Risk reporting compliance in the South African banking sector

TV Kheswa

orcid.org 0000-0001-7727-3646

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

Supervisor: Dr E Mulambya

NOTES TO EXAMINERS

- The mini-dissertation should demonstrate that the student has the ability to:
  - Do research
  - Constructively criticise own and others' research
  - Report the research results clearly, accurately and concisely with enough information to allow others to evaluate, and perform a similar study, should they wish to do so.
- This study represents the student's learning during a nine-month research project at master's degree level. It is therefore not necessary that the results represent a substantial contribution to the academic knowledge of the field.
- The mini-dissertation was written in article format and consists of three sections: Research project overview, Article, and Reflection. The focus of the mini-dissertation is on the article written by the student.
- The research project overview section should provide a high-level introduction to the research project that adequately prepares the reader to understand how the study fit into the Centre for Applied Risk Management (UARM)'s research projects.
- The potential journal selected by the student is intended as an academic learning experience for the student. If suitable, a reworked version of the article may be submitted to the selected journal post examination.
- The reflection section should provide a critical evaluation of the study, and also gives the student the opportunity to reflect on her/his personal learning during the project.
- The student should provide a study-specific summary of the literature related to the specific study in the article and is not expected to provide a separate chapter containing a risk culture literature review in the mini-dissertation, as this has been covered and assessed as part of the examined assignment for the Behavioural Risk Management module that forms part of this master's degree.
- The maximum word count for the article is 8000 words. This maximum word count includes words used in tables and figures, and excludes the article abstract, references and appendices. The maximum word count for the abstract is 300.
- The additional information in the appendices should be considered when evaluating the content of the three main sections of the dissertation.
- The role of the supervisors was to provide guidance and assistance on project conceptualisation, data analysis, interpretation and writing skills. The student carried the major responsibility for conceptualising, setting up, executing and writing up the research project.

- Turnitin was used to assist with plagiarism checking before the student was allowed to submit for examination.

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 members of the supervisory team 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 doing these edits, and for the grammatical correctness of the final document.

The main study supervisor gave the student permission to submit this mini-dissertation for examination.

ABSTRACT

Lessons learned from dealing with real-time risk management during the COVID-19 pandemic were different from those learned from the 2008 global financial crisis. A set of principles introduced by the Basel Committee on Banking Supervision (BCBS) were intended to improve risk management and decision-making processes for banks. Current research appears not to address the practicality of these principles and the compliance of South African banks with these principles. The purpose of this research was to explore the South African banking industry's compliance with BCBS 239. Using qualitative document analysis, this study employed documents available in the public domain, downloaded from the five biggest banks in South Africa. The results indicate that not all South African banks have achieved full compliance with BCBS 239. The initial full compliance status deadline was 31 January 2017, set by the South African Reserve Bank (SARB); however, two of the Big Five banks achieved it only by the year ended on 31 December 2022. The three other banks claim to be aligned with the Risk Data Aggregation and Risk Reporting (RDARR) principles. The results show that there are significant challenges facing the banking sector in South Africa in terms of risk reporting compliance. Since each bank publishes the information in a different way, there are notable variations in the risk reports. These findings are important to understand the impact of strong governance procedures as well as data management in relation to how the financial institutions will be able to withstand dangers and tumultuous changes during any potential crisis by putting the BCBS 239 principles into practice. This study is seemingly the first to investigate the South African banking industry's compliance with BCBS 239 in respect of making better risk-based decisions.

Keywords: Risk management, Risk reporting, Compliance, Risk governance, BCBS 239, Financial sector, Banks, Principles

ACKNOWLEDGEMENTS

I would like to thank the following:

- God for the knowledge and wisdom He bestowed in me to make a significant contribution to the world of risk management with this mini-dissertation.
- My wife, Relebohile Kheswa, for the love and support she gave me throughout the process, as well as the sacrifices she made to ensure that I complete this study and give it my best.
- My children, Lang'elihle and Nkazimulo: they are the light of my life and a gift beyond this world.
- My supervisor, Dr Emmanuel Mulambya, for his support throughout the journey and actually believing in me and this study.
- My study advisors and the team at the NWU Centre for Risk Management, for taking a chance on me to be one of the prestige students to enroll in this academic programme.
- The Kerlick team, Dr Elisabeth Lickindorf and Dr Graham Baker, for not only working on the writing of the article, but also providing a perspective from a reader outside the banking industry to ensure the relevance of the study.
- To Rudy Lingenfelder, with whom I started this journey under his guidance performing RDARR audits.
- And on the foundation are my parents (Nombali Flora Kheswa and Mbuyiswa Simon Kheswa) and my Clan: Zwane, Mangethe, Linda Mkhonto, Zikode kaPhikela, Makhonya, Mqhamzani, and Fanyane, who came to this Earth before my time and paved a path of great history that I inherited through their DNA to be born under their lineage.

TABLE OF CONTENTS

PREFACE ..... **III**

ABSTRACT ..... **IV**

ACKNOWLEDGEMENTS ..... **V**

TABLE OF CONTENTS ..... **VI**

LIST OF TABLES ..... **VII**

LIST OF FIGURES ..... **VII**

RESEARCH PROJECT OVERVIEW **1**

ARTICLE **3**

ABSTRACT 3
INTRODUCTION 5
BACKGROUND 6
METHOD 10
RESULTS AND DISCUSSION 12
CONCLUSION 22
REFERENCES 25

REFLECTION **27**

APPENDICES **29**

APPENDIX A 29
APPENDIX B 33

LIST OF TABLES

Research Project Overview: Table 1. Role players in the study of risk reporting compliance in the South African banking sector. 2
Article: Table 1. Summary of 14 RDARR principles recommended by the BCBS (BCBS, 2013). 6
Article: Table 2. Key terms employed in this paper. 7
Article: Table 3. Codebook on the analysis of risk reporting compliance in the South African banking industry. 14
Reflection: Table 1. Summary of the reflections in my journal……28
Appendix A. Initial Codebook……..29
Appendix B. Full Codebook. 33

LIST OF FIGURES

Figure 1. Count of D-SIBs by BCBS 239 compliance status. 12
Figure 2. Risk universe of the South African D-SIBs. 13

RESEARCH PROJECT OVERVIEW

There were differences between the lessons acquired from the global financial crisis of 2008 and the lessons learned from managing risks in real time during the COVID-19 outbreak. For banks, the set of guidelines brought forward by BCBS 239 were meant to enhance risk management and decision-making procedures.

This sparked an interest in the mind of the researcher about the compliance with the risk data aggregation and risk reporting (RDARR) principles by the South African banking industry. This led to the proposed research question: How does the South African banking industry comply with BCBS standard 239? This study aims to address whether banks prioritise compliance above making better risk-based decisions in accordance with BCBS 239's recommendations. Furthermore, the study aims to understand whether banks interpret these principles differently and, if so, does the regulator still view them as compliant?

The researcher occupies the role of third line of defence as an internal auditor in the organisation in which he is employed. The purpose of this role is to provide an independent objective assurance on the effectiveness of the management of risk across the group in which the organisation is a member, which is inclusive of compliance with BCBS standard 239.

The *Journal of Risk Research* has been chosen as the publication where this article may be published. The reason the researcher selected this journal is that it seeks to disseminate the most recent theoretical and empirical findings as well as commentary on risk communication, regulation, and management. This helps to investigate the connections between risk, society, and decision-making, as well as how to advance more effective risk management techniques. The Social Science Citation Index (SSCI), Scopus, and various business journal rankings, such as the Chartered Association of Business Schools (CABS) list and EBSCO (Business Source Corporate, Business Source Premier, TOC Premier), are just a few of the prestigious databases that index this journal, which makes it advantageous to use.

The following link will provide you with the author's writing guidelines required for the chosen journal: https://www.tandfonline.com/action/authorSubmission?journalCode=rjrr20&page=instructions

Additionally, this study provided the researcher with an opportunity to learn how to undertake an applied research project to demonstrate mastery of research at 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.

Research Project Overview: Table 1. Role players in the study of risk reporting compliance in the South African banking sector.

#	Team member	Role
1	Researcher	Conducted research through a qualitative study employing a literature review and document analysis, including preparation of the dissertation.
2	Supervisor (and additional study advisors)	Provided guidance and assistance on project conceptualisation, data analysis, interpretation and writing skills.
3	Editor	Advised during article writing workshops, and conducted a pre-final grammar-only edit of the dissertation.

ARTICLE

Risk reporting compliance in the South African banking sector

Abstract

Lessons learned from dealing with real-time risk management during the COVID-19 pandemic were different from those learned from the 2008 global financial crisis. A set of principles introduced by the Basel Committee on Banking Supervision (BCBS) were intended to improve risk management and decision-making processes for banks. Current research appears not to address the practicality of these principles and the compliance of South African banks with these principles. The purpose of this research was to explore the South African banking industry's compliance with BCBS 239. Using qualitative document analysis, this study employed documents available in the public domain, downloaded from the five biggest banks in South Africa. The results indicate that not all South African banks have achieved full compliance with BCBS 239. The initial full compliance status deadline was 31 January 2017 set by the South African Reserve Bank (SARB); however, two of the Big Five banks achieved it only by the year ended on 31 December 2022. The three other banks claim to be aligned with the Risk Data Aggregation and Risk Reporting (RDARR) principles. The results show that there are significant challenges facing the banking sector in South Africa in terms of risk reporting compliance. Since each bank publishes the information in a different way, there are notable variations in the risk reports. These findings are important to understand the impact of strong governance procedures as well as data management in relation to how the financial institutions will be able to withstand dangers and tumultuous changes during any potential crisis by putting the BCBS 239 principles into practice. The study is seemingly the first to investigate the South African banking industry's compliance with BCBS 239 in respect of making better risk-based decisions.

