

	and detection of suspicious transactions.	and accurate information …" (P20) "On the top of that, errors [that] take place due to manual exchanging of data will become less" (P38)
Risk Mitigation		
Mitigate money laundering risks	This code shows how the increased quality of KYC/customer data enabled Omani banks to easily detect and prevent suspicious transactions; thereby reducing money laundering risks.	"I think we [become] very highly efficient in terms of AML [Anti-money laundering] by detecting all suspicious transactions, because data is under the same umbrella and everything is in one place and assessment will be very easy and it will be controlled very well. Better than if it is split in other systems … " (P26) "If we collected the right KYC data and take policies and procedures seriously from the frontline until the CEO [Chief Executive Officer]. If that happened … we could fight 80%-90% of money laundering …we will reduce the risk on the bank from an AML perspective" (P12)
Mitigate compliance risks	This code shows how effective IG practices enabled Omani banks to comply with both national and international regulations, such as AML, PCI DSS and Basel.	"Without the data, it's very difficult and tedious to mitigate the compliance risks. So only, it's with a strong data, strong information governance in place, we are able to mitigate our compliance risks" (P24)

Appendix 6: Data Management Plan



An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

A Data Management Plan created using DMPonline

Creators: Jihad Al Wahshi, Pamela Abbott, Jonathan Foster

Affiliation: The University of Sheffield

Funder: Ministry of Higher Education – Oman

Template: The University of Sheffield Postgraduate Research DMP

ORCID iD: 0000-0002-8120-3517

Project abstract:

Background – Information governance (IG) plays a vital role in reducing the risks associated with creating, using, sharing and analysing banking information by ensuring effective compliance with national and international regulatory requirements. However, banks are overwhelmed by the ever-changing regulations of money laundering (ML) alongside the complexities of ML-transactional data (both structured and unstructured), making it difficult to manage large stream of data. The review of relevant literature shows that there is a lack of understanding with regard to IG adoption in the banking sector, as there is no efficient framework that could guide banks to follow best practices in governing information artefacts of ML. Research aims/objectives/questions – This qualitative study aims to investigate the role of information governance practices (or IG program) in mitigating the risks of money laundering within the context of the Omani banking sector. More specifically, it seeks to explore how information governance practices (or IG program) can support the integration of ML-transactional data, as well as the analysis about the information of anti-money laundering (AML) activities, including 'placement', 'layering', and 'integration'. Design/methodology/approach – In order to achieve the aim of the study, multiple case study approach is adopted, and IG framework by Tallon, Ramirez, and Short (2013) is used as a theoretical lens to guide the direction of this study. Semi-structured interviews will be conducted to gather the primary data from participants, coupled with a review of relevant documents (both public and private). A thematic analysis (TA) will be applied for coding the data, and purposive sampling technique will be used to recruit the research participants. Ethical considerations – To ensure high ethical standards, this research will strictly adhere to the University of Sheffield's ethics policy. Data will be collected after obtaining an ethical approval from the University's ethics committee. Expected contributions – This study is expected to make a contribution to both theory and practice in the information systems field. For theory, the outcome of the study will contribute to the existing body of knowledge by extending the theory of information governance by uncovering the structures and practices used to govern information artefacts in the banking industry. Furthermore, it will enrich the understanding of the role of IG in the context of money laundering, which is seldom explored in the extant literature. For practice, the result of the study will be valuable for regulators and policymakers as it can help them to gain insights into similarities and differences in governing ML information across various banks in Oman that can be used to refine or introduce new policies into their internal governance.

Last modified: 16-08-2020

An investigation into the role of information governance in mitigating the risks of money laundering: A case study of the Omani banking sector

Defining your data

- Where does your data come from?
- How often do you get new data?
- How much data do you generate?
- What format(s) are your data in?
- If pre-existing datasets are being used, where will these come from? How will they be used? Who owns them?

