Exploring cyber risk reporting in South African banks

TL Rikhotso

orcid.org 0009-0000-3919-8497

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Master of Commerce in Applied Risk Management* at the North-West University

Supervisor: Ms G Nyamah
Assistant supervisor: Mrs W Meiring

Graduation: May 2025

PREFACE

This mini-dissertation is the final deliverable for the Master of Commerce (MCom) in Applied Risk Management. The mini-dissertation was written in article format and consists of three sections: Research project overview; Article; and Reflection.

This mini-dissertation is the student's work. The student was responsible for the final concept, set up, execution of the research project and writing of the mini-dissertation. The supervisory team members contributed in an advisory and technical support capacity to the study's conception and design, analysis and interpretation of data, and critical revision of the manuscript. The mini-dissertation was language edited before submission for examination. However, the student is responsible for making these edits and for the grammatical correctness of the final document.

The primary study supervisor permitted the student to submit this mini-dissertation for examination.

ABSTRACT

Using a qualitative document analysis method, this research explored a unique area with actual risk work, in cyber risk reporting by South African banks listed on the JSE. The study used publicly available integrated reports, risk management reports, and corporate governance reports (collectively referred to as governance reports) from the top five JSE-listed banks, to address the research question: *How can South African banks and regulators enhance cyber risk reporting to better inform investors?* As a new research area, this question appeals to stakeholders of the banks and investors. Firstly, to address the research question, a literature review was conducted, analysing peer-reviewed academic literature, South African regulations, and SEC cyber risk reporting guidelines and regulations. This review informed the development of a thematic codebook containing themes and subthemes for cyber risk reporting information, useful for investor decision-making. The literature review highlighted gaps in South Africa's regulatory framework on cyber risk reporting. Secondly, the banks' governance reports were evaluated against these themes and subthemes to assess whether the information provided is beneficial for investor decision-making. The findings indicated that, while banks report some relevant cyber risk information, there are gaps in the completeness and comprehensiveness. As such, the study recommends that South Africa's regulators enhance regulatory requirements to mandate cyber risk incident reporting for investor decision-making and to provide more detailed guidance on information to be included in annual governance reports. It is also recommended that banks use these findings to evaluate and improve their reporting for greater transparency. Although this study has limitations, it offers valuable insights into the banking industry, regulators, and academics by providing guidance to the banks to improve their cyber risk reporting practices, suggesting improvements to the regulatory framework, and contributing to the body of knowledge on cyber risk reporting in a South African context.

Keywords: cyber risk, cyber threats, risk reporting, investor decision-making, South African banks

ACKNOWLEDGEMENTS

Thank you, God. You strengthened me and carried me through this process.

To my boys, your love and understanding have been my constant source of strength.
To my family and friends, who checked on me, rooted for me, prayed for me, and supported me from start to finish. I am grateful to have you all in my life.

To my supervisor Gloria, you pushed me to always do better. You were patient, and provided valuable feedback and direction. Thank you for your dedication to this process. To Wilna, assistant supervisor, thank you for your encouragement and guidance in this process.

Lastly, to the UARM team, thank you all for your valuable and diverse insights.

TABLE OF CONTENTS

PREFACE ..... **I**
ABSTRACT ..... **II**
ACKNOWLEDGEMENTS ..... **I**
TABLE OF CONTENTS ..... **IV**
LIST OF TABLES ..... **V**
LIST OF FIGURES ..... **V**
RESEARCH PROJECT OVERVIEW **1**
ARTICLE **3**
INTRODUCTION 3
BACKGROUND 4
METHOD 11
RESULTS AND DISCUSSION 14
CONCLUSION 23
REFERENCES 25
REFLECTION **28**
APPENDICES **30**

LIST OF TABLES

Table 1: Role players in the Exploring cyber risk reporting in South African banks study……. 2
Table 2: Summary of the documentary resources analysed to develop themes ……8
Table 3: Summarised thematic codebook of cyber risk reporting themes and subthemes…….....9
Table 4: Top five banks listed on the JSE……12
Table 5: The banks' governance reports documents reviewed for this study……12
Table 6: Evaluation criteria for evidence of cyber risk reporting……13
Table 7: Summary of findings: Alignment of incident reporting to the subthemes…….....14
Table 8: Cyber Risk Incident Reporting Findings…….....15
Table 9: Summary of findings: Alignment of cyber risk reporting to the subthemes……16
Table 10: Cyber Risk Reporting findings……...16
Table 11: Summary of findings: Alignment of governance to the subthemes…….....17
Table 12: Governance findings...…….....18
Table 13: Summary of findings: Alignment of Third-Party Reliance to the subtheme……19
Table 14: Third-Party Reliance findings……19
Table 15: Summary of findings: Reporting Format subthemes……20
Table 16: Reporting Format Findings……20

LIST OF FIGURES

Figure 1: Summary of the coding process for the thematic codebook……11
Figure 2: Diagram representation of the coding process followed for this study...……...13

RESEARCH PROJECT OVERVIEW

Digital transformation in banking has created new opportunities and driven innovation, however, it has also heightened cyber risks (Vasiliu-Feltes, 2024). As the cyber risk landscape expands, transparent and timely reporting is crucial for investors to make informed decisions and accurately assess an organisation's share price (Bhatia & Kaur, 2024; Chen *et al.*, 2022). This study explores cyber risk reporting by banks listed on the Johannesburg Stock Exchange (JSE), addressing the research question of how South African banks and regulators can enhance cyber risk reporting to better inform investor decision-making. Cyber risk reporting is part of actual risk work and is essential for effective risk management as it raises awareness of the risks that inform decision-making processes.

The paper is structured as follows: the abstract is an executive summary highlighting the key components of the research. The introduction contextualises the study and presents the research objectives. The background section highlights the crucial concepts from existing academic literature, and it outlines the requirements for cyber risk reporting in South African regulations and the US Securities and Exchange Commission (SEC), which is recognised as a leading example of international cyber risk reporting expectations that promote investor protection (Skinner, 2019). The thematic codebook of cyber risk reporting themes and subthemes emphasises the key reporting requirements described. The method section describes how the research was conducted and includes a document analysis of publicly available governance documents containing cyber risk reporting obtained from the bank's websites. The output is the second codebook, namely the banks' reporting codebook, containing key observations from the document analysis, a comprehensive view of the risk information disclosed by banks, and highlighting gaps in reporting. The results and discussion section summarises key findings, analyses their implications, assesses the extent to which bank statements align with identified themes and subthemes, and presents overarching conclusions. The conclusion highlights key outcomes, recommendations, the significance of the research, research limitations, and future research considerations. The references list key research and documents referred to in this study, and the reflection summarises what I have learnt as a researcher.

As a risk professional in the banking industry, I am interested in the topic of cyber risk, and there is a clear gap with regard to cyber risk incidents reported by banks, as this data is only reported to the local authorities and not to aid investor decision-making. Given that cyber risk is a growing concern, I was interested in exploring this gap and other aspects of cyber risk reporting to promote greater transparency for investors. Furthermore, there is a gap in the current literature on cyber risk incident reporting in South African banks. Therefore, the research contributes to the academic literature and

provides students and researchers with a unique perspective on cyber risk reporting in South Africa, enriching the existing body of knowledge.

The study also offers a comparative analysis of current reporting practices against international standards by analysing the SEC requirements. This allows banks and regulators to identify areas for improvement and ensure their practices are aligned with best practices globally. The study provides recommendations to improve the reporting requirements in cybersecurity laws and for banks to enhance their cyber reporting practices.

Additionally, this study allowed the researcher to learn how to do an applied research project to demonstrate mastery of research at the master's degree level within a research team context. The responsibilities of the different role players in this research project are described in Table 1.

Table 1. Role players in the 'Exploring cyber risk reporting in South African Banks' study.

#	Team member	Role
1	Researcher: Tlhokomelo Rikhotso	Documented the study literature review and conducted the study document analysis, including data collection, data analysis, and documenting results and key discussions and conclusions.
2	Supervisor: Gloria Nyamah Assistant Supervisor: Wilna Meiring	Provided supervision and guidance on the study.
3	Language Editor: Dr Wena Coetzee	Did a grammar-only edit of the dissertation before submission for examination.

References

Bhatia, A., & Kaur, A. (2024). The influence of information asymmetry on the interaction between voluntary corporate disclosure and cost of equity: evidence from publicly traded Indian enterprises. *International Journal of Law and Management*, *66*(1), 23-43. https://doi.org/10.1108/IJLMA-05-2023-0120

Chen, J., Henry, E., & Jiang, X. (2022). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, *187*(1), 199-224. https://doi.org/10.1007/s10551-022-05107-z

Skinner, C. P. (2019). Bank disclosures of cyber exposure. *Iowa L. Rev.*, *105*, 239. https://web-p-ebscohost-com.nwulib.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=0&sid=4933c4cd-fa6e-49c3-a25c-19a4def8b66c%40redis

Vasiliu-Feltes, I. (2024). Safeguarding financial resilience through digital trust and responsible innovation. *Journal of Risk Management in Financial Institutions*, *17*(2). https://doi.org/https://doi.org/10.69554/PWOV3485

ARTICLE

Exploring cyber risk reporting in South African banks

Introduction

The global financial services industry is experiencing a significant transformation with the integration of advanced technologies like artificial intelligence (AI), blockchain technologies, and automation (Vasiliu-Feltes, 2024). According to the World Economic Forum (2022), the use of advanced technologies is projected to increase substantially over the next two years, which is anticipated to impact cyber risk considerably. The growing adoption of advanced technologies presents heightened cyber risks, which could adversely affect organisations, lead to investment hesitation, and contribute to economic weaknesses (Vasiliu-Feltes, 2024).