Keywords: Risk management, Risk reporting, Compliance, Risk governance, BCBS 239, Financial sector, Banks, Principles

Acronyms

BASA – Banking Association of South Africa

BAU – Business-As-Usual

BCBS – Basel Committee on Banking Supervision

DMO – Data management organisation

EDP – Enterprise data programme

G-SIBs – Global systemically important banks

GIA – Group internal audit

RDARR – Risk data aggregation and risk reporting

IT – Information technology

FSB – Financial Stability Board

PA – Prudential Authority

Introduction

The principles incorporated in effective risk data aggregation and risk reporting (RDARR) standard 239, which is commonly known as Basel Committee on Banking Supervision (BCBS) 239, were issued by the Basel Committee on Banking Supervision (BCBS) in January 2013 (BCBS, 2013). These principles were written for global systemically important banks (G-SIBs), which are large banks, depending on the scale and the degree of influence they hold in global and domestic financial markets (BCBS, 2013). The BCBS and the Financial Stability Board (FSB) developed a criterion to identify these G-SIBs, of which there are 30 banks in total across the globe (FSB, 2022).

However, the BCBS advised that domestic systemically important banks (D-SIBs), which are banks that could significantly disrupt the domestic financial system and the overall economy if they are in crisis or to fail, to be included in the scope of this set of principles by national supervisors (BCBS, 2013). The BCBS published guidelines for identifying D-SIBs using an indicator-based measure to take into account the various aspects of harmful externalities and their contributions to systemic risk. The South African National Supervisor, which is the South African Reserve Bank (SARB), improved the methods for identifying the D-SIBs in South Africa by the addition of indicators and criteria that more accurately reflect South African situations (SARB, 2019). These D-SIBs are commonly known as the Big Five banks in South Africa.

The set of principles introduced by BCBS 239 were intended to improve risk management and decision-making by the G-SIBs and D-SIBs. However, compliance with RDARR processes was then called into question when lessons learned from dealing with real-time risk management during the COVID-19 pandemic were different from those learned from the 2008 global financial crisis. The problem came to light when banks prioritise compliance above making better risk-based decisions in accordance with BCBS 239's recommendations. If different banks apply these guidelines differently, the national supervisor (SARB in South Africa) still views them as compliant.

The purpose of this study was to explore the interpretation of, and compliance with, these guidelines by South African banks. Moreover, the study explored how the principles have assisted South African D-SIBs in identifying significant risks that they believe are most important in terms of undermining their capacity to accomplish their strategic goals. The following research question was addressed: How does the South African banking industry comply with BCBS 239? Many related studies have been conducted on this matter elsewhere but not based on the South African context. Current research appears not to address the practicality of these principles, and the compliance of South African banks.

The study's findings are essential for understanding how financial institutions would be able to endure risks and turbulent changes throughout a potential crisis. Furthermore, the study is seemingly the first to examine how well the South African banking sector complies with BCBS 239 in terms of making better risk-based choices.

Background

Many organisations, particularly those in the banking industry, learned the hard way in 2008 that their information technology (IT) and data infrastructures were not adequate to support their RDARR. Some banks were, therefore, unable to manage their risks effectively, leading to serious repercussions for both the stability of the financial system as a whole and of the particular institutions themselves (BCBS, 2013). In response, the BCBS introduced standard 239 (BCBS 239), which advocates a set of 14 principles to enhance risk management and decision-making processes for banks and other financial service institutions (Elhassouni, 2020). These principles are summarised in Table 1

Article: Table 1. Summary of 14 RDARR principles recommended by the BCBS (BCBS, 2013).

1.	**Overarching governance and infrastructure**	
Principle 1	Governance	Strong governance structures that are in line with other Basel Committee guidelines and principles should be applied to a bank's risk data aggregation capabilities and risk reporting procedures.
Principle 2	Data architecture and IT infrastructure	In addition to adhering to the other principles, a bank should design, develop, and maintain data architecture and IT infrastructure that fully supports its risk data aggregation capabilities and risk reporting processes both in normal times and during stressful or emergency situations.
2.	**Risk data aggregation capabilities**	
Principle 3	Accuracy and Integrity	To satisfy normal and stress/crisis reporting accuracy requirements, a bank should be able to produce accurate and trustworthy risk data. To reduce the likelihood of errors, data should be aggregated primarily automatically.
Principle 4	Completeness	All relevant risk information for the entire banking group should be able to be collected and aggregated by a bank. Data that enable identifying and reporting risk exposures, concentrations, and developing hazards should be made available by business line, legal entity, asset type, industry, area, and other groupings, as applicable for the risk in issue.
Principle 5	Timeliness	The standards of accuracy and integrity, completeness, and adaptability should all be met by a bank in order to create aggregate and current risk data in a timely way. The precise date will depend on the kind of risk being monitored, how volatile it could be, and how important it is to the bank's overall risk profile.
Principle 6	Adaptability	In order to satisfy a wide range of on-demand, ad hoc risk management reporting demands, including those made in times of stress or crisis, those made in response to shifting internal needs, and those made in order to satisfy regulatory inquiries, a bank should be able to produce aggregate risk data.
3.	**Risk reporting practices**	
Principle 7	Accuracy	Risk should be properly and accurately reflected in risk management reports, which should provide aggregated risk data. Reports ought to be compared and verified.

Principle 8	Comprehensiveness	All significant risk categories within the organisation should be covered in risk management reports. The size, complexity, and risk profile of the bank's operations, as well as the needs of the recipients, should all be taken into account when determining the depth and scope of these reports.
Principle 9	Clarity and usefulness	Clear and succinct information should be communicated in risk management reports. Reports must be clear and thorough enough to allow for well-informed decision-making.
Principle 10	Frequency	The frequency of risk management report preparation and distribution should be decided by the board and senior management (or other recipients as required). The frequency requirements should take into account the recipients' needs, the reported risk's nature, how quickly it can change, the value of reports in supporting solid risk management, and the effectiveness and efficiency of decision-making within the bank. Reporting should happen more frequently when there is stress or a crisis.
Principle 11	Distribution	The appropriate stakeholders should get risk management reports while ensuring confidentiality is upheld.
4. Supervisory review, tools and cooperation		
Principle 12	Review	Supervisors need to regularly assess how well a bank is following the aforementioned11 principles.
Principle 13	Remedial actions and supervisory measures	Supervisors should be equipped with the right tools and resources to demand prompt and efficient corrective action from banks to fix flaws in their risk data aggregation and risk reporting procedures.
Principle 14	Home/host cooperation	Regarding the monitoring, examination, and application of the principles as well as any necessary corrective action, supervisors should collaborate with pertinent supervisors in other jurisdictions.

Table 2 tabulates the definition of terms used in this dissertation.

Article: Table 2. Key terms employed in this paper.

No.	Term	Definition	Source
1	BCBS 239	Standard number 239 of the Basel Committee, which refers to the principles for Effective Risk Data Aggregation and Risk Reporting.	BCBS, 2013
2	Compliance	Complying with the BCBS standard 239 as required by the national supervisor.	SARB, 2013
3	National supervisor	Domestic body that is responsible for regulating and supervising financial institutions.	SARB, 2013
4	D-SIBs	Banks that could significantly disrupt their domestic financial system and the overall economy.	BCBS, 2013
5	G-SIBs	Large banks based on their influence in global and domestic financial markets.	FSB, 2013
6	Risk data aggregation	Defining, gathering and processing risk data according to the bank’s risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging or breaking down sets of data.	BCBS, 2013

7	Risk reporting	A method of identifying risks tied to or potentially impacting a bank's business processes.	Posey, 2021

Numerous studies have been conducted by various authors that describe the practice of the BCBS 239 principles. For example, banks must, among other things, adopt controls of risk data that are as stringent as those that apply to accounting data and guarantee that aggregated risk data accurately reflect all acceptable risks (Grody & Hughes, 2016b). Although the standard (BCBS 239) was introduced a decade ago, there is still much ambiguity surrounding it, primarily because of the possibility for bias in how each individual institution interprets the principles. Given the complexity of its implementation and the difficulties in interpreting it, the banking institutions' projects and initiatives have had to be implemented over an extended period of time (up to 24 months), which has significantly delayed compliance (Martins et al., 2022).

Indeed, like their international counterparts, South African banks continue to experience considerable difficulties implementing their BCBS 239 programmes (PwC, 2016). Given that BCBS 239 is a principles-based standard, it is not surprising that its definition of compliance differs from bank to bank. Some banks delegate the decision on how to evaluate compliance with BCBS 239 to their internal audit teams.

According to PricewaterhouseCoopers, a large accounting firm, BCBS 239 programmes need to contribute to developing a method for certifying or validating compliance status in order to connect all of the activities and deliverables to changes made in accordance with the principles, which is an intricate process (PwC, 2016). Because South African banks are smaller and less complex than G-SIBs, they should consider the possibility that the national supervisor may have higher expectations for compliance based on the lessons learned from their international counterparts (PwC, 2016).