The data for this research will come from banking professionals (Chief Information officer (CIO), information governance/IT staff, and Anti-money laundering officers) in 6 selected banks in Oman, namely (1) Bank Muscat; (2) National Bank of Oman; (3) Bank Dhofar; (4) Sohar International Bank; (5) Oman Arab Bank; and (6) HSBC Oman Bank. These qualitative data will be gathered once during the fieldwork activity. The data format of each category has been chosen in line with the UK data service (see https://www.ukdataservice.ac.uk/manage-data/format/file-formats.aspx). In general, the chosen formats are widely-used formats such as MS Word and plain text, which are compatible with various computer programs, and therefore the formatted files can remain readable/usable in the future. Details of research data are described below:

1. **Interview transcripts**

Software: QSR NVivo 12; Microsoft word

Data format: MS Word (.doc/.docx); QSR Nvivo Project (.nvp)

Estimate data volume: 2 GB

**assuming average Word file size of 350KB*

2. **Audio-recordings**

Software:Audacity; QSR NVivo 12

Data format: Waveform Audio Format (.wav); QSR Nvivo Project (.nvp)

Estimate data volume: 2 GB

**assuming average wav file size of 4MB*

3. **Field notes**

Software: Microsoft Notepad; QSR NVivo 12

Data foramt: Plain text, ASCII (.txt); QSR Nvivo Project (.nvp)

Estimate data volume: 500 MB

**assuming plain text file size of 40KB*

4. **Public and private documents**

Software: Adobe Acrobat Reader DC; QSR NVivo 12

Data format: PDF (.pdf); QSR Nvivo Project (.nvp)

Estimate data volume: 2 GB

**assuming plain text file size of 4MB*

Total estimated data volume: 6.5 GB

**Note: The documents will be available in both Arabic and English

Looking after your data

- What different versions of each data file do you create?
- What additional information is required to understand each data file?
- Where do you store your data?
- How do you structure and name your folders/files?
- How is your data backed up?
- How will you test whether you can restore from your backups?
- What safeguards will you put into practice?

Data storage and security

All research related materials will be stored on the UoS information school's secure 'X: drive', which is managed and maintained by IT services. This research storage is password protected using a University account, and will only be accessed by the principal researcher and supervisory team. To ensure high availability and redundancy of data, the research storage drive is backed up regularly by IT team, and split between two data centres which could ensure quick and easy retrieval of stored data in case of disaster or hardware failure. To ensure that the backup can be restored, the researcher will perform a monthly restoration test by requesting IT services team to provide a copy of snapshot for a particular period of time.

Data Backup

The researcher will follow a 3-2-1 backup strategy (3 copies; 2 different storage media; 1 offsite). Throughout the project lifecycle, research data and files will be backed up to two hard drives (HDD) in addition to the master copy which will be stored on the University's file server mentioned above.

- **HDD 1**

Encrypted external hard drive with two-factor authentications to be updated (synchronised) on a weekly basis using Microsoft SyncToy 2.1 software. This drive will be kept and locked in a secure physical location at the information school.

- **HDD 2**

Another backup copy will be stored on the departmental laptop and will be synchronised on an hourly basis during the working days (Monday to Friday). To minimise the risks of data breaching or hacking, this laptop will not be used for surfing the internet and will be protected by password and data encryption at rest.

Moreover, the researcher will store an additional copy on the University's Google drive as a proactive measure in case these backups are not functioning properly.

Incremental data will be configured and cross-verified after each run by reviewing the error logs and compare the data size between the source and destination.

File structure and naming convention

Following the recommendation of the University of Sheffield, the research data and documentation files will be grouped and organised using a hierarchical structure, by which more frequent accessible files to be placed at higher-level folders. This structure will help to restrict access to the folder level while simplifying the management of permissions. Another benefit of organising data into a hierarchical structure is that it will enable the researcher and collaborators to identify and allocate research data files efficiently and effectively. Higher-level folders will be named by topic, following by sub-topics (e.g., 1. Interview--> 1.1 Interview transcripts --> 1.2. Focus group transcripts).

For this study, file naming convention will be consistent with the University of Queensland's Division of Technology, Information and Learning Support (TILS)(see https://www.library.qut.edu.au/about/management/documents/QUTTILSDocNamingConvention.pdf).

TILS convention naming consists of four parts joined together with an underscore character (_), including a prefix, document title, version number, and date of creation. The below provides more information on how these parts are interconnected and used.

<type><document title><version number><date>

Where:

<type> specifies the type of event/data material (e.g., AGD: Agenda, REP: Report ...etc).