Cyber risk is defined as “operational risk associated with the performance of activities in cyberspace that threaten information assets, information communications technology resources and technological assets, and may cause material damage to the tangible assets of an organisation, disrupt its operations or cause reputational harm” (Strupczewski, 2021, p. 6). According to Tosun (2021), the broader implications of cyber risk extend beyond the economic impact, negatively affecting individuals, organisations, and investors. Furthermore, cyber risk breaches can damage an organisation’s reputation, eroding investor confidence and potentially triggering a sell-off of the organisation's shares, which negatively impacts its share prices (Tosun, 2021). Thus, the need for transparent cyber risk reporting has become increasingly critical due to the rise in cyber breaches. Bhatia and Kaur (2024) state that comprehensive risk reporting gives investors the visibility to accurately assess the impact of a breach on the organisation and make informed investment decisions.

In line with this global trend, the South African banking sector has increasingly adopted advanced technologies such as automation, resulting in increased cyber risks and challenges to the security and stability of financial institutions (Uddin *et al*., 2020). The 2023 Annual Crime Statistics Report by the South African Banking Risk Information Centre (SABRIC) highlights this growing threat, reporting a 45 percent surge in digital banking fraud incidents in 2023, compared to only 24 percent in 2022 (SABRIC, 2023). Furthermore, financial losses from digital banking fraud surged by 47 percent in 2023, reaching ZAR 1 082 million, compared to a 68 percent increase in 2022. In addition, SABRIC raised concerns about the growing use of generative AI for fraudulent activities, highlighting the adaptability of cybercriminals to new technologies (SABRIC, 2023). To address the increasing concern of cyber risk, South Africa implemented a regulatory framework aimed at mitigating cyber risks. However, no regulatory requirement mandates the reporting of cyber risks to investors by

banks. Moreover, South Africa's cyber risk laws do not specify the type of cyber risk information that should be reported to address investor needs, nor prescribe a consistent reporting format. This lack of visibility and standardisation makes it challenging for investors to evaluate the potential financial and operational impact of cyber risks on banks, thereby hindering informed investment decisions.
Effective corporate governance depends on transparency as a crucial part of information sharing (IoDSA, 2016). Banks provide risk information to stakeholders in their annual reports (IoDSA, 2016; JSE, 2024). However, no literature was found to have explored cyber risk reporting to aid investor decision-making. It is, therefore, unclear whether such reports provide adequate information on a bank's cyber risk to investors. Thus, this study aimed to fill the gap in the literature and performed a document analysis with the following research question in mind: *How can South African banks and regulators enhance cyber risk reporting to better inform investors?* To answer this research question, the study employed a two-phased research approach. Firstly, South African regulatory documents related to cyber risk reporting and international regulatory documents from the SEC were thematically analysed to identify key themes and subthemes related to cyber risk reporting. Secondly, the integrated reports of the top five JSE-listed banks were evaluated for evidence of informative cyber risk reporting using these key themes and subthemes.

This study aimed to give new and valuable insights into an underexplored research area. Furthermore, the research approach and findings are valuable to the South African regulators and banks by highlighting potential improvements in cyber risk reporting, which would enhance transparency for better-informed investor decision-making.

Background

This section briefly discusses cyber risk reporting and key concepts from select academic literature to address the first research objective to explore cyber risk reporting requirements for South African banks listed on the JSE. Key regulatory documents, including the SEC cyber risk regulatory documents, the South African Reserve Bank's (SARB) directive on cybersecurity and cyber resilience within the national payments system, and the King IV Report on Corporate Governance, were analysed inductively to identify themes and subthemes and generated codes related to cyber risk reporting. These emerging themes and subthemes were then refined using a constant comparative approach (Boeije, 2002) to determine which cyber risk information should be included in the integrated reports of banks.

The importance of cyber risk reporting

Cyber risk is increasingly becoming a key risk for organisations in South Africa as it can cause severe financial, reputational, and legal damage (Gao *et al.*, 2020). This is echoed by the South African Risk

Report issued by the Institute of Risk Management South Africa (IRMSA), highlighting cyber risk as one of the top risks (IRMSA, 2024). As cyber breaches grow more frequent, transparent risk reporting is essential for investors to evaluate the potential impact of these incidents on a company's performance (Bhatia & Kaur, 2024; Gao *et al*., 2020). Effective risk reporting provides investors with the necessary visibility to assess the impact of cyber risk on an organisation, allows them to make informed investment decisions, and provides insight into how management is responding to these risks (Bhatia & Kaur, 2024). Underreporting cyber risk incidents limits investors' understanding of the evolving cyber risk landscape (Morgan, 2020). According to Bhatia and Kaur (2024); (Chen *et al*., 2022; Pieterse, 2021), organisations should implement effective reporting policies, as well as timely reporting, to reduce information asymmetry, increase the transparency of cyber risk, and enhance stock market liquidity. However, there is a counterargument that reporting too much information can increase exposure to additional risks, such as revealing vulnerabilities to potential attackers and exposing information that is still being investigated to the perpetrators (Egloff & Smeets, 2023).

Cyber risk reporting is viewed as an ethical responsibility, requiring companies to take appropriate actions and make ethical decisions to manage and mitigate the risk (Radu & Smaili, 2021; Smaili *et al.*, 2022). Reporting on cyber risk after a breach, demonstrates ethical corporate behaviour, while withholding such information raises doubts about the company's integrity and ethical conduct (Chen *et al*., 2022). Elshandidy *et al*. (2022) has shown that increasing the quantity of cyber risk reporting does not significantly impact an organisation's value. However, Chen *et al.* (2022) states that investors penalise organisations that reduce disclosures after a breach, regardless of its severity, as this raises concerns about the organisation's ethical conduct. Therefore, providing specific and verifiable cyber risk reports helps to build investor's trust (Bansal & Axelton, 2024; Smaili *et al*., 2022).

International standards on cyber risk reporting

The SEC is recognised as a leading example of international standards for cyber risk reporting that promote investor protection (Skinner, 2019). It first introduced comprehensive cyber risk reporting requirements in 2011, which were refined in 2018 (Gerding, 2023) and further updated in 2023 to enhance transparency and aid investors in making informed decisions (SEC, 2023). The SEC rules emphasise the need for specific, non-generic disclosures (Chen *et al.*, 2022). They require public organisations to report material cyber risk incidents timely within four business days (SEC, 2023). The SEC states that materiality refers to information that would significantly alter a reasonable investor's decision-making process (SEC, 1999), and organisations should perform a materiality assessment for cyber incidents (SEC, 2023). This approach to materiality has been criticised for being ambiguous (Lopez, 2023). Additionally, organisations are mandated to provide periodic cybersecurity risk management, strategy and governance practices (SEC, 2023). This ensures

timely and consistent information that investors can use to evaluate the potential impact of cyber risk incidents on an organisation (Gerding, 2023).

The SEC states that cyber risk disclosures should be submitted through the SEC's reporting system, making them easily accessible to investors and reducing search time and costs (SEC, 2023). Furthermore, the disclosures should be labelled using a specific labelling format called inline extensible business reporting language (inline XBRL), which enhances the usefulness and comparability of the data, making it more accessible for retrieval, comparison, filtering, and analysis against other companies and prior years. This standardised labelling format using inline XBRL helps to reduce information asymmetry by lowering information processing costs (SEC, 2023).

Cyber risk reporting obligations in South African legislation

South Africa has enacted legislation aimed at combating cyber risks. Key provisions include requirements for organisations to report cyber risk incidents to regulatory authorities and to incorporate cyber risk information into corporate governance reports. This section provides a brief overview of relevant legislation impacting South African organisations.

The Electronic Communications and Transactions Act 25 of 2002 governs unauthorised access, data interference, denial of service, and cybercrimes such as computer-related extortion and fraud. This act does not require the reporting of cyber risks (South African Government, 2002). In 2013, the Protection of Personal Information Act 4 of 2013 (POPIA) was established. POPIA requires organisations to implement appropriate measures to secure the integrity and confidentiality of personal information against loss, damage, or unauthorised access, including that due to cyber breaches. Additionally, POPIA mandates that data breaches be reported to the information regulator and affected parties as soon as reasonably possible, using a specified template that includes details of the breach, potential consequences, and remedial actions (Information Regulator, 2013, n.d.). However, there is no requirement to disclose these data breaches to investors. In 2020, the Cybercrimes Act 19 of 2020 was enacted, which is South Africa's primary legislation on cybercrime. It mandates financial institutions to report cyber risk incidents to the South African Police Services (SAPS) within 72 hours of detection, with no requirement to disclose these breaches to investors (South African Government, 2020).