A banking institution that achieves compliance with BCBS 239 is thought to be better equipped to foresee new market opportunities while also preventing future instances of financial market volatility (Martins et al., 2022). The banking industry has shifted to a "capabilities-based" perspective of compliance in the absence of specified compliance standards. With their regulators, institutions are deciding which skills must be displayed and at what level of maturity, which will serve as the foundation for reviewing compliance.

National supervisors have yet to provide explicit guidance on what constitutes compliance, but some lone examples of criteria are being provided (PwC, 2016). Because most banks perceive BCBS 239 compliance to be "just a data programme" or a risk issue, they have had difficulty implementing it across the organisation. A more fundamental cultural shift from the reactive to the proactive use of

risk information is, therefore, necessary for full compliance. Fundamentally, the institution must assume responsibility for continued adherence to BCBS 239 regulations (PwC, 2016).

On the other hand, Chakravorty (2015) argues that the deadlines given to banks to comply with BCBS 239 are difficult to achieve because of the challenges in data management and the declining profitability of most banks. He argues that the majority of banks are affected by the new rules and guidelines for aggregating risk data. However, the overriding goal of the BCBS 239 standard, and the fact that compliance is expected and evaluated by the national supervisor, sets it apart from earlier standards (Chakravorty, 2015).

According to a survey conducted by PwC (2016), most South African banks were planning to achieve material compliance by 1 January 2017. However, most of the banks interviewed in 2016 had not yet defined what full material compliance meant. For this reason, they wanted the South African Reserve Bank to extend the 1 January 2017 deadline (PwC, 2016). The SARB therefore issued a directive requesting D-SIBs to provide a report related to the extent of the respective bank's compliance with BCBS 239 by 30 September 2017 (SARB, 2016).

The national supervisor then held a meeting with the boards of directors of D-SIBs in 2017 on the progress made in achieving full compliance with BCBS 239 (SARB, 2017), and concluded that compliance with BCBS 239 is not a one-time exercise. As a result, the banks needed to describe processes adopted to ensure periodic assessments, continued application, monitoring, improvement and embedding of the principles in ongoing risk management frameworks (SARB, 2017).

The latest available progress report on adopting the BCBS 239 principles was published in 2020 by the Bank for International Settlements (BIS), which is an international financial institution offering banking services for national central banks, and a forum for discussing monetary and regulatory policies adopted by 63 central banks including the SARB.

According to the report, none of the banks had achieved complete compliance with the BCBS 239 principles (BIS, 2020). There are few precisely predefined measures that banks under their reach can use to track compliance with the law because BCBS 239 is a principles-based regulation.

There are no clearly defined penalties and/or repercussions for non-compliance, in contrast to many other financial regulations. If the principles are not followed and the data infrastructure is not changed to meet BCBS 239 requirements, the possible results could be fines and higher capital add-on charges, reputational risk, or a loss of competitive advantage (Kelemen, 2020).

The present study explored compliance of the South African D-SIBs with the BCBS 239 principles as of 2023, and the influence of the standard on their risk reporting. These results are crucial for comprehending how financial institutions will be able to withstand risks and tumultuous changes during any potential crisis by putting the BCBS 239 principles into practice.

Method

Study design

This is a qualitative study employing a literature review and document analysis of the risk reports published by the Big Five banks of South Africa. The primary research instrument in this study was the researcher, who had to demonstrate that the research project was conducted in a credible, transferable and trustworthy manner (Golafshani, 2003).

Data gathering

The literature review was based on articles downloaded from electronic platforms using North-West University's Google Scholar, JSTOR, and EBSCO Discovery Service (EDS) as sources. The following keywords were used for searches: BCBS 239 compliance status, risk data aggregation and risk reporting, risk reporting practices, and compliance status of BCBS 239 for South African banks. Moreover, the researcher obtained, and was guided by the directives issued, by the national supervisor (SARB) on its website, the progress reports in adopting the BCBS 239 principles on the BIS website, and position papers by PwC, a large auditing firm, in relation to BCBS 239.

Document analysis performed in this study was based on documentary data and not material collected from human subjects, so that no demographic data were required or gathered. Document analysis is efficient, cost-effective and manageable (Cardno, 2018). The data acquired are in the public domain, and the documents examined are unique to the sources and kept on the websites, available under "investor relations", of their respective organisations, comprising the Big Five banks in South Africa. The documents analysed were the Basel pillar 3 risk and capital management reports, and integrated reports for the year ended 31 December 2022, and 30 June 2023. Since the banks' annual financial statements were deemed irrelevant to the goals of the study, they were disregarded.

Data analysis

For the literature review, the researcher employed deductive thematic analysis to extract useful codes relating to the study objective of exploring the interpretation of, and compliance with, BCBS 239 guidelines by the South African banks. Thematic analysis, in this case, is defined as a method

to identify, analyse and report patterns or themes within data (Braun & Clarke, 2006). These codes relate to the compliance requirements of D-SIBs for RDARR practices. Thematic analysis is widely used for analysing qualitative data and is commonly employed when conducting a literature review.

The researcher examined the literature on BCBS 239 published by experts and the BCBS to compile an initial study-specific codebook, tabulated in Appendix A (Martins et al., 2022). This was followed by the analysis of documents from the five banks under study.

The researcher engaged in the process of comparing codes in the study data, by matching whether themes from the banks' reports or documents were aligned with those in the literature, and to examine whether the risk reporting practices are aligned with those recommended by BCBS 239. To verify the extent to which the banks have progressed, the full compliance status was also examined in these reports. The results were tabulated in Appendix B.

The pillar 3 risk and capital management reports give details about the operational and financial performance of the five banks. They are largely of interest to equity and debt investors in the bank, credit rating companies, depositors, regulators, and numerous other stakeholders. Risk and regulatory disclosures are included in the information provided, which can be used to evaluate the group's financial performance.

The objective of the reports is to provide a comprehensive view of the banks' regulatory capital and risk exposures, as well as evidence of how the banks' business model, initiatives, and approach to risk governance benefit their stakeholders.

In respect of reliability, all the information in the reports is unaudited; however, they are approved by the board of each respective bank and are prepared in accordance with board-approved internal control processes.

The final results are tabulated in the codebook, presented in Table 3 in the results and discussion section.

Ethical considerations

Analysis of documents available in the public domain: even though the information may be public, care was taken not to expose North-West University (NWU) to legal action by not identifying specific organisations in the report, which are not revealed in the discussion of the findings.

The researcher worked closely with his appointed study supervisors during the study where guidance was provided, and was trained to understand and manage the study risks. The study was conducted only after approval from the Optentia Scientific Committee and the Faculty of Economic and Management Sciences Research Ethics Committee (EMS-REC) at NWU.

Results and discussion

Document analysis of the D-SIBs in South Africa showed that the compliance status of the banks is reported in the Basel pillar 3 disclosure risk and capital management report.

The study's findings demonstrate that there is ambiguity because different banks define compliance differently, and interpret these principles differently. Each bank publishes data differently, as shown in the various reporting results, showing inconsistencies in risk reports. These inconsistencies are demonstrated in the final codebook with examples of how each bank applied its interpretation of the codes. The results are outlined in the final codebook tabulated in Table 3.

From the analysis of the reports provided in the final codebook (item 16), only two of the Big Five banks have achieved BCBS 239 full compliance status, as illustrated on Figure 1.

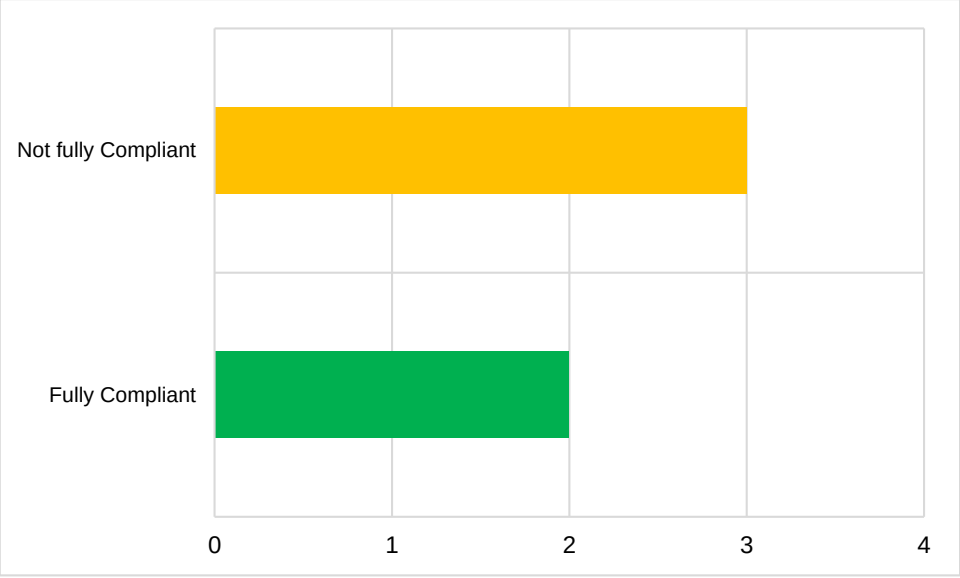

Figure 1. Count of D-SIBs by BCBS 239 compliance status.