<document title> describes the purpose of the document (e.g., Interview guide)

<version number>indicates minor or substantive changes and edits to files (e.g., V1.1: minor change; V2.0: significant change)

<date> The date of file creation or collection (e.g., YYYY-MM-DD: 2020-07-14)

Version control

In order to keep track of the changes and modifications made to the original research data or files, version numbering will be embedded within the file name (e.g., Informed Consent_2020-07-14_V1.0). This versioning system is particularly useful because it will provide details on the level of changes (minor or substantive) made to the document, as well as the file history organised by date.

Data documentation

A plain-text file with a name "README" will be embedded in data files in order to provide contextual information that can enable other users who have access to these data collection to make informed use of data. For example, the contextual information under the folder 'interview' will include a descriptive detail about each interview, such as interview date, interviewee name, pseudonym of interviewee, and occupation of the interviewee. Data list template as prescribed by the UK data service will be adapted and embedded at the interview-folder level to quickly identify and locate relevant interview transcripts or audio (see https://www.ukdataservice.ac.uk/media/604454/datalist.gif). Nvivo software will be used to sort and organise data documentations by importing relevant templates such as informed consent and interview guide into Nvivo project and store them in the "documentation" folder.

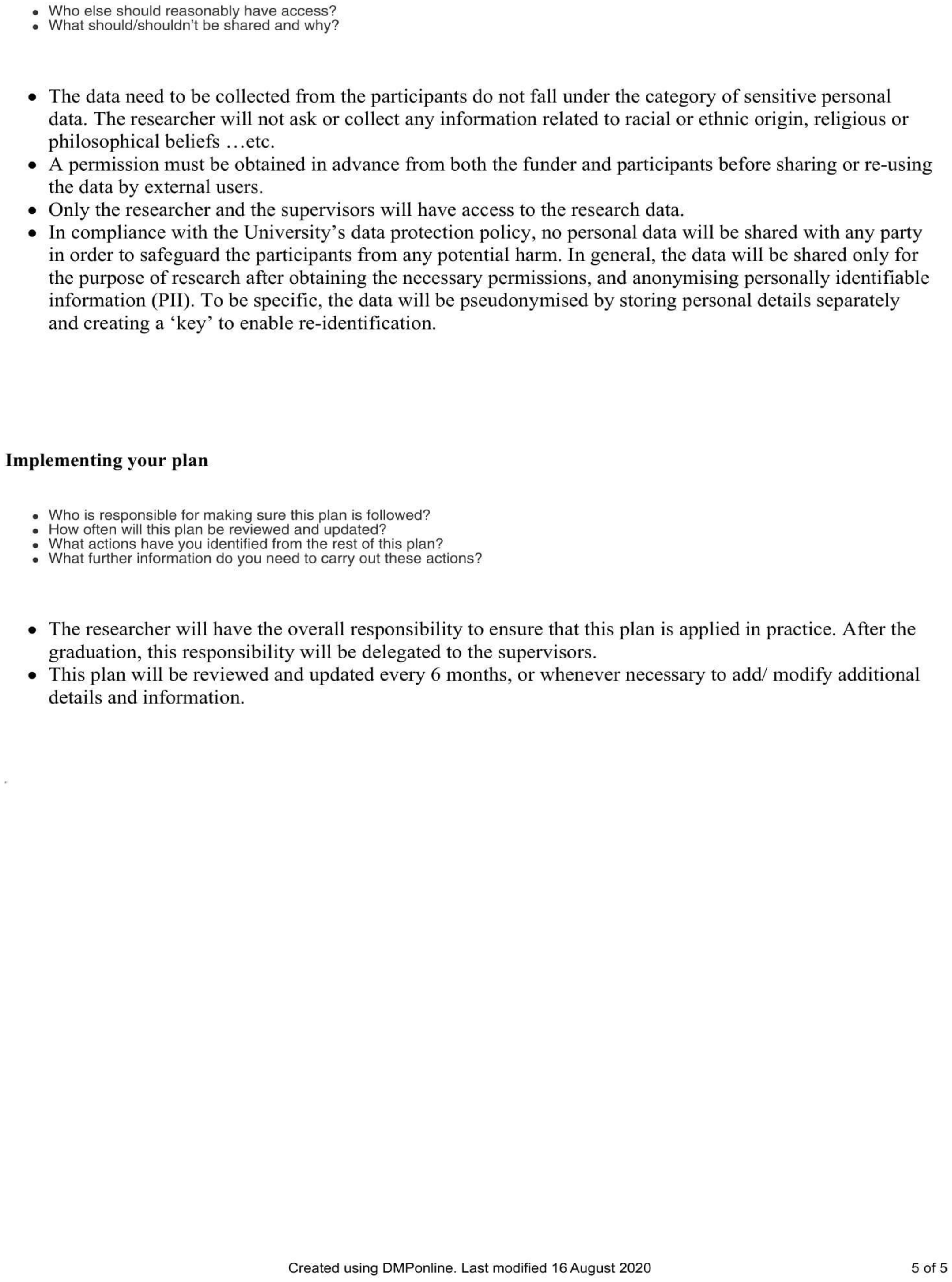
Archiving your data

- What should be archived beyond the end of the project?
- For how long should it be stored?
- When will files be moved into the archive?
- Where will the archive be stored?
- Who is responsible for moving data to the archive and maintaining it?
- Who should have access and under what conditions?

The researcher is obliged to ensure the confidentiality and anonymity of participants' data from inappropriate access. With this in mind, unless it is required by the University for verification purposes, no data will be archived prior obtaining consent /or approval from the original source (i.e., banks). As such, the duration of preservation will depend upon the permission given by the data owner or participants. If approved, then the interview recording and transcripts will be deposited into ORDA—the University's data repository—for a period of ten years, as recommended by the university. The researcher will be responsible for arranging and moving the relevant data into the archive. The access to archived data will be restricted to only the researcher and the supervisors unless otherwise formally authorised to other users. The data should not be used for any business purposes without a written approval from the researcher.

Sharing your data

- Could any of your data be considered sensitive personal data under the GDPR?
- Does permission need to be obtained for future re-use and sharing?
- Have participants transferred copyright (if necessary)?