South African organisations listed on the JSE must adhere to the JSE listing requirements, which mandate them to report any information that could directly or indirectly impact their share prices (JSE, 2024). Furthermore, the JSE states that organisations should provide detailed descriptions of material risks specific to the company, its industry, and its securities and avoid generic disclosures. Moreover, the JSE defines material information as "information that, if omitted or misstated, could

impact users' economic decisions" (JSE, 2024). Organisations are mandated to include this information in the organisation's annual reports, which are publicly available on their websites. South African-listed companies are also required to adhere to the King IV Report on Corporate Governance, which mandates publishing integrated annual reports that address critical issues affecting the organisation's ability to generate value (IoDSA, 2016). However, the King IV Report does not explicitly require reporting of cyber risk incidents (IoDSA, 2016). According to Du Toit *et al.* (2017), integrated reports that provide high-quality, relevant information, help investors and stakeholders make informed decisions.

Banks in South Africa are subject to specific regulations addressing risk reporting. The Prudential Authority (PA), a division of the SARB, issued Directive 2 of 2019, which requires banks to report material cyber risk incidents to the PA within one day of discovery. The report is submitted on a prescribed form and should detail the nature and scope of the incident, the type of threat (e.g., malware, data breach), and its financial and operational impact (SARB, 2019). In 2024, the PA enhanced its directives on cyber risk reporting and issued Directive 01 of 2024 on cybersecurity and cyber resilience within the national payments system. This directive mandates banks to establish and maintain adaptive cybersecurity frameworks, define governance roles, identify critical operations and assets, implement protective measures, and have detection, response, and recovery plans. Additionally, banks are required to report material cyber risk incidents to the PA within 24 hours and to submit a detailed report within 48 hours, which includes the incident type and nature, impact on services and stakeholders, recovery and remediation plan, and provides regular updates to the PA. The PA defined material cyber incidents as "a disruption of a business activity, process or function which has, or is likely to have, a severe and widespread impact on the financial institution's operations, services to its customers, or the broader financial system and economy" (SARB, 2024). However, there is no stipulated format or template for writing the report. While this ensures the regulator is informed of potential financial system risks, public reporting is not mandated, limiting investor awareness.

SARB Regulation 43(1) requires banks to report their risk profile and risk management practices (SARB, 2016). Furthermore, the Basel Committee on Banking Supervision (BCBS) Pillar 3 requires banks to enhance transparency by providing detailed reports on their operational risk profile (BCBS, 2023). The Financial Sector Conduct Authority (FSCA) and the PA issued a Joint Standard 2 of 2024, focusing broadly on cybersecurity and cyber resilience requirements for all financial institutions. This standard mandates reporting material cyber risk incidents to the authorities but does not stipulate a reporting format or timeline (FSCA & PA, 2024). While South African legislation addresses cyber risk reporting, there remain gaps in public disclosure for investor decision-making.

A thematic codebook of cyber risk reporting themes and subthemes for investors' information needs

In light of the limited cyber risk reporting requirements in South Africa, this study considered the SEC requirements to identify best practices that could enhance South Africa's cyber risk reporting. A thematic codebook was developed based on the review of various SEC cyber risk regulatory documents, South African Directive 01 of 2024, which sets comprehensive cyber risk requirements for banks, and the King IV Report on Corporate Governance. These documents were selected to highlight international best practices and South African regulatory requirements, with the aim of providing information useful for investor decision-making. The regulatory documents, summarised in Table 1, were analysed to identify key themes and subthemes for cyber risk reporting, which are detailed in the summarised thematic codebook in Table 2. The detailed thematic codebook has been included in the appendix.

Table 2: Summary of the key documentary resources analysed to develop themes.

Source	Published	Key outcomes
Institute of Directors	2016	The King IV Report on Corporate Governance outlines the principles and best practices for corporate governance in South Africa. These include reporting requirements for companies listed on the JSE (IoDSA, 2016).
SARB Directive 01 of 2024	2024	Directive 01 of 2024 on cybersecurity and cyber resilience within the national payments system issued by the PA outlines requirements for banks to establish robust cybersecurity frameworks and specifies reporting requirements for material cyber risk incidents (SARB, 2024).
U.S. SEC	2023	The SEC's *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* document outlines new rules adopted to enhance and standardise public companies' disclosures on cybersecurity risk management, strategy, governance, and incident reporting (SEC, 2023).
U.S. SEC	Amendments published in 2023	SEC Regulation S-K includes an amended item 106, which sets periodic cybersecurity risk reporting requirements. These requirements encompass disclosures on cybersecurity risk management, strategy, and governance practices (SEC, n.d.-a).
U.S. SEC	Amendments published in 2023	SEC Form 8-K Item 1.05 includes amended requirements for reporting material cybersecurity incidents, specifying the information and format needed for reporting these incidents (SEC, n.d.-b).

Table 3: Summarised thematic codebook of cyber risk reporting themes and subthemes.

Theme	Subtheme	Subtheme description	Codes	References
Cyber risk incident reporting	Material cyber incidents	Cyber risk incidents that are determined to be material are reported.	Material cyber risk incidents reported	(SEC, 2023)
	Incident details	Cyber risk incident disclosures should clearly describe the incident's nature, scope, timing, and detail the actual or potential impact on operations and finances.	Nature/Scope/Timing/Cyber risk incident impact	(SEC, 2023; SARB, 2024)
	Potential and past incidents	Report potential and past material cyber risk incidents. Revisit previous disclosure, including updates on related financial or legal issues.	Past incidents/Potential incidents/Updates	(SEC, 2023; SARB, 2024)
	Timeliness of incident reporting	Incidents are reported timely in line with regulatory requirements.	Timeliness	(SEC, 2023; SARB, 2024)
Cyber risk reporting	Cyber risk management process	Reports should thoroughly address the cyber risk management process, outlining the process for cyber risk identification, assessment and management. Explain how cybersecurity processes are incorporated into the organisation's broader risk management framework. Highlight the process to monitor the cyber risk management process. Additionally, the reports should cover the organisation's cybersecurity strategies.	Cyber risk identification/Cyber risk assessment/ Cyber risk management process/ Cybersecurity process integration/Cyber risk management process monitoring/Cybersecurity strategies	(IoDSA, 2016; SEC, n.d.-a)
	Material cyber risk impact	Indicates whether any risks from cyber risks have materially affected or are reasonably likely to materially affect the business strategy, operations, or financial condition.	Material impact/Business strategy impact/Operational impact/Financial impact	(SEC, 2023, n.d.-a, n.d.-b)

Theme	Subtheme	Subtheme description	Codes	References
Governance	Board of Directors (BOD) oversight	Identifies the board committee or subcommittee responsible for overseeing risks from cyber risks and how they are informed about such risks.	Board Committee/ Board of Directors/Oversight/BOD Risk communication	(IoDSA, 2016; SEC, 2023; n.d.-a).
	Management	Discloses the role of management in assessing, monitoring, and managing cybersecurity risks, including responsible roles or committees, their expertise, how they are informed about cyber risk incidents and cyber risks, and whether they report such information to the Board of Directors.	Management role/ Management position or committee/ Management's risk assessment role/Management's risk monitoring role/Relevant expertise / Management risk communication/ Board engagement	(SEC, 2023, n.d.-a)
Third-party reliance	Outsourced cybersecurity process	Discloses information on the organisation's reliance on third-party cybersecurity services and provides a view of in-house versus outsourced cybersecurity capacity. Describes the process for managing cyber risks associated with these external providers.	In-house risk management/Outsourced risk processes/Third-party cyber risk oversight	(SEC, 2023, n.d.-a)
Reporting format	Information access	Information should be easily accessible and published on a known website (e.g. company website) or prescribed platform.	Platform/Accessible	(IoDSA, 2016; SEC, 2023; n.d.-b).
	Templates	The incident report and annual report follow a specified template or format. Cyber risk reporting is placed in consistent sections of the organisation's reports (e.g. the risk management section of the Governance Report).	Standardised form/Templates/ Report section/Consistent placement	(SEC, 2023, n.d.-b)

Method

The first phase of the study involved developing a thematic codebook by analysing the SEC cyber risk regulatory documents, SARB Directive 1 of 2024, and the King IV Report on Corporate Governance. This codebook was designed to support the second study objective, which was to explore whether the current cyber risk reporting by the JSE-listed banks provides investors with the necessary information for effective decision-making. These requirements were categorised into broad themes, which captured overarching cyber risk reporting objectives. Each theme was further broken down into subthemes, representing specific components of cyber risk reporting within that theme, and codes, which are keywords derived from the subtheme description to capture the core elements of the subtheme. Together, these themes, subthemes, and codes provided a structured view of information required for investor decision-making. Five themes were defined. The cyber risk incident reporting theme focuses on the effective and timely reporting of cyber risk incidents that have materialised, including crucial information required for effective cyber risk incident reporting. The cyber risk reporting theme outlines the key cyber risk information for bank reports, including the risk management process and the impact of experienced risks. The governance theme describes the governance structure for cyber risk management, highlighting roles and responsibilities of the Board of Directors and management. The third-party reliance theme addresses the organisation's reliance on external cybersecurity services and its oversight of third-party-related cyber risks. Finally, the reporting format theme states that information should be accessible on a known website or platform, presented in a standard template or format, and within consistent report sections. Figure 1 is a diagrammatic representation of the coding process.