The reported codebook shows common themes of what is to be reported; however, there is ambiguity in the interpretation of how each bank defines what is to be reported. This makes it difficult to conclude what it means to be “fully compliant”, especially when the national supervisor does not provide a standard definition of full compliance. The most common examples (illustrated in the codebook outlined in Appendix B) are the great differences in the comprehensiveness of the “risk

universe" for each bank, where the number of principal risks defined differs for each bank. These are summarised in Figure 2.

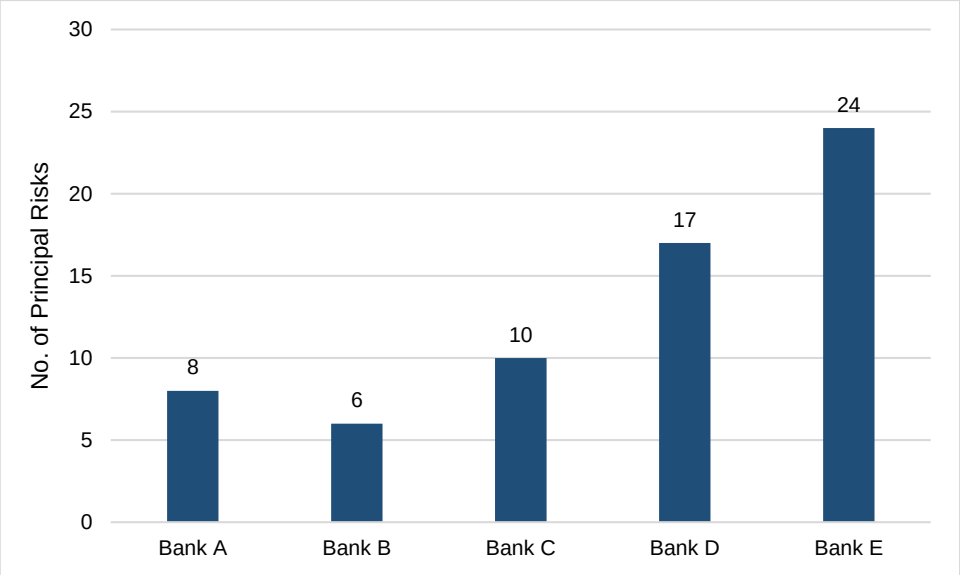

Figure 2. Risk universe of the South African D-SIBs.

These results show that there are clear challenges in relation to risk reporting compliance in the South African banking sector. The D-SIBs have adopted the risk reporting practices recommended by the BCBS, although each bank seems to have its own interpretation of the BCBS 239 principles. The banks that are not fully compliant do not report on the level of compliance achieved to date, and the ones that are fully compliant do not report on the level of compliance by each risk type and each principle, which implicates the assessed bank's degree of compliance.

Article: Table 3. Codebook on the analysis of risk reporting compliance in the South African banking industry.

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	**Bank B**	**Bank C**	**Bank D**	**Bank E**
1	Principle	A guideline	"In 2013, the BCBS published regulations (BCBS 239) pertaining to the principles RDARR. The Group's risk data aggregation capabilities and risk reporting practices are aligned with the principles of BCBS 239."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under BCBS Standard number 239."	"BCBS 239 was published in January 2013, setting out principles to strengthen banks' risk data aggregation capabilities and internal risk reporting practices. In turn, effective implementation of the principles is expected to enhance banks' risk management and decision-making processes. D-SIBs were required to comply with the principles by 1 January 2017."	"BCBS 239: Principles for Effective RDARR was issued in January 2013. The principles aim to strengthen banks' risk management practices by improving their RDARR practices."	"We manage non-financial risks under the umbrella of operational risk, by adopting the sound principles of operational risk management in our non-financial risk framework that drives the standardised management of all non-financial risk types."
2	Risk data aggregation	"To be able to compare performance to risk appetite and tolerance, the bank must define, collect, and process risk data in accordance with its risk reporting standards. Sorting, combining, or dissecting data sets are examples of this."	"Internal and external data is utilised in meeting regulatory requirements and the management of risk. The Group enters into selected data and analytics partnerships with third parties to enhance and heighten its understanding of customers. Internal data is owned and managed by the respective business units with regular assessment of data quality via their respective risk governance structures."	"Generate accurate, reliable and up-to-date risk data across the banking group activities to identify and report risk exposures, concentration and emerging risks."	"Risk reports to the board, board risk committees, segment/operating business risk committees and senior management include the following: • risk exposure and risk-adjusted business performance; • comparison of risk management performance against risk appetite, limits and indicators; • periodical reviews of progress against and deviations from the risk management plan;	"All (tier 1) core risk appetite metrics are being tracked within the board-approved risk appetite targets at 31 December 2022 with the exception of those related to cyberrisk (two out of 23 metrics) – management action is in place to manage the risk accordingly."	"Risk reports are compiled at business unit level and are aggregated to the enterprise level for escalation through the governance structures based on materiality."

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
3	Risk reporting	A method of identifying risks tied to or potentially impacting an organisation's business processes.	"The objective of risk reporting is to provide timeous, accurate, comprehensive and useful information to the Board and senior management to facilitate informed decision-making. Board and senior management risk committees determine their requirements in terms of content and frequency of reporting under both normal and stressed conditions. Risk reporting processes flow from the business unit and relevant risk committees to the ERC and thereafter to Board committees."	"Risk reporting is clear, concise and puts management and the board in a position to make informed risk decisions."	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"Balance Sheet Management (BSM) provides strategic direction, insight and motivation in managing capital risk to the Group Assets and Liabilities Management and Executive Risk Committee (ALCO) through appropriate risk reporting and analytics and by providing strategic input within the group's defined risk appetite."	"Risks are reported and discussed in the risk governance structures and executive management committees. Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."
4	Enterprisewide risk management (ERM)		The process of identifying potential events that may affect the group negatively, managing risk so that it remains within the risk appetite of the group, and providing reasonable assurance with regard to the achievement of the goals of the group. The board of directors, management and other personnel drive this process and apply it in strategy setting throughout the group.	"The Enterprise Risk Management Framework (ERMF): (1) Outlines the approach to the management of risk and provides the basis for setting frameworks and policies, and establishing appropriate risk practices throughout the Group, (2) Defines the risk management process and sets out the activities, tools, techniques and the operating model to ensure material risks can be identified and managed."	"As part of the reporting, interrogation and control processes, Enterprise Risk Management (ERM) drives the implementation of more sophisticated risk assessment methodologies through the design of appropriate policies and processes, including the deployment of skilled risk management personnel in every business."	"The Group's Enterprisewide Risk Management Framework (ERMF) enables the group to identify, measure, manage, price and control its risks and risk appetite, and relate these to capital requirements to help ensure capital adequacy and sustainability, thereby promoting sound business behaviour by linking these aspects with performance measurement and remuneration practice." "	"The second line of defence directs the definition of the enterprisewide risk management programme. They facilitate execution of risk lifecycle activities and provide expert advice, guidance and support to the first line of defence team. They have oversight of the implementation and effective execution of risk and returns decisions within the set risk appetite and target strategy."

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
5	Risk governance	"The actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks."	"The Group identifies and assesses risks and opportunities arising from internal and external environments, and proactively identifies emerging risks. To ensure effective risk management, our consolidated response is monitored as follows: • Uphold the risk governance structure at Group, country, business and Group functions, with clear Board escalation and oversight."	"We have an extensive, multi-layered structure to govern risk, however, our board is ultimately responsible for risk management. This includes ensuring that risks are adequately identified, measured, managed and monitored and that good governance is maintained.“	"The risk governance and management structure is set out in the group’s risk management framework. As a policy of the board, the group risk management framework delineates the roles and responsibilities of key stakeholders in business, support and control functions across the group.” “	"The board of directors has the ultimate responsibility for the group’s business strategy, financial soundness, governance, risk management and compliance and has allocated oversight of risk governance to the Group Risk and Capital Management Committee (GRCMC). This includes, among other things, the overall effectiveness of the process relating to corporate governance, internal controls, risk management, capital management and capital adequacy."	"Our risk management system is governed by appropriately mandated governance committees and fit-for-purpose governance documents. Governance committees are in place at both a board and management level. These committees have mandates and delegated authorities that are reviewed regularly. Members have the requisite skills and expertise to manage risk."
6	Compliance	Complying with rules, laws, and guidelines set by the national regulator.	"Manage the funding and high-quality liquid assets (HQLA) position in line with the Board-approved framework and ensure compliance with regulatory requirements."	"We believe that RDARR is more than a compliance requirement and that mature RDARR capabilities add value to our understanding and management of risk."	"The Group’s implementation of BCBS 239 resulted in enhanced risk management and decision-making processes, and risk data maturity. Focus has shifted from remediation of compliance gaps to maintaining compliance."	"RDARR compliance for the bank’s key tranche 3 risk types. (AML risk, Conduct risk, and cyber risk) met the RDARR compliance requirements for the December 2022 deadline."	"Risk management reports comply with the standards set out by BCBS239."