- Who else has a right to see or use this data?



- Who else should reasonably have access?
- What should/shouldn't be shared and why?

- The data need to be collected from the participants do not fall under the category of sensitive personal data. The researcher will not ask or collect any information related to racial or ethnic origin, religious or philosophical beliefs …etc.
- A permission must be obtained in advance from both the funder and participants before sharing or re-using the data by external users.
- Only the researcher and the supervisors will have access to the research data.
- In compliance with the University's data protection policy, no personal data will be shared with any party in order to safeguard the participants from any potential harm. In general, the data will be shared only for the purpose of research after obtaining the necessary permissions, and anonymising personally identifiable information (PII). To be specific, the data will be pseudonymised by storing personal details separately and creating a 'key' to enable re-identification.

Implementing your plan

- Who is responsible for making sure this plan is followed?
- How often will this plan be reviewed and updated?
- What actions have you identified from the rest of this plan?
- What further information do you need to carry out these actions?

- The researcher will have the overall responsibility to ensure that this plan is applied in practice. After the graduation, this responsibility will be delegated to the supervisors.
- This plan will be reviewed and updated every 6 months, or whenever necessary to add/ modify additional details and information.

Appendix 7: Descriptions of Case Studies

1. Local Bank 1

Bank 1 is one of the leading financial institutions in Oman. The bank has the largest network of branches and ATMs across the country, enabling it to serve a diverse customer base that spans urban and rural areas. It operates with a strategic vision to provide innovative financial solutions that meet the evolving needs of its customers. Its strategic focus is anchored in customer-centricity, digital transformation, and expanding its market reach both locally and regionally. As a leader in the Omani banking sector, Bank 1 is often acting as a benchmark for other financial institutions in terms of governance practices and regulatory compliance. This market position provides it with access to substantial resources, including advanced technology infrastructure and specialized human resources. This enables the bank to implement sophisticated Information Governance (IG) frameworks that support its digital transformation and compliance goals. However, its expansive operations also introduce challenges, such as coordinating IG practices across various departments, business units, and geographical locations. Internally, Bank 1 has cultivated a culture of innovation and compliance, driven by its strategic emphasis on aligning with international standards and best practices. This proactive approach to governance is influenced by its commitment to maintaining stakeholder trust and achieving sustainable growth.