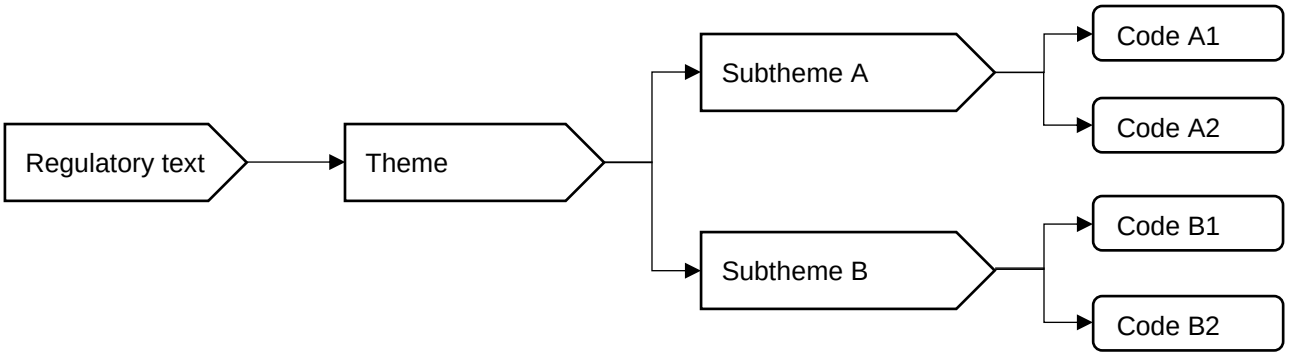

Figure 1: Summary of the coding process for the thematic codebook.

The second phase involved evaluating the governance reports of the top five JSE-listed banks for evidence of these themes and subthemes. Using document analysis as described by (Bhangu *et al.*, 2023; Bowen, 2009), cyber risk-related information was systematically extracted from the governance reports of banks. The research focused on the top five banks listed on the JSE, selected through purposeful sampling to ensure analysis of the most significant market participants (Patton, 2002). While six banks are listed on the JSE, Finbond Group Limited was excluded from the study,

given its minimal market impact, representing less than 1% of the total banking sector's market capitalisation. The selected banks represent 99% of the South African banking sector's market capitalisation, with a combined value exceeding ZAR1.5 trillion. This significant market coverage ensured a comprehensive view of cyber risk reporting practices across the sector. Details of the banks and their market capitalisation are presented in Table 4.

Table 4: Top five banks listed on the JSE.

Listed bank	Market capital (ZAR)
FirstRand Limited	461.10B
Standard Bank Group	404.55B
Capitec Bank Holdings	372.68B
Absa Group Limited	151.25B
Nedbank Group Limited	144.63B

(ListCorp, 2024)

The study analysed publicly available secondary data from the 2023/2024 annual integrated reports, corporate governance reports, or risk reports (collectively referred to as governance reports in this study) from the top five banks to extract information on cyber risks and material cyber risk incidents impacting the bank. Table 5 shows the reviewed reports from the listed banks.

Table 5: The banks' governance reports documents reviewed for this study.

Bank name	Reporting year	Governance reports reviewed
Absa Group Limited	December 2023	Integrated Report Pillar 3 Risk Management Report Financial Results Booklet Sustainability Report
Capitec Bank Holdings	February 2024	Annual Integrated Report
FirstRand Limited	June 2024	Basel Pillar 3 disclosure First Rand Corporate Governance Material risk factor disclosure in terms of paragraph 7.f.7 of the JSE listings requirements
Nedbank Group Limited	December 2023	Integrated Report Pillar 3 Risk and Capital Management Report Governance Report
Standard Bank Group	December 2023	Annual Integrated Report Risk and Capital Management Report Governance Report

Once the cyber risk statements from the banks' governance documents were extracted, a deductive content analysis approach was applied to categorise statements into themes and subthemes defined in the thematic codebook. This process allowed for the flexibility to assign multiple subthemes to an

individual statement, where appropriate. Deductive content analysis was useful for comparing predefined categories across different banks (Elo & Kyngäs, 2008). After coding, descriptive analysis was applied to identify patterns and trends in the data, allowing for a deeper understanding of recurring themes and reporting practices (Naeem *et al.*, 2023). This process resulted in the creation of a secondary codebook, namely the banks' reporting codebook, which provided a clear and comprehensive view of the risk information disclosed by the banks, and highlighted gaps between the predefined thematic codebook and the banks' actual reporting. The banks' reporting codebook also highlighted cyber risk disclosures that did not align with the codes from the thematic codebook. These new codes, identified from the statements of the banks, were reviewed and considered as part of the results and discussion section. The detailed banks' reporting codebook is provided in the appendices. Additionally, statements were evaluated for their alignment with each subtheme using three alignment categories that are summarised in Table 6. These alignments highlighted cyber risk reporting gaps.

Table 6: Evaluation criteria for evidence of cyber risk reporting.

Criterion	Evaluation	Key
The information provided by the bank is relevant to cyber risk reporting and can be linked to themes and subthemes to assess good cyber risk reporting, which aids investor decision-making.	Fully aligned	FA
The information provided by the bank is relevant to cyber risk reporting, and can be partially linked to themes and subthemes, to assess good cyber risk reporting which aids investor decision-making.	Partially aligned	PA
The information provided by the bank relate to cyber risk, however it cannot be adequately linked to the themes and subthemes.	Not aligned	NA

After the alignment was applied to each statement, the average alignment was determined per subtheme based on the most common alignment across all the banks. Figure 2 provides a summary of the coding process.

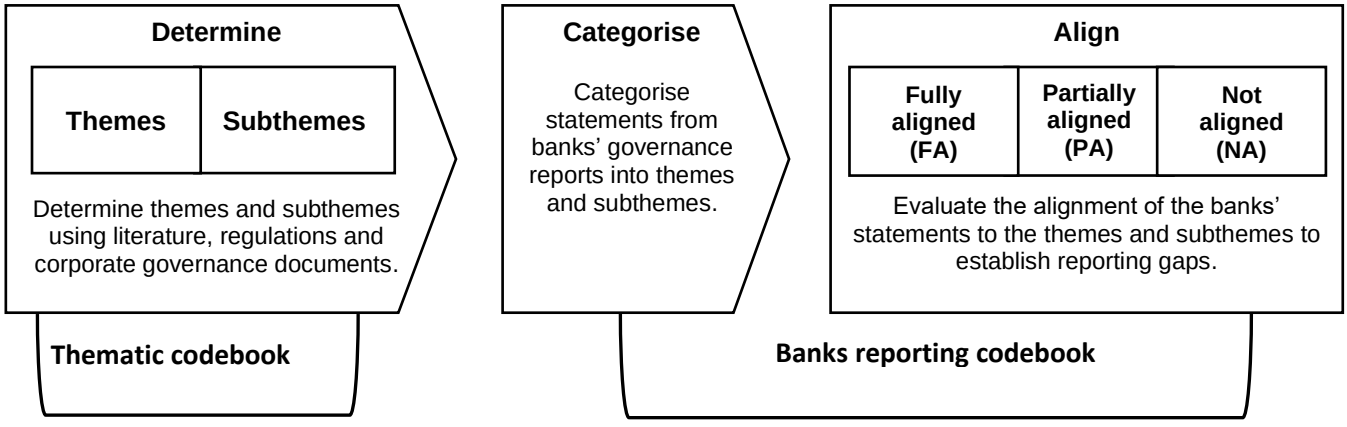

Figure 2: Diagram representation of the coding process followed for this study.

Results and discussion

This section explores cyber risk reporting practices found in the bank governance reports. To maintain confidentiality, the specific banks were not named in the discussion of findings, however, the banks and the list of analysed documents are included in Table 4 and 5, for reference.

Statements from the banks' governance reports were evaluated against the themes and subthemes from the thematic codebook and categorised as fully aligned (FA), partially aligned (PA) or not aligned (NA) to the subthemes. This evaluation indicated how well the banks' statements align with investor requirements and revealed gaps in the comprehensiveness and quality of banks' cyber risk reporting, which are discussed further in this section. This section is organised into five parts, corresponding to the five themes from the thematic codebook: cyber risk incident reporting, cyber risk reporting, governance, third-party reliance, and reporting format. Each main theme is analysed and the findings are presented in two ways. Firstly, a summary table displays the alignment of the banks' statements for each subtheme. Secondly, a detailed table provides the general findings for each theme and subtheme.

Cyber risk incident reporting

This section presents key observations for the cyber risk incident reporting theme, which focuses on the disclosure of material cyber risk incidents that have occurred, including the provision of essential information needed for transparency and timeliness. Among the themes assessed, cyber incident reporting was one of the least reported by banks. Overall, the statements made by banks to this theme were not aligned (NA). Although three banks provided minimal information aligning to the theme and subthemes, the details lacked necessary information to make the disclosure useful. Table 7 provides a summary of the findings from the analysis of the reports of every bank, as well as the average for all the banks in the study.

Table 7: Summary of findings – alignment of cyber risk incident reporting to the subthemes

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
Cyber risk incident reporting	Material cyber risk incidents	NA	FA	NA	FA	FA	**FA**
	Incident details	NA	NA	NA	NA	NA	**NA**
	Past and potential incidents	NA	NA	NA	NA	NA	**NA**

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
	Timeliness of incident reporting	NA	NA	NA	NA	NA	**NA**

Table 8 presents the research findings supported by quotes from bank reports.

Table 8: Cyber risk incident reporting findings.