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
7	Three Lines of Defence (3LoD)	An effective governance operating model that enables the banks' Board of Directors and management to carry out and monitor the affairs of the group to meet the obligations of the group to its depositors, regulators and shareholders with the aim of creating and protecting value sustainably. The 3LoD defines risk management, risk oversight and assurance roles across businesses and functions of the group.	"The Group applies a three lines of defence model in support of the combined assurance model to govern risk across all businesses and functions. The ERMF assigns specific responsibilities to each line of defence."	"The focus remained on improving the risk maturity and clearly delineating the lines of defence in our risk management framework. • 1st line of defence is Risk ownership • 2nd line of defence is Risk control • 3rd line of defence is Independent assurance (internal audit)."	"The group obtains assurance that the principles and standards in the operational risk management framework are adhered to by the three lines of defence model, which is integrated in operational risk management."	"The 3LoD Model forms an important part of the ERMF, which provides the structure in which the group operates. If risks taken are not managed and controlled effectively, it can prevent the group from achieving its strategic objectives. The roles and responsibilities of the 3LoD model provides a structure for considering risk and control, to ensure that they are appropriate and managed effectively."	"The three lines of defence model is leveraged to maintain a strong risk culture with an emphasis on doing the right business, the right way."
8	Accuracy	Closeness of agreement between a measurement or record or representation and the value to be measured, recorded or represented.	"The objective of risk reporting is to provide timeous, accurate, comprehensive and useful information to the Board and senior management to facilitate informed decision-making."	"Ensure reports are accurate, convey aggregated risk data and are reconciled and validated"	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"The Group has acted in good faith and has made every reasonable effort to ensure the accuracy and completeness of the information contained in this document,"	"Risk information is subject to strong data and reporting controls. It is integrated into all business reporting and governance structures. Our governance structure enables oversight and accountability through appropriately mandated board and management committees."

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
9	Comprehensiveness	Extent to which risk reports include or deal with all risks relevant to the firm.	"The ERMF includes risks taken by the Group that are foreseeable and material enough to merit establishing specific Group-wide control frameworks. These are grouped into eight principal risks that account for the vast majority of the total risk faced by the Group." "	"The risks we manage include: • Credit risk • Operational risk • Market risk • Capital and liquidity risk • Reputational risk • Operational risk consists of the following categories: • Fraud risk • IT risk • Information risk • Compliance and legal risk • Other risks."	"Risk limits for all risk types are integral to risk management and are instrumental in constraining risk taking within appetite. Qualitative risk appetite principles are designed to support a strong risk culture in the group and provide a foundation to ensure appropriate behaviour and conduct. The risks, and the roles and responsibilities of the various stakeholders across business, support and control functions are described in the group's risk management framework, e.g. • Liquidity risk • Funding liquidity risk • Market liquidity risk • Credit risk • Settlement risk • Country risk • Credit default risk • Other risks."	"For 2023, our top 10 risks, indicated below, are selected as top-of-mind risks rather than business-as-usual principal risks. 1. Business Risk (Including Geo-Political and Country/Sovereign Risks) 2. Credit Risk 3. Cyberrisk 4. People Risk 5. Strategic Execution Risk 6. 6 Organisational Resilience Risk 7. Operational risk (including emerging-IT, digital transformation and data risks) 8. Climate Risk 9. Reputational and Conduct Risks 10. Capital Risk."	"Our risk universe represents the risks that are core to our financial services business. We organise these into strategic, financial and non-financial categories and biennially identify key enterprise risks. • Strategic risks • Financial risks • Non-financial risks."
10	Clarity and usefulness	The ability of risk reporting to be easily understood and free from indistinctness or ambiguity.	"Reports provide key insights into developing industry, sector and product trends and incorporate agreed management actions to modify behaviour and strategy in accordance with specific findings."	"Risk reporting is clear, concise and puts management and the board in a position to make informed risk decisions. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements."	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"These enhancements to Group's modelling and risk management tools allow the bank to stay ahead and respond to a crisis appropriately. More specifically, they enable the bank to make informed strategic decisions in these unprecedented times through: (1) delivering analysis and insights to enable well-informed decision-making."	"Risk information is subject to strong data and reporting controls. It is integrated into all business reporting and governance structures. Our governance structure enables oversight and accountability through appropriately mandated board and management committees. The three lines of defence model is leveraged to maintain a strong risk culture with an emphasis on doing the

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
							right business, the right way."
11	Frequency	The rate at which risk reports are produced over time.	"Board and senior management risk committees determine their requirements in terms of content and frequency of reporting under both normal and stressed conditions."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under BCBS 239. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements."	'"Regular risk reporting enables the board, senior management, the risk, compliance and capital committee (RCCC) and relevant subcommittees to evaluate and understand the level and trend of material risk exposures and their impact on the group's capital position, and to make timely adjustments to the group's future capital and strategic plans."	"The risk appetite, risk profile and risk exposures are reported regularly to the board and senior management through various governance committees and reviewed annually as part of the three-year group business plan."	"Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."
12	Distribution	Ensuring that the adequate people or groups receive the appropriate risk reports.	"Risk reporting processes flow from the business unit and relevant risk committees to the ERC and thereafter to Board committees."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under BCBS 239. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements."	"Reporting of risk information follows the governance structure. Specialist risk committees and segment/ operating business risk and compliance committees report to the RCCC and its subcommittees. Relevant executive committees receive reports on the risk profile, material risk exposures, risk-adjusted business performance and key risk issues. The RCCC submits reports to the board and highlights control issues to the audit committee."	"The board of directors has the ultimate responsibility for the group's business strategy, financial soundness, governance, risk management and compliance and has allocated oversight of risk governance to the Group Risk and Capital Management Committee (GRCMC). "	"Risks are reported and discussed in the risk governance structures and executive management committees. Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
13	Risk appetite	A description of what type and how much risk the group is willing to take on or keep taking on in executing its strategy. The group expresses risk appetite both quantitatively, using risk measures such as economic capital and risk limits, and qualitatively in terms of policies and controls.	"The Group's risk appetite: • Specifies the level of risk the Group is willing to take in pursuit of its strategy. • Considers all principal and material risks individually and, where appropriate, in aggregate."	"Our risk appetite is the level of risk we are willing to accept while pursuing our objectives."	"The Group's risk appetite is the aggregate level and the type of risks the group is willing and able to accept within its overall risk capacity in the execution of its strategy. It is captured by a number of qualitative principles and quantitative measures."	"Risk appetite is an articulation and allocation of the risk tolerance or quantum of risk the group is prepared to accept in pursuit of its strategy. Risk appetite is integrated into the group's strategic and business planning process and is approved by the board and monitored by varying levels of senior management, with ongoing oversight and coordination by Group Risk."	"Risk appetite is an expression of the amount or type of risk we are willing to take in pursuit of our financial and strategic objectives, reflecting our capacity to sustain losses and continue to meet our obligations as they fall due, under both normal and a range of stress conditions."
14	Risk exposure	Means how much risk being taken on, described in terms of how likely the risk event(s) are to happen and their impact on the goals.	"Key risk scenarios are a summary of the extreme potential risk exposure for each risk in the suite of operational and resilience risks and includes quantitative and qualitative assessments of the potential frequency of risk events, the average size of losses and extreme scenarios."	"The following tables contain an analysis of the credit risk exposure of loans and advances for which an Expected Credit Loss (ECL) allowance is recognised. "	"The group's risk exposure through its association with and usage of third parties, in particular vendors, remains an area of focus. "	"Developing appropriate metrics to provide insight into risk exposure trends and building in escalation triggers to alert and prompt action via indicators [key risk indicators (KRIs), key control indicators (KCIs), key performance indicators (KPIs)];"	"Risk exposures are reported on a regular basis to the board and senior management through our governance committees."
15	Risk universe	The complete picture of the risks across all business lines, functions, geographical locations and legal entities of the group. These risks are captured through the risk identification process. A qualitative list of the key risks that the group faces is kept.	"ERMF and frameworks include risk appetite and stress testing, as well as the 8 principal risks. These are grouped into eight principal risks that account for the vast majority of the total risk faced by the Group. • Financial principal risks • Non-financial principal risks • Risks straddling both financial and non-financial risks."	"Our risk universe consists of 6 risk categories that are managed by the EXCO, the Risk and capital management committee (RCMC), the Risk committee (RISCO), the Retail bank credit committee (RCC), the Business bank credit committee (BCC), the Asset and liability committee (ALCO) and the Data Steerco. These committees report to the	"A complete view of the group's principal and supporting risk universe is outlined below on this report: • Liquidity risk • Counterparty credit risk • Pre-settlement risk • Traded market risk • Non-traded market risk • Equity investment risk • Climate risk • Operational risk (including information	"The Group's risk universe is defined, actively managed and monitored in terms of the ERMF, in conjunction with the Capital Management Framework and its sub-frameworks, including the Economic Capital Framework. A summary table of the key risk types impacting the group highlights the mapping of the 17 key ERMF risk types to the 12 quantitative	"Our risk universe represents the risks that are core to our financial services business. We organise these into strategic, financial and non-financial categories and biennially identify key enterprise risks. These top enterprise risks require focused management because they represent material impacts to the strategy. We regularly scan the environment for

No.	Code	Code description	Examples of quotes from risk reports of South African D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
				RCMC, which is mandated by the board to oversee risk management."	technology (IT) and cyber risk) • Compliance and conduct risk • Other risks"	risk types of the Economic Capital [and Internal Capital Adequacy Assessment Process ICAAP)] Framework."	changes to ensure that our risk universe remains relevant. "
16	BCBS 239 full compliance	A status where a bank has received full compliance of the regulation BCBS 239.	Full compliance status not observed.	Full compliance status not observed.	"GIA validated the status of all material risk types and the group is fully compliant with the requirements of BCBS 239 for the standardised approach for measuring counterparty credit risk (SA-CCR), achieving full compliance by 31 December 2022 along with all other principal risk types."	"RDARR compliance for the bank's key tranche 3 risk types. (AML risk, Conduct risk, and cyber risk) met the RDARR compliance requirements for the December 2022 deadline. This follows compliance already having been met in December 2019 for the bank's key risk types (credit risk, market risk, operational risk, liquidity risk, investment risk and IRRBB)."	Full compliance status not observed.