Bank Muscat offers a diverse range of financial products and services catering to retail, corporate, investment, and Islamic banking customers. These include personal loans, savings and current accounts, wealth management services, corporate financing, and trade finance. The bank has also positioned itself as a leader in digital banking, with robust online and mobile banking platforms designed to enhance customer experience and operational efficiency. As the largest bank in Oman, Bank Muscat manages vast amounts of data across multiple departments and customer segments. This scale necessitates robust data governance mechanisms to ensure data accuracy, security, and accessibility.

2. Local Bank 2

Bank 2 is one of the pioneering banks in Oman that established in 1973. As the first bank established in Oman, Bank 2 has built a legacy of trust and reliability, striving to balance tradition with modernity in its strategic approach. The bank's vision aligns with Oman's 2040 goals, emphasizing the adoption of cutting-edge technologies and the creation of sustainable financial solutions through innovation and operational excellence. Its strategic goals include enhancing operational efficiency, and strengthening its position as a trusted financial partner across Oman.

Bank 2 offers a diverse portfolio of products and services, tailored to meet the needs of individuals, businesses, and institutional clients. Its retail banking services include personal loans, savings and current accounts, credit cards, and home financing. On the corporate side, the bank provides trade finance, cash management, corporate lending, and treasury solutions. Bank 2 also has a robust Islamic banking arm under the Muzn brand, offering Sharia-compliant financial products and services. Additionally, the bank is known for its investment in digital banking platforms, providing seamless and secure online and mobile banking experiences.

Bank 2 operates within a competitive banking sector characterized by rapid technological advancements and increasing regulatory demands.

Internally, the bank emphasizes customer-centricity, innovation, and compliance with regulatory frameworks. Its organizational culture promotes agility, enabling it to respond swiftly to market changes while maintaining operational stability. Additionally, the bank continuously investing in technologies like artificial intelligence (AI), big data analytics, and cybersecurity.

3. Local Bank 3

Bank 3 is a prominent financial institution in Oman, established in 1984. The bank's mission centers on maintain a strong financial position, delivering excellent customer service, Driving innovation and digital transformation, and complying with regulatory requirements. The bank received various awards in recognition for its brand and products, including accolades for excellence in digital banking, customer service, and innovative financial solutions. Notable awards include the 'Best Digital Bank in Oman', reflecting its commitment to leveraging technology to enhance customer experiences.

Similar to other commercial banks, Bank 3 offers a comprehensive range of financial products and services tailored to meet the diverse needs of retail, corporate, and institutional clients. its retail products include savings and current accounts, personal loans, credit cards, mortgages, and insurance products. For corporate clients, the bank provides trade finance, working capital solutions, and cash management services. Additionally, OAB has a robust Islamic banking window, offering Sharia-compliant financial solutions such as Murabaha financing, Ijarah leasing, and Sukuk investments.

Bank 3 operates in a dynamic financial landscape marked by increasing competition, regulatory pressures, and rapid technological advancements. The bank's mid-sized structure enables it to remain agile and responsive to market changes while maintaining a strong focus on customer needs. Bank 3 places a high emphasis on digital innovation, continuously investing in technologies to enhance customer experiences and operational efficiency. Internally, the bank fosters a culture of innovation, compliance, and accountability, ensuring its operations align with global best practices and local regulatory frameworks.

4. Local Bank 4

Bank 4, established in 1990, is the fastest growing bank in Oman. The bank's mission is to deliver exceptional financial services by offering innovative and customer-centric solutions that meets the diverse needs of its customers. It also aims to maintain a strong financial position by managing risk effectively. The core value of the bank is to deliver trust and confidence through exceptional service, transparency, and commitment to excellence. The bank offers similar products to other commercial banks, which include customer and corporate banking services. Additionally, the bank has invested heavily in digital banking platforms, offering seamless and secure online and mobile banking experiences.

The organisational structure of Bank 4 reflects its commitment to enhance operational efficiency and customer satisfaction. It comprises distinct divisions, including Retail Banking, Wholesale Banking, Treasury and Investments. Each division operates with autonomy while maintaining alignment with the bank's overarching strategic goals. This structure ensures that the bank can deliver specialized services to different customer segments while fostering coordination and synergy across its operations. Bank 4 emphasizes innovation, compliance, and customer-centricity, which shape its operational strategies and information governance (IG) practices.