Themes	Subthemes	Research findings	Quote from bank
Cyber risk incident reporting	Material cyber risk incidents	Overall, the banks moderately covered the reporting on material cyber risk incidents in 2023 / 2024. Three banks (Banks B, D, and E) made disclosures on their material cyber risk incidents, with Bank E disclosing that they reported two material cyber risk incidents, which were successfully managed, while the other two banks (Banks B and D) confirmed that they did not experience any material cyber risk incidents. The remaining two banks (Banks A and C) provided no commentary on this subtheme. Bank E provided no details on the incidents reported. It is worth noting that although Bank E reported two cyber risk incidents, they also expressed that there were no major successful breaches in its cyber defence, making reporting the two incidents unclear as to whom they were reported to and if the incidents occurred.	Despite increased digitisation and hybrid working, overall cyber risk remains within our appetite, with no material incidents reported.“ (Bank B, 2023) “For a second consecutive year, we recorded no severity 1 or 2 incidents; however, we remain highly vigilant, particularly as cyber threats increase globally.” (Bank D, 2023) “Two material cyber incidents were reported and successfully managed by the CCMT (Cybercrisis Management Team) in 2023.” (Bank E, 2023)
	Incident details	Banks provided no details on the incidents experienced.	None found
	Potential and past incidents	Banks did not update on historical incidents or discuss potential incidents.	None found
	Timeliness of incident reporting	Bank E reported two incidents in their governance report, however, provided no indication of the timing of the incidents.	None found

Summary of findings

Overall, banks included minimal information on material cyber risk incidents. Although three of the five banks included statements on cyber risk incidents (Bank B, D and E), with one bank, confirming that they reported two incidents (Bank E), there were no details of the incident such as nature, scope, or impact, to provide investors with the transparency required to assess the risk and make informed decisions. Furthermore, Bank E disclosed the cyber risk incidents in its annual report without indicating when the incident occurred, making it difficult to assess whether this disclosure is timely and, therefore, useful for investor decision-making.

Cyber risk reporting

This section presents key observations for the cyber risk reporting theme, which broadly outlines the key cyber risk information for banks' governance reports, including the risk management process, and the impact of experienced risks. The banks reported the cyber risk reporting theme the most, and the overall alignment was partially aligned (PA), as banks provided some details mainly on their cyber risk management processes, and limited information on material cyber risk impact.

Table 9 provides a summary of the findings from the analysis of the bank's reports per bank as well as the average for all the banks in the study.

Table 9: Summary of findings – alignment of cyber risk reporting to the subthemes.

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
Cyber risk reporting	Cyber risk management process	PA	PA	PA	PA	PA	PA
	Material cyber risk impact	NA	NA	NA	PA	NA	NA

Table 10 presents the research findings supported by quotes from bank reports.

Table 10: Cyber risk reporting findings.

Themes	Subthemes	Research findings	Quote from bank
Cyber risk reporting	Cyber risk management process	Banks reported on several aspects of their cyber risk management processes; therefore, this subtheme had the most aligned statements. However, the overall alignment is PA, as the information provided lacks the depth needed for full alignment. Notably, Bank D achieved a FA as its statements addressed most of the key requirements for this subtheme. All banks included information on risk management processes, cyber risk identification, cyber risk management strategies and broader operational risk management integration. Some banks mentioned their cyber risk appetite, noting that they were operating within it or that a cyber risk appetite had been established. These statements on appetite, while informative, do not align with investor-focused reporting needs	"Improved cyber risk management by embedding the cyber-security risk management framework, formulating a cyber risk appetite statement and reviewing the governance structures (Bank A, 2024). "Cyber incidents are managed through mature existing processes, continuously tested and improved." (Bank E, 2023) "Our information and cybersecurity strategy is based on ISO 27001/2 and the best-practice principles of the ISF Standard of Good Practice" (Bank C, 2024)

Themes	Subthemes	Research findings	Quote from bank
		and they had no code aligned. The King IV Report on Corporate Governance, however, encourages banks to report instances where a certain risk breached their tolerance levels. The banks did not include such statements for cyber.	
	Material cyber risk impact	This subtheme was minimally aligned in the banks' statements, with only one of the five banks (Bank D) providing information on the financial and operational impacts of material cyber risk. Due to the limited statements aligned with this subtheme, the overall alignment is rated as NA. Statements addressing other significant impacts, including material impacts on business strategy and operational and financial consequences, are absent.	"Possible business model impacts and effects on capitals – decreases financial loss as a result of potential fraud, cybercrime and data loss." (Bank D, 2023)

Summary of findings

All banks provided varied details on their cyber risk management processes, partially covering all codes under this subtheme. There was a noticeable gap in the lack of information on material cyber risk impact, lacking details on potential impacts on business strategy, operations, and finances.

Governance

This section presents key observations for the governance theme, broadly describing the governance structures for cyber risk management and highlighting the roles and responsibilities of the Board of Directors and management. The overall alignment to this theme was partially aligned (PA). Table 11 summarises the findings from the analysis of the bank's reports per bank as well as the average for all the banks in the study.

Table 11: Summary of findings – alignment of governance to the subthemes.

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
Governance	Board of Directors (BOD) oversight	FA	FA	PA	PA	PA	PA
	Management	NA	NA	PA	NA	PA	NA

Table 12 presents the research findings supported by quotes from bank reports.

Table 12: Governance findings.

Themes	Subthemes	Research findings	Quote from bank
Governance	Board of Directors (BOD) Oversight	Banks A and B provided statements that fully aligned (FA) with this subtheme, as they highlighted board committees or subcommittees responsible for cyber risk, board oversight activities related to cyber risk, and communication measures to keep the board informed about cyber risk escalations. Banks C, D, and E provided partially aligned (PA) statements on these similar areas. Additionally, banks included statements that addressed board-level expertise in cybersecurity. However, it is worth noting that no code aligned to board experience was included, as the SEC does not consider it essential for investor decision-making.	"The group information technology committee focuses on key activities to protect value, including managing technology risk, information security, and cybersecurity. The committee held 4 meetings during the year and achieved a participation rate of 97%." (Bank B, 2023) "Risk and capital management committee (board subcommittee) – Focus areas for 2024/2025 – IT and cybersecurity risk (including system stability and resilience)," (Bank C, 2024) "An advanced cyber management information system has been embedded to produce metrics that inform the board and management when cyber risk increases outside of the risk appetite." (Bank E, 2023)
	Management	Management was among the lowest reported subsegments, as banks poorly disclosed management oversight. Banks A, B, and D provided no information on management positions, risk assessments, monitoring, expertise, or communication. Bank C partially addressed management positions, monitoring, and communication. Bank E only partially disclosed management roles. The overall alignment for this sub-segment is NA due to the overall lack of disclosure from all banks.	"Weekly group EXCO meetings - where IT is represented by the chief information officer, and formal IT prioritisation meetings provide platforms to discuss strategic information and cybersecurity matters and initiatives, emerging risks and the alignment of IT risk management priorities." (Bank C, 2024)

Summary of findings

The BOD demonstrated a strong alignment with cyber risk oversight compared to management. Banks A and B provided comprehensive disclosures on board oversight activities. However, overall, governance reports lacked sufficient detail to meet the subtheme's requirements fully. While some banks mentioned board level cyber risk expertise, this topic is not explicitly required for investor decision-making as noted by the SEC (SEC, 2023). Regarding management oversight, all banks provided limited or no information on management roles, risk assessments, monitoring, expertise,

or communication. This highlights a significant gap in disclosing management's role in cyber risk management.

Third-party reliance

This section presents key observations for the third-party reliance theme, which requires organisations to describe their reliance on third-party cyber risk security services and the management of cyber risk linked to third parties. The overall alignment for this theme was partially aligned (PA). Table 13 provides a summary of the findings from the analysis of the bank's reports, per bank, as well as the average for all the banks in the study.

Table 13: Summary of findings – alignment of third-party reliance to the subtheme

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
Third-party reliance	Outsourced cybersecurity process	PA	PA	PA	NA	FA	PA

Table 14 presents the research findings supported by quotes from bank reports.

Table 14: Third-party reliance findings

Themes	Subthemes	Research findings	Quote from bank
Third-party reliance	Outsourced cybersecurity process	Statements from banks partially aligned (PA) with this subtheme. Bank A disclosed information on both in-house and outsourced cyber risk management processes but excluded third-party oversight. Bank B focused on outsourced risk processes and third-party oversight, but did not highlight in-house services. Bank C included a partially aligned statement on outsourced risk processes in place, while Bank D only reported minimum information on third-party oversight. Bank E, however, fully aligned with the subtheme, providing comprehensive details on in-house risk management and outsourced risk processes. Overall, banks aligned partially to the subtheme. It is worth noting that banks (A, B, and E) included details on their cyber risk insurance policies, with all of them opting to have insurance with external companies rather than in-house.	"The bank has a cyber and privacy due-diligence process in place for third-parties that includes a risk assessment, integrity checks, contracts containing the required cyber and privacy clauses, as well as assurance that the cyber controls are implemented on a risk-based approach." (Bank E, 2023) "We placed considerable emphasis in 2023 on managing our third-parties as cyber and information risks were trending across the industry. We adopted threat profiling, dark-web risk mitigation strategies and assessed operational readiness of critical third parties to mitigate cyber threats and information risks that may emerge." (Bank B, 2023) "Uncertainty over the cyber-security posture of the group's key vendors remains an area of concern, however the use of cyber-security ratings from an external cyber-security rating agency provide some assurance in this regard" (Bank A, 2024).