The evidence from the analysis of Bank A suggests that “The Group’s risk data aggregation capabilities and risk reporting practices are aligned with the principles of BCBS 239.” However, this does not say whether Bank A has achieved full compliance with the BCBS 239 regulation or not. The compliance status for Bank A was reported for the year ended 31 December 2020.

The analysis of Bank B indicates that RDARR is more than just a compliance requirement; it enhances the understanding of risk management and decision-making processes. However, there is no confirmation that the bank has achieved full compliance with BCBS 239. The results simply state that clear and concise risk reporting enables management and the board to make informed risk decisions.

According to the analysis for Bank C, in order to determine the group’s compliance with the RDARR principles, the independent BCBS 239 compliance assessor, which is Group Internal Audit (GIA), submitted an audit report to the Prudential Authority (PA), clearly indicating the in-scope risk types across the 11 principles. This report was supplemented by the Banking Association of South Africa’s (BASA) attestation procedures and audit guidelines. The group was completely compliant with BCBS 239 by 31 December 2022, together with all other primary risk types, according to GIA’s validation of the status of all material risk types.

In order to comply with BCBS 239 compliance requirements, Bank D reportedly used a strategic approach as noted in the pillar 3 risk management report for 2022. Bank D made the decision to build a more long-term solution to address the management of enterprise data rather than concentrating exclusively on the compliance requirements. The bank achieved full compliance status by the deadline of December 2022.

According to the analysis for Bank E, risk management reports comply with the standards set out by BCBS 239. However, this does not say whether Bank E has achieved full compliance with the BCBS 239 regulation or not. The results indicate that the group risk and capital management committee periodically reviewed updates on progress to achieve BCBS 239 compliance in accordance with the scope and deadlines agreed with the SARB. However, the reported update did not confirm whether Bank E has achieved full compliance status or not.

Conclusion

The objective of the study was to explore risk reporting compliance with BCBS 239 of the South African banking sector. These principles are applicable to D-SIBs, which are commonly known as the Big Five banks in South Africa. Material compliance for these D-SIBs was initially planned to be achieved by 1 January 2017 (SARB, 2015). However, there has been a number of extensions by the South African National Supervisor as compliance status was a challenge to achieve.

The results show that only two D-SIBs achieved full compliance status of the BCBS 239, both achieving it by the year ended 31 December 2022. Other banks claim to be aligned with the RDARR principles; however, the reports are not clear on the progress of the compliance status. The study indicated that understanding the meaning of “fully compliant” and then making progress towards that goal are difficult and call for multi-year work plans (PwC, 2017).

The goal of risk reporting is to give the board and senior management timely, accurate, complete, and valuable information to support decision-making. The findings demonstrate that the South African banking industry faces definite difficulties with respect to risk reporting compliance. The D-SIBs have implemented Basel’s recommended risk reporting processes; nevertheless, each bank interprets the BCBS 239 principles differently in accordance with its own set of guidelines. As a result, there are significant differences in risk reports since every bank releases the information in a unique manner.

A study limitation was the availability of data, and articles, on South African banks based on the South African context. Many studies and articles were published during the early phases of BCBS 239 implementation for the 1 January 2017 deadline. However, there has been a lack of consistency and follow-up articles on the progress of the compliance status of the South African D-SIBs. The pillar 3 capital and risk management reports of the D-SIBs state that the SARB extended the full compliance deadline to 31 December 2022. There is a scarcity of literature published in 2023 to report on progress following the newly extended deadline.

The study indicated a future research possibility to investigate how the South African banking industry’s compliance with BCBS 239 is correlated to making better risk-based decisions. The outcomes of these better risk-based decisions can be studied based on how the D-SIBs will perform during the economic pressures influenced by rising inflation, increasing interest rates, loadshedding, as well as the Russia/Ukraine war, to name just a few factors.

In ensuring full compliance with BCBS 239, the study recommends that the national supervisor, the SARB, needs to force the D-SIBs to submit an audit report clearly indicating the in-scope risk types, also known as principal risks, across all principles, and mandatory reporting of progress on the pillar 3 risk and capital management reports. To enable a proficient assessment of the compliance situation, the SARB ought to incorporate an all-inclusive questionnaire that includes structured deliverables and benchmark data. The evaluation ought to be carried out using the well-known four-point rating scale developed by the Bank for International Settlements (KPMG, 2016). The four ratings are defined as follows (BIS, 2020):

“

- *Rating of “4” – The Principle is fully complied with: the objective of the Principle is fully achieved within the existing architecture and processes;*
- *Rating of “3” – The Principle is largely complied with: only minor actions are needed in order to fully comply with the Principle;*
- *“Rating of “2” – The Principle is materially non-complied with: significant actions are needed in order to progress further or achieve full compliance with the Principle; and*
- *Rating of “1” – The Principle has not been implemented.*

“

If all the D-SIBs risk reports were consistently rated in this way, they would avoid ambiguity.

Number of words:

Abstract: 285 (max: 300 words)

Article: 7889 *(max 8,000, excluding abstract and references)*

References

Azevedo, G., Oliveira, J., Sousa, L., & Borges, M. F. R. (2022). The determinants of risk reporting during the period of adoption of Basel II Accord: evidence from the Portuguese commercial banks. *Asian Review of Accounting*, *30*(2), 177-206.

BCBS. (2013). Principles for effective risk data aggregation and risk reporting. *Bank for International Settlements*, *8*.

BIS. (2020). Progress in adopting the Principles for effective risk data aggregation and risk reporting. https://www.bis.org/bcbs/publ/d501.pdf

Cardno, C. (2018). Policy Document Analysis: A Practical Educational Leadership Tool and a Qualitative Research Method. *Educational Administration: Theory & Practice*, *24*(4), 623-640.

Chakravorty, R. (2015). BCBS239: Reasons, impacts, framework and route to compliance. *Journal of Securities Operations & Custody*, *8*(1), 65-81.

Deloitte. (2019). BIS assessment of BCBS 239 compliance. https://www2.deloitte.com/us/en/pages/regulatory/articles/bis-assessment-bcbs-239-principle-compliance.html

Dill, A. (2019). *Bank Regulation, Risk Management, and Compliance: Theory, Practice, and Key Problem Areas*. Taylor & Francis.

Elhassouni, J. (2020). The implementation of credit risk scorecard using ontology design patterns and BCBS 239. *Cybernetics and Information Technologies*, *20*(2), 93-104.

FSB. (2022). 2022 List of Global Systemically Important Banks (G-SIBs). https://www.fsb.org/2022/11/2022-list-of-global-systemically-important-banks-g-sibs/

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-607.

Grody, A. D., & Hughes, P. J. (2016a). Risk Accounting-Part 1: The risk data aggregation and risk reporting (BCBS 239) foundation of enterprise risk management (ERM) and risk governance. *Journal of Risk Management in Financial Institutions*, *9*(2), 130-146.

Grody, A. D., & Hughes, P. J. (2016b). Risk accounting-part 2: The risk data aggregation and risk reporting (BCBS 239) foundation of enterprise risk management (ERM) and risk governance. *Journal of Risk Management in Financial Institutions*, *9*(3), 224-248.

Kelemen, A.-K. (2020, 02 March 2020). Regulatory Roadmap - BCBS 239. https://www.bbht.de/blog/regulatory-roadmap-legal-data-for-banking-bcbs-239.html

KPMG. (2016). Challenges around the implementation and validation of BCBS239/Risk Data Aggregation Programme. https://kpmg.com/za/en/home/insights/2016/08/challenges-around-the-implementation-and-validation-of-bcbs239.html

Martins, J., Mamede, H. S., & Correia, J. (2022). Risk compliance and master data management in banking–A novel BCBS 239 compliance action-plan proposal. *Heliyon*, *8*(6), e09627.

PwC. (2011). In times of uncertainty- an insight into effective Risk Reporting in a changing market. https://www.pwc.com.au/industry/banking-capital-markets/assets/insight-into-effective-risk-reporting-sep11.pdf

PwC. (2016). South African BCBS 239 Survey. https://www.pwc.co.za/en/publications/bcbs-239-implementations-in-south-africa.html

PwC. (2017). BCBS 239 - Raising the standard. https://www.pwc.com/gx/en/financial-services/assets/BCBS-239.pdf

SARB. (2015). D2 /2015: Effective risk data aggregation and risk reporting. https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2015/6629

SARB. (2016). D5/2016: Compliance with principles for effective risk data aggregation and risk reporting. https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2016/7465

SARB. (2017). Directive G2/2017. In (07 February 2017 ed.). South Africa: South African Reserve Bank.