5. Local Bank 5

Bank 5 was established in 2007 and rebranded in 2018 to reflect its expanded vision and strategic objectives. The bank aims to become a world-leading Omani service company, assisting customers, communities, and individuals in achieving prosperity and growth. Furthermore, it aims to expand internationally by building strategic partnerships, leveraging advanced technologies, and offering innovative financial solutions tailored to diverse markets. Its strategic objectives include enhancing financial inclusion, investing in digital transformation, and aligning with Oman’s vision 2040 by contributing to the nation’s economic diversification and development. The bank offers a comprehensive suite of financial products and services tailored to retail, corporate, and institutional clients.

The bank's rebranding in 2018 signified a strategic shift towards becoming a more agile and customer-focused institution, aiming to align with global banking standards and technological advancements. This necessitates robust information governance (IG) practices to manage data effectively and comply with regulatory requirements. Additionally, the bank's corporate governance philosophy emphasizes accountability, fairness, responsibility, and transparency. This commitment influences IG practices by promoting ethical data management and decision-making processes.

6. Islamic Bank 6

Bank 6 was established in 2013 as the first Islamic bank in Oman. It operates with a strategic vision to provide innovative and Sharia-compliant financial solutions. The bank strives to be a trusted partner for its customers, offering banking services that strictly align with Islamic principles and values. Bank 6 differentiated itself from conventional banks by offering a wide range of Sharia-compliant products, such as Mudharaba, Musharaka, Murabaha, Istisna, Ijarah, Musawama, and Salam—as described in the table below. The bank's commitment to Sharia compliance drives its operational strategies and influences its corporate culture. The need to align all financial products and practices with Sharia principles introduces unique governance requirements. Information governance (IG) frameworks must integrate Sharia guidelines to ensure transparency and compliance in data management and reporting. Its relatively smaller size compared to larger commercial banks allows it to maintain agility and focus on customer-centric services, particularly within the niche of Islamic finance.

Islamic Product(s)	**Definition**
Murabaha (Cost-Plus Financing)	A financing arrangement where the bank purchases an asset and sells it to the customer at a pre-agreed profit margin, allowing deferred payment.
Ijarah (Leasing)	An arrangement where the bank leases an asset to the customer for a fixed period and rental amount. Ownership remains with the bank until a transfer agreement.
Mudaraba (Profit-Sharing)	A partnership where one party provides capital (Rab-ul-Mal) and the other manages the business (Mudarib). Profits are shared as per agreement, and losses are borne by the capital provider.

Musharaka (Joint Venture)	A joint partnership where both the bank and the customer contribute capital to a project or asset, sharing profits and losses in proportion to their investment.
Sukuk (Islamic Bonds)	Sharia-compliant financial certificates representing ownership in tangible assets, services, or investments. Profits are distributed, but interest (Riba) is not permitted.
Istisna (Manufacturing Contract)	A contract where the bank finances the production of goods or assets, which are manufactured and delivered at a pre-agreed time and price.
Salam (Advance Payment)	A forward contract where the bank pays in advance for goods to be delivered at a future date, often used in agricultural or manufacturing sectors.
Takaful (Islamic Insurance)	A cooperative insurance model where participants contribute to a fund used to support members in times of need, avoiding elements of uncertainty and gambling.
Wakalah (Agency Agreement)	A contract where the bank acts as an agent (Wakil) on behalf of the customer to manage investments or execute transactions under agreed terms.
Qard Hasan (Benevolent Loan)	An interest-free loan extended by the bank to customers, intended to assist with specific needs without any profit to the bank.

Table 32: Islamic Products

The Bank also serves the government sector, commercial clients and other corporates by providing wholesale banking. The Bank supported the employees with training and development by providing full financial support to commence their academic and professional qualifications. The organisational structure of Bank 6 is designed to support its Islamic banking mandate. It includes key divisions such as Retail Banking, Corporate Banking, Treasury and Investment, Sharia Compliance, and Risk Management. The Sharia Supervisory Board plays a critical role in ensuring that all products and services comply with Islamic law.

This additional governance layer differentiates the bank from conventional banks, adding a unique dimension to its decision-making and product development processes.