Summary of findings

Banks included statements on outsourced cyber risk processes, primarily focusing on third-party cyber risk oversight statements. Insurance was mentioned by Banks A, B and E and has been identified as a missing code in our analysis. The SEC is silent on the inclusion of this information; however, it contributes to a comprehensive view of cyber risks and the measures the organisation has implemented to manage and mitigate these risks.

Reporting format

This section presents key observations for the reporting format theme, which states that cyber risk information in organisational governance documents should be easily accessible, published on a known website or platform, and presented in a standard template. The researcher assessed the reporting format theme by evaluating the ease of locating the reports analysed. The ease of locating cyber risk-related statements within the report was considered to assess the template's subtheme. These two indicators were used to check how the bank's reports aligned with the reporting format theme requirements. The reporting format theme had an overall alignment of partially aligned (PA), which is the average of the alignment of the subthemes. Table 15 provides a summary of the findings from the analysis of the bank's reports per bank as well as the average for all the banks surveyed in the study.

Table 15: Summary of findings – reporting format subthemes

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for all banks
Reporting format	Information access	FA	FA	FA	FA	FA	FA
	Templates	NA	NA	FA	NA	NA	NA

Table 16 presents the research findings supported by quotes from bank reports.

Table 16: Reporting format findings.

Themes	Subthemes	Research findings	Quote from bank
Reporting format	Information access	Governance reports for all banks were readily accessible and downloaded from their respective websites.	"All the reports listed are available at https://www.*Company website*/investor-relations/." (Bank D, 2023) " Integrated Report - These reports are available on our website at *company website*.co.za" (Bank E, 2023)

Themes	Subthemes	Research findings	Quote from bank
	Templates	There is no prescribed template or format for regulatory reports or for presenting cyber risk information. However, cyber risk information was accessible through a keyword search for "cyber" in the governance reports. Banks published multiple, varied governance reports, making it difficult to determine which contained cyber risk information. All available reports for each bank were reviewed, but the lack of consistency resulted in an average alignment of not aligned (NA) for this theme. Bank C was the only fully aligned (FA) bank in the template's subtheme, as it produced a single integrated annual report, which contained all relevant cyber risk information.	

Summary

The reports were all easily accessible from the banks' websites. The information in their governance documents was generally accessible, as relevant cyber risk statements could be located with a keyword search. However, there was inconsistency in report formats and types across banks. All banks provided multiple reports containing cyber risk information, though they varied in format and type. Banks D and E issued both integrated and governance reports, while Bank C offered a single annual integrated report, consolidating all relevant information. Banks A, D, and E all had Pillar 3 Reports, while Bank A issued a material risk factor disclosure report, Bank B issued a Risk and Capital Management Report and Bank D also issued a Sustainability Report containing cyber risk information. All these reports contained statements on cyber risk. This inconsistency in reporting formats, with cyber risk information dispersed across multiple documents, makes identifying and analysing cyber risk information and comparing across the banks challenging and time-consuming. A consistent approach across the banks with a unified source for cyber risk information would enhance comparability and accessibility.

Summary results and discussion

The analysis of banks' governance reports revealed that while there were some statements supporting investor decision-making, significant gaps remain. The study applied five themes, aligned to the themes from the thematic codebook, cyber risk incident reporting, cyber risk reporting, governance, third-party reliance, and reporting format. Four themes showed partial alignment (PA), indicating valuable information was provided for investors, however, there was a general lack of

depth of information provided across the themes. One theme (cyber incidents reporting) had no alignment (NA), due to the minimal or no information across all the banks. Within the cyber risk incidents reporting theme, banks provided limited information on material cyber risk incidents, often lacking the details such as the nature, scope, impact, or timing of the incident. This could be due to the absence of regulatory requirements mandating cyber risk incident disclosures for investor decision-making, contributing to this reporting gap. Regulatory guidance mandating prompt and standardised incident disclosures published on the bank's website, or any other suitable platform would improve transparency. Additionally, there is no definitive framework for assessing materiality with both the SEC and South African regulators directing banks to make this determination and providing only broad guidelines. This ambiguity can result in inconsistent reporting of cyber incidents among banks, as they may apply different standards. Additionally, for the cyber risk reporting theme, disclosures on the material impact on business strategy, operations, and finances were minimal. This indicates a lack of guidance and clarity on information needed by investors. Therefore, establishing regulatory guidelines addressing these gaps could provide clear expectations for cyber risk information disclosure.

Banks should enhance their reporting on various aspects of their cyber risk management process, such as cyber risk identification, assessment, and their process to monitor the cyber risk management process. Furthermore, banks should provide more details on how cyber risk is integrated into the banks' broader risk management processes and systems. Lastly, banks should provide details of lessons learnt and the material impact of cyber risk on their operations, finances and business strategy, as this information was omitted by most banks. Regarding the governance theme, banks lacked details on board-level information. They should enhance the details provided on the board's process for oversight of cyber risk and the process to ensure the board is aware of the banks' cyber risk and any material cyber incidents experienced. Information on management's role in cyber risk management was notably underreported. Similarly, clear regulatory guidance is needed on governance-related disclosures that banks should incorporate in their annual governance reports to enhance reporting completeness. On the third-party reliance theme, banks reported outsourced cyber risk processes, mainly in monitoring third-party relationships and cyber risk insurance, but with limited consistency. Regulatory guidance should be enhanced to aid banks provide a more comprehensive view. Lastly, the reporting format theme lacked standardisation in reporting formats and templates, which hindered consistency and comparability. Recommended solutions include structured guidance on the report's format, specifying which is the main report that contains this cyber risk information while other reports cross-reference it.

Statements from the banks revealed "new codes" that emerged beyond the initial literature review. Banks A, B, and E revealed codes that included board training, experience, and expertise, all of which aligned with King IV's disclosure standards. However, the SEC does not consider this

information necessary for investor decision-making. Banks C and E highlighted the importance of management and employee training, reporting on in-house cyber risk training programmes. While the SEC does not require this information, it demonstrates a proactive approach to cyber risk management. Additionally, Bank D disclosed engagement with industry experts to stay updated on cyber risk trends. While the SEC is silent on the need for this information, including this detail demonstrates the bank's commitment to keeping pace with emerging risks. Furthermore, Banks B, D, and E reported on investments in cybersecurity. Similarly, the SEC does not mandate that this disclosure be made. However, it reflects the banks' commitment to strengthening cyber resilience and providing a view into the banks' future planning. Moreover, all banks emphasised cyber risk as a key concern and future focus area. Banks B and D even identified opportunities arising from cyber risk. Banks A, B, and E discussed cyber risk appetite, although this may not directly align with investor-focused reporting. Bank E also shared valuable lessons learnt from past cyber incidents. Lastly, as mentioned by Banks A, B, and E, insurance offers additional transparency on risk management practices. While not explicitly required by the SEC, this information might be beneficial to investors. No codes were identified for these disclosures in the thematic codebook, indicating that the information reported by the banks has not been explicitly designated as necessary for investor decision-making. These emerging codes warrant further review and assessment, as they may offer additional value to investors and deserve regulatory consideration.

Conclusion

This study used document analysis to assess cyber risk reporting practices in South African banks, aiming to provide recommendations to enhance reporting standards. The research addressed the following question: *How can South African banks and regulators enhance cyber risk reporting to better inform investor decision-making?* While this is a new research area, it appeals to the banking sector, regulators, and academics, and contributes to the literature on South African cyber risk reporting.

The study analysed how cyber-risk-related statements made by the top five JSE-listed banks, in their governance reports, aligned to themes and subthemes determined as part of the literature review. The research findings revealed that cyber-risk-related statements by the banks, partially aligned (PA) to the themes, except for the incident reporting theme, which was not aligned (NA). This indicated that banks are providing cyber risk information that is considered relevant and needed to aid investor decision-making, however, gaps remain in comprehensiveness.

To address the third study objective of making recommendations to enhance cyber risk reporting in South African listed banks, the following suggestions are proposed: regulatory bodies should strengthen cyber risk reporting requirements in two key areas. Firstly, regulations should mandate timely disclosure of material cyber incidents to investors, including specific guidance on required

information such as incident nature, scope, timing, and impact, as well as updates on past incidents. Additionally, regulators should consider offering clearer guidance on materiality determinations to promote consistency in reporting across banks. Secondly, they should establish clear guidance for comprehensive governance disclosures covering board oversight, the role of management, risk management processes, and third-party oversight. These enhanced requirements would improve the completeness and consistency of cyber risk reporting in annual governance reports. Banks should strengthen their cyber risk reporting in several areas. Firstly, they should introduce new reporting elements that were not previously reported on, such as the material impact of cyber risk on business strategy, operations, and finances. Banks should also start reporting on management's cyber risk oversight responsibilities, expertise, and their reporting to the board. Secondly, banks should strengthen existing disclosures on the cyber risk management process, with more comprehensive reporting on risk identification, assessment, and monitoring. They should better articulate cyber risk integration into the broader risk management framework and enhance cybersecurity strategy reporting. Additionally, they should improve governance-related disclosures, providing greater detail on the board's cyber risk oversight process and enhanced reporting on third-party cybersecurity processes, distinguishing between in-house and outsourced approaches. Lastly, to improve accessibility, banks should consolidate all cyber risk information into a single report with appropriate cross-referencing in other reports.