SARB. (2019). A methodology to determine which banks are systemically important within the South African context. https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-

stability/resolution-planning/A-methodology-to-determine-which-banks-are-systemically-important-within-the-South-African-context%20(2).pdf

REFLECTION

Examining the South African banking industry's adherence to BCBS 239 was the study's main goal. The D-SIBs, also referred to as the “Big Five” banks in South Africa, are subject to these guidelines. This journey for me started in 2020, when I was assigned to perform an audit on BCBS 239 at one of the main banks.

The subject has since been of key interest to my heart, especially when it comes to the topic of risk management. The theme in banking is moving towards using data to enable risk-based decision making, and thus the RDARR principles were presented by the Basel committee as the solution required to achieve this goal.

As I was performing this audit, I realised that each division within the bank was interpreting these principles differently, and each risk type had its own implementation strategy based on their interpretation. I was then curious to research more about this topic, and how the regulator assessed compliance status.

After going through a period of searching for a suitable programme, I decided to pursue the Master’s Programme in Applied Risk Management (MARM) at NWU, as it was designed specifically for employees in my shoes who wish to grow in a senior risk-management related role, but more importantly, it addresses the requirements for risk management expertise in the South African industry.

Having a National Qualifications Framework (NQF) 8 qualification, I was very comfortable that I knew how to conduct academic research. However, this perspective changed very quicky during my first year of studies as I had to re-learn everything I thought I knew in preparing to conduct this study. I had to undergo training to learn how to do independent research and apply different research methods, including how to use EndNote for referencing, which was a new experience for me. I was taken into a deeper context to understand the fundamentals of risk management, risk assessment tools, risk governance, compliance, and the regulatory environment, as well as risk reporting tools and formats. This equipped me with enough knowledge to submit my draft proposal for the topic of my interest.

Reflexivity in research is increasingly being encouraged. Accordingly, Table 1 provide a summary reflective journal for my study.

Table 1. Summary of reflections for my study.

Date	Insight	Action
03 March 2023	Presented my research proposal to my supervisor and study advisors.	My topic was interesting; however, I needed to refine my title for it to be suitable for the study.
10 March 2023	My supervisor took me through the advantages and disadvantages of doing a document analysis study, compared with an interview-based study.	I changed my research proposal, to exclude interviews, and made it a full document analysis study.
03 May 2023	I attended a workshop on the introduction to article writing, planning, and concept outline.	This helped me refine my concept outline to structure my study objective and expectations.
02 June 2023	The writers' retreat session on preparing the Introduction, Background, and Method sections made me realise that they were missing a lot of key details I had never considered before. This was a very painful experience.	I changed my Introduction, Background, and Method to write them according to the guidelines provided by the study advisors.
18 August 2023	My codebook was not properly documented, and did not address the findings for each bank, only the overall example of the findings across all banks.	I had to redevelop my codebook and table it according to academic requirements. Moreover, I had to show the findings of each bank in the codebook.

As indicated on the reflection journal, the journey was full of highs and lows, especially with the academic writing retreat sessions. There was a point where I felt misunderstood and that my article was no longer addressing the research objective. However, I had to sit down with my study advisors and supervisor to get their perspective and reach a common ground. This is when I was re-introduced to the concept of a cold reader, something that I always employ in my audit reports at work. I had to adopt the perspective that I need to write from the perspective of a cold reader and remove assumptions that the reader understands the banking concepts and processes, and thus, and can follow through the arguments and points I was bringing forth in the article.

The research process exceeded my expectations as my article is not just an academic paper, but a practical example of applied risk management research that investigates the South African banking industry's compliance with BCBS 239 in terms of making better risk-based decisions. The findings indicate that the banking sector in South Africa has some challenges when it comes to the risk reports complying with the BCBS 239 principles. Though each bank is free to interpret the BCBS 239 principles in line with its own set of standards, the D-SIBs have adopted Basel's suggested risk reporting procedures. The fact that each bank provides the information in a different way means that there are big variations in the risk reports.

These findings are crucial for understanding how these financial institutions will be able to withstand risks and tumultuous changes during any potential crisis by putting the BCBS 239 principles into practice. Data management, including corresponding data and IT infrastructure, are also important.

APPENDICES

Appendix A

Appendix A. Initial Codebook.

No	Code	Code description	Examples from literature	Sources
1	Principle	A guideline	• "This paper presents a set of principles to strengthen banks' risk data aggregation capabilities and internal risk reporting practices (the Principles). " • "In PwC's view, all banking institutions should be considering the principles whether explicitly for regulatory compliance purposes or implicitly for enhancing key aggregation and reporting capabilities." • "The study consolidates existing theory on Basel Committee 239 regulation, namely by merging literature focusing, on one hand, the principles that compose the standard and, on the other hand, the suggested individual best-practices for implementing it."	(BCBS, 2013), (PwC, 2017), (Martins et al., 2022)
2	Risk data aggregation	To be able to compare performance to risk appetite and tolerance, the bank must define, collect, and process risk data in accordance with its risk reporting standards. Sorting, combining, or dissecting data sets are examples of this .	• "Many in the banking industry recognise the benefits of improving their risk data aggregation capabilities and are working towards this goal." • "There is a significant consensus within existing literature that banks must ensure a continuous development of their skill set on what concerns risk data aggregation and risk reporting, mainly due to the recent events related to the global financial crisis that were the final proof that the banking system has little to none ability to reach accurate risk data in a systematic, efficient and effective manner"	(BCBS, 2013), (Martins et al., 2022)
3	Risk reporting	A method of identifying risks tied to or potentially impacting an organisation's business processes.	• "These risk reporting capabilities should also allow banks to conduct a flexible and effective stress testing which is capable of providing forward-looking risk assessments." • "Main findings indicate that the risk reporting differences found across the years of analysis are not statistically significant." • "Risk reporting is the vehicle for communicating the value that the Risk function brings to an organisation."	(BCBS, 2013), (Azevedo et al., 2022), (PwC, 2011)

No	Code	Code description	Examples from literature	Sources
4	Enterprisewide risk management (ERM)	The process of identifying potential events that may affect the group negatively, managing risk so that it remains within the risk appetite of the group, and providing reasonable assurance with regard to the achievement of the goals of the group. The board of directors, management and other personnel drive this process and apply it in strategy setting throughout the group.	• "The longer-term response of regulators is focused on implementing more robust enterprise risk management (ERM) frameworks and technology infrastructures." • "system described in this paper provides the foundation for complying with BCBS 239 by creating a true enterprise risk management (ERM) system. It should become the framework for effective risk governance and improvements in risk culture."	(Grody & Hughes, 2016a), (Grody & Hughes, 2016b)
5	Risk governance	"the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks."	• "BCBS 239 effectively sets the parameters for enterprise risk management (ERM) and provides the foundation on which risk governance and risk cultures can positively evolve" • "the business risks inherent in banking would lead bank boards of directors, in the interest of their shareholders, to establish their own internal risk governance systems."	(Grody & Hughes, 2016b), (Dill, 2019)
6	Compliance	Complying with rules, laws, and guidelines set by the national regulator.	• "Supervisors should periodically review and evaluate a bank's compliance with the eleven Principles above." • "It has taken the industry and supervisors time to work through these challenges and agree what achieving full compliance means and how to achieve it." • "A detailed questionnaire including benchmark information and structured deliverables foster an efficient and focused assessment of the compliance status."	(BCBS, 2013), (PwC, 2017), (KPMG, 2016)
7	Three Lines of Defence (3LoD)	An effective governance operating model that enables the banks' Board of Directors and management to carry out and monitor the affairs of the group to meet the obligations of the group to its depositors, regulators and shareholders with the aim of creating and protecting value sustainably. The 3LoD defines risk management, risk oversight and assurance roles across businesses and functions of the group.	• "validation should be conducted separately from audit work to ensure full adherence to the distinction between the second and third lines of defence, within a bank's internal control system." • "New documentation also needs to satisfy independent validation and compliance assessments by second and third-line-of-defence teams." • "Bank regulators have endorsed the 3LOD model, which the industry had developed shortly after the GFC to more systematically manage operational risk in financial institutions. Considered a best-practice standard by the BCBS, 3LOD has global application."	(BCBS, 2013), (PwC, 2016), (Dill, 2019)
8	Accuracy	Closeness of agreement between a measurement or record or representation and the value to be measured, recorded or represented.	• "Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated." • "Most of the reports are automated with clear and reliable source data. Manual reports are either in the process of being automated, or contain appropriate controls to ensure report accuracy."	(BCBS, 2013), (BIS, 2020), (Grody & Hughes, 2016b), (Deloitte, 2019)

No	Code	Code description	Examples from literature	Sources
			• "also function as a control The aggregate algorithms also function as a control mechanism to prove the accuracy of reports." • "To ensure accuracy of the reports: a) Develop automated check functions, on reasonableness and on validations b) Develop procedures for, reporting"	
9	Comprehensiveness	Extent to which risk reports include or deal with all risks relevant to the firm.	• "Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients."	(BCBS, 2013)
10	Clarity and usefulness	The ability of risk reporting to be easily understood and free from indistinctness or ambiguity.	• "Risk management reports should communicate information clearly and concisely. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. " • "these reports should be developed in line with the recipient's information needs."	(BCBS, 2013), (Martins et al., 2022)
11	Frequency	The rate at which risk reports are produced over time.	• "The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank." • "To ensure further control, risk reports should be produced at a higher frequency during stress or crisis moments."	(BCBS, 2013), (Martins et al., 2022)
12	Distribution	Ensuring that the adequate people or groups receive the appropriate risk reports.	• "Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained." • "At the same time risk management reports should be distributed to the entire set of relevant parties, the inherent confidentiality must be always assured."	(BCBS, 2013), (Martins et al., 2022)
13	Risk appetite	A description of what type and how much risk the group is willing to take on or keep taking on in executing its strategy. The group expresses risk appetite both quantitatively, using risk measures such as economic	• "Risk appetite is the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders" as defined by the Senior Supervisors Group report," • "BCBS 239 requires that banks are able to provide the group board with an aggregate view of the organisation's risk profile relative to	(BCBS, 2013), (PwC, 2016)