Bank 6 operates under both the Central Bank of Oman’s regulatory framework and Sharia law, which necessitates dual compliance. This creates additional complexity in IG practices, requiring robust mechanisms to manage and reconcile these overlapping requirements. As an Islamic bank, the bank must include strict screening processes to ensure that all investments and transactions comply with ethical and Sharia-compliant criteria.

7. Foreign Bank 7

Bank 7 was established in 1964 as the largest financial institutions in the Middle East and Africa (MEA) region. The bank has branches in multiple countries across the MEA region, Europe, Asia, and the USA. The vision of Bank 7 is to be the institution of choice for customers, employees, investors, and suppliers by delivering exceptional banking services that drive economic growth, creating value for stakeholders, and support sustainable development. Strategically, the bank focuses on expanding its international presence, leveraging digital transformation, and aligning with country’s national vision to support economic diversification and development.

Bank 7 offers a wide range of financial products and services across various segments, including personal banking, asset management, and business banking. The bank also offers Sharia-compliant Islamic banking products, catering to clients seeking ethical financial solutions.

The bank operates in a dynamic and highly competitive financial environment, which requires strict adherence to diverse regulatory frameworks across multiple jurisdictions; each with unique regulatory and cultural requirements, making compliance a cornerstone of its strategy. Additionally, the bank must navigate geopolitical factors, economic volatility, and varying market conditions that influence its operations, governance practices, and strategic decisions.

The organisational structure of Bank 7 includes various divisions –such as Retail Banking, Corporate Banking, Treasury, and Risk Management— that overseen by senior executives. The Board of Directors, comprising experienced professionals, provides strategic direction and oversight. The bank operates subsidiaries and affiliates across multiple countries, enhancing its global footprint.

8. Specialised Bank 8

Bank 8 was established in 1997 as a government-owned financial institution dedicated to support the economic development and diversification of Oman. The institution has evolved to become a cornerstone of development financing in the country. In 2023, a significant restricting transformed Bank 8 into the “Development Bank”, enhancing its capital to approximately $1.3 billion USD and increasing its financing capacity to up to $19.5 million USD for specific projects.

Bank 8 aims to be the preferred partner in financing projects, and small and medium enterprises (SMEs) in alignment with national development plans. Its mission encompasses supporting economic diversification, fostering job creation for Omanis, and contributing to the goals outlined in Oman Vision 2040.

Unlike other commercial banks, the Bank offers specialized financial products tailored to developmental needs of Oman. These products focus on developmental impact and economic sustainability, setting Bank 8 apart from profit-oriented commercial banks. The below table outlines these products along with their descriptions:

Product/ Service	**Description**
Development Loans	Low-interest or interest-free loans aimed at financing projects in key sectors such as agriculture, fisheries, tourism, healthcare, education, and manufacturing. These loans are designed to promote economic diversification and job creation.
SME Financing	Tailored financial solutions and advisory services for small and medium-sized enterprises (SMEs) to encourage entrepreneurship and support business growth across various sectors.
Project Financing	Funding for large-scale projects that align with national development priorities, including infrastructure, industrial ventures, and other initiatives that contribute to economic growth.
Sector-Specific Funding	Financial support targeting specific sectors such as logistics, mining, quarries, and light installations, in line with the government's economic diversification strategy.
Microfinance	Small loans provided to micro-enterprises and self-employment projects to stimulate grassroots economic activity and support low-income entrepreneurs
Green Economy Project Support	Financing for environmentally sustainable projects, including those aimed at achieving zero carbon emissions and promoting green technologies.

Table 33: Specialised Products

Bank 8 operates under the supervision of the Central Bank of Oman and Ministry of Finance, with a Board of Directors overseeing its strategic direction. The bank’s structure includes dedicated divisions for managing loans, project evaluations, and sector-specific financing. Its teams work closely with government agencies to align its financing strategies with national development plans. The bank's activities are influenced by governmental priorities, macroeconomic policies, and sectoral development strategies.

As a government-owned bank, Bank 8 must maintain high levels of transparency and accountability, adhering to government reporting requirements and audit standards. However, the Bank often operates under budgetary constraints, requiring effective information governance practices to maximize the impact of its activities.