This study's limitations include a focused population of the top five banks. This was done to ensure a manageable research scope within the allocated time. Furthermore, the documents reviewed for this research were limited to bank governance documents and excluded other potential information sources, such as media reports. This reliance on the banks' accuracy and completeness of their governance reports creates a risk of missing relevant risk information. Lastly, the potential subjectivity of the researcher when evaluating the statements for alignment to the subthemes was another limitation; to mitigate bias, close collaboration with the supervisor was maintained. Future research could consider expanding the scope to include organisations listed on the JSE that operate in other industries. Moreover, the study could be expanded to evaluate a broader document scope that includes media coverage and other independent sources. Lastly, research exploring changes in cyber risk reporting over time, comparing reporting across banks, and analysing practices in other countries with similar regulatory frameworks, could also be beneficial.

Despite its limitations, this study provides a foundation for understanding the current state of cyber risk reporting in South African banks and highlights areas for improvement, offering a valuable basis for future research on this critical topic.

References

ABSA Group Limited. (2023). *Integrated Report*. https://www.absa.africa/wp-content/uploads/2024/04/Absa-Group-Limited-Integrated-Report.pdf

Bansal, G., & Axelton, Z. (2024). Impact of Cybersecurity Disclosures on Stakeholder Intentions. *Journal of Computer Information Systems*, *64*(1), 78. https://doi.org/10.1080/08874417.2023.2180785

BCBS (Basel Committee on Banking Supervision). (2023). DIS Disclosure requirements DIS60 Operational risk. Retrieved 10 Sepetember 2024, from https://www.bis.org/basel_framework/chapter/DIS/60.htm

Bhangu, S., Provost, F., & Caduff, C. (2023). Introduction to qualitative research methods–Part I. *Perspectives in Clinical Research*, *14*(1). https://doi.org/10.4103/picr.picr_253_22

Bhatia, A., & Kaur, A. (2024). The influence of information asymmetry on the interaction between voluntary corporate disclosure and cost of equity: evidence from publicly traded Indian enterprises. *International Journal of Law and Management*, *66*(1), 23-43. https://doi.org/10.1108/IJLMA-05-2023-0120

Boeije, H. (2002). A purposeful approach to the constant comparative method in the analysis of qualitative interviews. *Quality and Quantity*, *36*. https://doi.org/info:doi/10.1023/A:1020909529486

Bowen, G. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2). https://doi.org/10.3316/QRJ0902027

Capitec Bank Holdings. (2024). *Annual integrated report*. https://www.capitecbank.co.za/globalassets/pages/investor-relations/financial-results/2024/annual-report/integrated_annual_report_2024.pdf

Chen, J., Henry, E., & Jiang, X. (2022). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, *187*(1), 199-224. https://doi.org/10.1007/s10551-022-05107-z

Du Toit, E., Van Zyl, R., & Schütte, G. (2017). Integrated reporting by South African companies: a case study. *Meditari Accountancy Research*, *25*(4). https://doi.org/doi/10.1108/MEDAR-03-2016-0052

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, *46*(3), 502-533. https://doi.org/10.1080/01402390.2021.1895117

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1). https://doi.org/info:doi/10.1111/j.1365-2648.2007.04569.x

Elshandidy, T., Elmassri, M., & Elsayed, M. (2022). Integrated reporting, textual risk disclosure and market value. *Corporate Governance*, *22*(1). https://doi.org/info:doi/10.1108/CG-01-2021-0002

First Rand Limited. (2024). *First Rand Basel Pillar 3 disclosure*. https://www.firstrand.co.za/media/investors/basel-pillar-3-disclosure/firstrand-basel-pillar-3-disclosure-june-2024.pdf

FSCA (Financial Sector Conduct Authority), & PA (Prudential Authority). (2024). *Cybersecurity and Cyber Resilience Requirements*. South African Reserve Bank Website: South African Reserve Bank Retrieved from https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2024/Joint-Communication-2-of-2024-Publication-of-the-Joint-Standard-Cybersecurity-and-cyber-resilience

Gao, L., Calderon, T. G., & Tang, F. B. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

Gerding, E. (2023). *Cybersecurity Disclosure* U.S. Securities and Exchange Commission. Retrieved February 25 from https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

Information Regulator. (2013). *Protection of Personal Information Act (4 of 2013)*. Government Gazette, 37067 Retrieved from https://www.gov.za/documents/protection-personal-information-act

Information Regulator. (n.d.). Guidelines completing section 22 security compromise notification form. https://inforegulator.org.za/wp-content/uploads/2020/07/Guidelines-on-completing-a-Security-Compromise-Notification-ito-Section-22-POPIA.pdf
IoDSA (Institute of Directors Southern Africa). (2016). *King IV Report on Corporate Governance in South Africa*. Intitude of Directors. https://www.iodsa.co.za/page/KingIVIPpolicy#:~:text=When%20quoting%20any%20text%20directly,reference%20above%20must%20be%20used.&text=IoDSA%20sees%20the%20infringement%20of,marks%20in%20a%20serious%20light.
IRMSA (The Institute of Risk Management South Africa). (2024). Risk Report. Retrieved 01 November 2024, from https://www.irmsa.org.za/page/IRMSARiskReport2024
JSE (Johannesburg Stock Exchange). (2024). JSE Limited Listings Requirements. https://www.jse.co.za/sites/default/files/media/documents/2019-04/JSE%20Listings%20Requirements.pdf
ListCorp. (2024). *Johannesburg Stock Exchange Banks*. Retrieved 10 October from https://www.listcorp.com/jse/sectors/financials/banks
Lopez, L. (2023). The Road to the Rules: The SEC Mandates Cybersecurity Disclosures. *Temple Law Review*, *96*. https://heinonline-org.nwulib.idm.oclc.org/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/temple96&men_hide=false&men_tab=toc&kind=&page=65
Morgan, G. (2020). A Care-Based Stakeholder Approach to Ethics of Cybersecurity in Business. *The Ethics of Cybersecurity*, *21*. https://doi.org/info:doi/10.1007/978-3-030-29053-5_6
Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231205789
Nedbank Group Limited. (2023). *Governance Report*. https://www.nedbank.co.za/content/dam/nedbank/site-assets/AboutUs/Information%20Hub/Integrated%20Report/2024/2023%20Nedbank%20Group%20Governance%20Report__pdf.pdf
Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative Social Work*, *1*(3). https://doi.org/info:doi/10.1177/1473325002001003636
Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, *28*, 1-21. https://doi.org/10.23962/10539/32213
Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of Business Ethics*, *177*(2). https://doi.org/info:doi/10.1007/s10551-020-04717-9
SABRIC (South African Banking Risk Information Centre). (2023). South African Banking Risk Information Centre 2023 Annual Crime Statistics. https://www.sabric.co.za/media/vjyn5f4d/sabric-annual-crime-stats-2023-2.pdf
SEC (US Securities and Exchange Commission). (1999). *SEC Staff Accounting Bulletin: No. 99 – Materiality*. Retrieved from https://www.sec.gov/interps/account/sab99.htm
SEC (US Securities and Exchange Commission). (2023). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. US Securities and Exchange Commission Retrieved from https://www.sec.gov/files/rules/final/2023/33-11216.pdf
SEC (US Securities and Exchange Commission). (n.d.-a). *Commodity and Securities Exchanges - Regulation S-K Item 106 Cybersecurity*. U.S. Securities and Exchange Commission Retrieved from https://www.sec.gov/about/divisions-offices/division-corporation-finance/rules-regulations-schedules
SEC (US Securities and Exchange Commission). (n.d.-b). *Form 8-K Current Report - Pursuant to Section 13 OR 15(d) of The Securities Exchange Act of 1934*. U.S. Securities and Exchange Commission Website: U.S. Securities and Exchange Commission Website Retrieved from https://www.sec.gov/files/form8-k.pdf
Skinner, C. P. (2019). Bank disclosures of cyber exposure. *Iowa L. Rev.*, *105*, 239. https://web-p-ebscohost-com.nwulib.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=0&sid=4933c4cd-fa6e-49c3-a25c-19a4def8b66c%40redis
Smaili, N., Radu, C., & Khalili, A. (2022). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance*, *27*(4), 1049. https://doi.org/10.1007/s10997-022-09637-6

South African Government. (2002). *Electronic Communications and Transactions Act (25 of 2002)*. Government Gazette, 23708 Retrieved from https://www.gov.za/documents/electronic-communications-and-transactions-act
South African Government. (2020). *Cybercrimes Act (19 of 2020)*. Government Gazette, 44651 Retrieved from https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf
South African Reserve Bank. (2016). *Banks Act, 1990 (Act No. 94 OF 1990) Amendment of Regulations*. South African Reserve Bank Retrieved from https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-regulations/2016/7306
South African Reserve Bank. (2019). *Reporting of material information technology and/or cyber incidents*. South African Reserve Bank Retrieved from https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2019/9487
South African Reserve Bank. (2024). *Directive in respect of cyber security and cyber-resilience within the national payment system*. South African Reserve Bank Retrieved from https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Directive%20in%20respect%20of%20cybersecurity%20and%20cyber-resilisnce%20within%20the%20national%20payment%20system.pdf
Standard Bank Group. (2023). *Annual integrated report*. https://www.standardbank.com/static_file/StandardBankGroup/filedownloads/RTS/2023/SBG_AnnualIntegratedReport2023.pdf
Strupczewski, G. (2021). Defining cyber risk. *Safety science*, *135*, 6. https://doi.org/10.1016/j.ssci.2020.105143
Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*. https://doi.org/10.1016/j.irfa.2021.101795
Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability a synthesis of literature. *Risk Management*, *22*(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2
Vasiliu-Feltes, I. (2024). Safeguarding financial resilience through digital trust and responsible innovation. *Journal of Risk Management in Financial Institutions*, *17*(2). https://doi.org/https://doi.org/10.69554/PWOV3485
World Economic Forum. (2022). Global Cybersecurity Outlook 2022 - Insight Report. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

REFLECTION

My journey in this master's course began with various application-based assignments on diverse topics during the first year using various research methods. I decided that my mini dissertation would be a document analysis. The next question was finding a topic I was interested in and defining what I wanted to achieve. Cyber risk quickly captured my interest as it is a growing threat in the banking sector. As a risk professional in a bank, I recognise cyber risk as one of the critical areas we need to address. Choosing this topic allowed me to deepen my understanding of cyber risk in my industry, and exploring its reporting aspects was relevant.

My study's objective was to explore cyber risk reporting in South Africa to support investor decision-making and offer recommendations to banks and regulators on enhancing this reporting. A challenge of this study was obtaining information on cyber risk incidents, which banks are not required to report to the public. This meant there was limited information although exploring reporting for general cyber risk revealed interesting insights. Creating the thematic codebook of cyber risk reporting themes and subthemes and the banks' reporting codebook was a valuable learning experience and the most enjoyable part of the project, especially because I love working with spreadsheets. Organising and refining the codebooks required multiple iterations, and each review led to improvements. The coding process was rewarding, and I plan to incorporate a similar approach in my work.

One of my personal goals in joining this programme was to improve my writing skills. Analysing the codebooks taught me how concise statements can sometimes convey more meaning than lengthy ones. I believe that identifying key concepts (or codes) before writing can make my professional writing clearer and more impactful. Reflecting on this journey, I am grateful for the challenge of completing a mini dissertation while balancing work and life. I believe I have met my personal objectives, improving my writing, expanding my knowledge of operational risk management, and keeping my analytical skills sharp. These skills will continue to be developed as an ongoing journey, and this master's programme has been an excellent learning curve.

The dashboard on the following page presents a comprehensive overview of the study, highlighting its key findings and recommendations for both regulators and banks.

Exploring cyber risk reporting in South African banks

Research question: How can South African banks and regulators enhance cyber risk reporting to better inform investors?

Method

- Document analysis
- Analysed integrated reports, corporate governance and risk reports for the top 5 JSE-listed banks

Summary of Results table - indicates an overview of findings from the analysis of the bank's reports

Themes	Subthemes	Bank A	Bank B	Bank C	Bank D	Bank E	Average for subtheme	Average for theme
Cyber incident reporting								NA
	Material cyber incidents	NA	FA	NA	FA	FA	**FA**	
	Incident details	NA	NA	NA	NA	NA	**NA**	
	Potential and past incidents	NA	NA	NA	NA	NA	**NA**	
	Timeliness of incident reporting	NA	NA	NA	NA	NA	**NA**	
Cyber risk reporting								PA
	Cyber risk management process	PA	PA	PA	FA	PA	**PA**	
	Material cyber risk impact	NA	NA	NA	PA	NA	**NA**	
Governance								PA
	Board of Directors (BOD) oversight	FA	FA	PA	PA	PA	**PA**	
	Management	NA	NA	NA	NA	NA	**NA**	
Third-party reliance								PA
	Outsourced cybersecurity process	PA	PA	PA	NA	FA	**PA**	
Reporting Format								PA
	Information access	FA	FA	FA	FA	FA	**FA**	
	Templates	NA	NA	NA	NA	NA	**NA**	

Key findings:

1. Gaps identified in the South Africa regulatory framework for cyber risk reporting
2. Lack of comprehensive cyber risk reporting by banks, specifically relating to cyber risk incident reporting

Recommendations for regulators

Enhance cyber risk reporting regulations

1. Mandate cyber risk incident reporting to investors.
2. Offer clearer guidance on materiality determinations.
3. Enhance guidance on the information to be included in periodic reports.

Recommendations for banks

Banks to enhance cyber risk reporting

1. Refer to this study on areas to improve their cyber risk reporting.
2. Consolidate all cyber risk information into a single report with appropriate cross-referencing in other reports.

APPENDICES

Appendix A: Expanded codebook

The image below shows a summary of the completed and expanded code book that links all cyber risk reporting themes and subthemes.

Figure 3: Image of the researcher showing the expanded codebook

Appendix B: Reflexivity journal

Item	Experience/Insight	Action
The research proposal process	The research proposal process was challenging. I had to restart at the beginning of the year, focusing on identifying a suitable topic for a document analysis. Cyber risk reporting was ideal, given its increasing importance on banks and the growing importance of understanding and managing cyber risk. Additionally, I recognised a gap in obtaining cyber incident information, and believed this was worth exploring. The research process itself was demanding, especially as I adjusted to working with a supervisor. The literature review was the most challenging part, as I re-did it several times, based on feedback from my supervisor and professors. My proposal was eventually accepted, confirming the relevance of my chosen topic and approach. Balancing this work with my job was difficult, as my workplace was undergoing a reorganisation, and I had increased responsibilities with a colleague on maternity leave.	I presented a range of study options and study objectives to my supervisor, and we discussed the benefits and drawbacks of each. Cyber risk emerged as the most relevant, interesting, and value-adding topic. I dedicated weekends, late nights, and early mornings before work to my proposal, often sacrificing my social life to stay on track.
Background	Reworking the background section for my mini dissertation took considerable time. Although I initially developed it as part of the proposal, it required substantial revision for the mini dissertation to focus on the reporting aspect of cyber risk. The process was time-consuming, due to the need to identify relevant academic sources that emphasised the importance of cyber risk reporting for investors. While there is abundant material on cyber risk, specific information on cyber risk reporting, especially from a South African perspective, was limited, there is also a lack of resources linking cyber risk reporting to investor needs. Reviewing regulatory reports added to the time pressure. I focused on the SEC guidelines, as they highlight information deemed valuable to investors, and used this as a reference to assess whether South African reporting aligns with those standards. It proved beneficial in the end as I was able to highlight gaps in South Africa's cyber risk reporting framework. The extensive literature review helped me refine the research objectives and was instrumental in developing the thematic codebook.	I spent considerable time reviewing academic literature on cyber risk reporting, collecting information, and allowing the key themes to emerge naturally without preconceived expectations. Although not all the information was relevant, the process allowed me to identify the core themes and develop the narrative around them.
Data collection process	Initially, the plan was to review only the integrated reports of the top five banks. However, as I began the process, I realised that each bank reports differently and uses multiple reports to	I took a methodical approach to extracting relevant cyber risk information from the reports. A key challenge was that each report had a unique tone and structure, requiring extra time to understand

	capture various aspects of cyber risk information. This led me to expand my review to include multiple reports per bank. I conducted a keyword search for "cyber" across these reports and briefly considered searching for "risk" as well. However, I found that searching for "risk" produced excessive information, which led me away from cyber-specific data and down a path of general risk reporting. Thus, I decided to focus solely on cyber-related terms to maintain relevance.	their nuances. Additionally, some banks repeated information across various reports with slight variations, so I had to identify and account for these duplicates.
Coding of information	The coding process for the thematic review was time-consuming but manageable. My supervisor provided guidance on the structure and format, which helped me organise information and group-related topics effectively. After categorising the data, I stepped back to understand the high-level message that each requirement conveyed. Using this approach, I applied themes and subthemes to the regulatory statements. The coding process for the banks' reports presented different challenges. First, I had to identify and collect statements from multiple reports. Then, interpreting these statements was complex, as each report had a unique writing style and language, making it challenging to accurately assign themes and subthemes. Additionally, I discovered new themes not covered in the initial codebook, which I marked as new codes for further analysis.	Engaging with my supervisor was also beneficial; discussing my approach to coding and assigning themes helped solidify my understanding. Throughout the coding process I treated the codebook as a working document, frequently updating and refining it.
Results and discussion	The results and discussion section initially presented challenges, particularly in effectively displaying the data. Initially, I aimed to quantify statements by calculating the percentage related to each theme across banks, but this approach proved ineffective in delivering a clear message. Following discussions with my supervisor, I shifted to a different format that was clearer and more impactful. Determining the alignment of statements (as fully aligned, partially aligned, or not aligned) required some subjectivity. In cases where alignment was ambiguous, I made judgement calls based on the degree and relevance of the information provided. My findings indicated that, while relevant information is available, there is a need for clearer regulatory guidance on what should be reported and for banks to improve the comprehensiveness of their reporting and the structure of their disclosures.	Working closely with my supervisor, consulting on my analysis approach, and discussing alignment decisions greatly supported my process. Focusing on addressing the research objectives in my conclusion helped to effectively bring the study to a well-rounded close.