No	Code	Code description	Examples from literature	Sources
		capital and risk limits, and qualitatively in terms of policies and controls.	its risk appetite (not a single metric but split by risk types and defined appetite metrics/limits). SA banks should consider whether the siloed or business unit level form of reporting will enable them to fully meet the Principles, i.e. give them the ability to properly aggregate data up to group/ bank level."	
14	Risk exposure	Means how much risk being taken on, described in terms of how likely the risk event(s) are to happen and their impact on the goals.	• "The principles are designed to support banks' efforts to: Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level." • "At least one member must have experience in identifying, assessing, and managing risk exposures of large, complex firms. The chair must be an independent director."	(Chakravorty, 2015), (Dill, 2019)
15	Risk universe	The complete picture of the risks across all business lines, functions, geographical locations and legal entities of the group. These risks are captured through the risk identification process. A qualitative list of the key risks that the group faces is kept.	• "Risk management reporting must comprehend the entire scope of material risk areas within the bank." • "Risk management reports should include exposure and position information for all significant risk areas (eg credit risk, market risk, liquidity risk, operational risk) and all significant components of those risk areas (eg single name, country and industry sector for credit risk). Risk management reports should also cover risk-related measures (eg regulatory and economic capital)." • "Reports should identify emerging risk concentrations, provide information in the context of limits and risk appetite/tolerance and propose recommendations for action where appropriate."	(Martins et al., 2022), (BCBS, 2013)
16	BCBS 239 Full Compliance	A status where a bank has received full compliance of the regulation BCBS 239	• "Although it is not possible to establish an action plan generic enough to ensure full compliance with BCBS 239 to the entire set of banks, based on the previous experience of other entities, by combining the existing scientific and grey literatures, it is possible to outline a sequence of steps that, when effectively completed, provide the institution with the ability to operate in accordance with the regulations." • "All institutions subject to the Principles should ensure they have clear definitions of full compliance, with tangible measures. Banks must also define their own criteria and minimum standards for remaining fully compliant."	(Martins et al., 2022), (PwC, 2017)

Appendix B

Appendix B. Full codebook based on documents from the banks under study.

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	**Bank B**	**Bank C**	**Bank D**	**Bank E**
1	Principle	A guideline	"In 2013, the BCBS published regulations (BCBS 239) pertaining to the principles for risk data aggregation and risk reporting (RDARR). The Group's risk data aggregation capabilities and risk reporting practices are aligned with the principles of BCBS 239."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under Basel Committee on Banking Supervision (BCBS) Standard number 239."	"BCBS 239 was published in January 2013, setting out principles to strengthen banks' risk data aggregation capabilities and internal risk reporting practices. In turn, effective implementation of the principles is expected to enhance banks' risk management and decision-making processes. Domestic systemically important banks (D-SIBs) were required to comply with the principles by 1 January 2017."	"BCBS 239: Principles for Effective Risk Data Aggregation and Risk Reporting was issued in January 2013. The principles aim to strengthen banks' risk management practices by improving their RDARR practices. Complying with the principles will improve the ability of banks to provide rapid and comprehensive risk data by legal entity and business line. This will ultimately enhance banks' decision-making processes and improve their resolvability. This has been incorporated into local bank regulations through Directive 2/2015, which require D-SIBs to comply with the principles from 1 January 2017."	"We manage non-financial risks under the umbrella of operational risk, by adopting the sound principles of operational risk management in our non-financial risk framework that drives the standardised management of all non-financial risk types."
2	Risk data aggregation	To be able to compare performance to risk appetite and tolerance, the bank must define, collect, and process risk data in accordance with its risk reporting standards. Sorting, combining, or dissecting data sets are examples of this.	"Internal and external data is utilised in meeting regulatory requirements and the management of risk. The Group enters into selected data and analytics partnerships with third parties to enhance and heighten its understanding of customers. Internal data is owned and managed by the respective business units with regular	"Generate accurate, reliable and up-to-date risk data across the banking group activities to identify and report risk exposures, concentration and emerging risks."	"Risk reports to the board, board risk committees, segment/ operating business risk committees and senior management include the following: • risk exposure and risk-adjusted business performance; • feedback on implementation and monitoring of risk management processes; • comparison of risk management performance against risk	"The risk appetite, risk profile and risk exposures are reported regularly to the board and senior management through various governance committees and reviewed annually as part of the three-year group business plan. In addition to the core risk appetite metrics, a large variety of risk appetite metrics are operated within the board-approved risk appetite targets. The full	"Risk reports are compiled at business unit level and are aggregated to the enterprise level for escalation through the governance structures based on materiality."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
			assessment of data quality via their respective risk governance structures. All key datasets are subject to the requirements of the Group's data and records management policies and standards. The content and level of aggregation are adjusted to suit the needs of each committee."		appetite, limits and indicators; • periodical reviews of progress against and deviations from the risk management plan; • changes in the external or internal environment and their potential impact on the group's risk profile; • the impact of climate change on the risk profile of the group; • an assessment of whether risk responses are effective and efficient in design and operation; • tracking of the implementation of risk responses; • analysis and lessons learnt from significant audit findings, changes, trends, successes, failures and events; and • the identification of emerging risks. The data strategy is designed through the lens of risk and data capabilities and in support of the group's integrated data architecture. Risk data governance has been incorporated into the overall risk management framework, supported by a culture of accountability for data set by executive management. "	suite of risk appetite metrics and qualitative statements is defined at each level of tiered governance for different risk types and monitored regularly by relevant oversight risk committees and the board, if appropriate. All (tier 1) core risk appetite metrics are being tracked within the board-approved risk appetite targets at 31 December 2022 with the exception of those related to cyberrisk (two out of 23 metrics) – management action is in place to manage the risk accordingly."	

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
3	Risk reporting	A method of identifying risks tied to or potentially impacting an organization's business processes.	"The objective of risk reporting is to provide timeous, accurate, comprehensive and useful information to the Board and senior management to facilitate informed decision-making. Board and senior management risk committees determine their requirements in terms of content and frequency of reporting under both normal and stressed conditions. Risk reporting processes flow from the business unit and relevant risk committees to the ERC and thereafter to Board committees."	"Risk reporting is clear, concise and puts management and the board in a position to make informed risk decisions."	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"Balance Sheet Management (BSM) provides strategic direction, insight and motivation in managing capital risk to the Group Assets and Liabilities Management and Executive Risk Committee (ALCO) through appropriate risk reporting and analytics and by providing strategic input within the group's defined risk appetite."	"Risks are reported and discussed in the risk governance structures and executive management committees. Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."
4	Enterprisewide risk management (ERM)		The process of identifying potential events that may affect the group negatively, managing risk so that it remains within the risk appetite of the group, and providing reasonable assurance with regard to the achievement of the goals of the group. The board of directors, management and other personnel drive this process and apply it in strategy setting throughout the group.	"The Enterprise Risk Management Framework (ERMF): • Outlines the approach to the management of risk and provides the basis for setting frameworks and policies, and establishing appropriate risk practices throughout the Group. • Defines the risk management process and sets out the activities, tools, techniques and the operating model to ensure material risks can be identified and managed. • Ensures appropriate responses are in place	"As part of the reporting, interrogation and control processes, Enterprise Risk Management (ERM) drives the implementation of more sophisticated risk assessment methodologies through the design of appropriate policies and processes, including the deployment of skilled risk management personnel in every business. ERM ensures (and Group Internal Audit (GIA) provides periodic assurance) that all policies, processes and systems are adequately designed and effectively implemented for pertinent risk information to be accurately captured, evaluated and escalated	"The Group's Enterprisewide Risk Management Framework (ERMF) enables the group to identify, measure, manage, price and control its risks and risk appetite, and relate these to capital requirements to help ensure capital adequacy and sustainability, thereby promoting sound business behaviour by linking these aspects with performance measurement and remuneration practice. "	"The second line of defence directs the definition of the enterprisewide risk management programme. They facilitate execution of risk lifecycle activities and provide expert advice, guidance and support to the first line of defence team. They have oversight of the implementation and effective execution of risk and returns decisions within the set risk appetite and target strategy."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
				to protect the Group and its stakeholders. • Sets out principal risks and assigns clear ownership and accountability for these risks."	appropriately and timeously"		
5	Risk governance	"the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks."	"The Group identifies and assesses risks and opportunities arising from internal and external environments, and proactively identifies emerging risks. To ensure effective risk management, our consolidated response is monitored as follows: • Uphold the risk governance structure at Group, country, business and Group functions, with clear Board escalation and oversight."	"We have an extensive, multi-layered structure to govern risk, however, our board is ultimately responsible for risk management. This includes ensuring that risks are adequately identified, measured, managed and monitored and that good governance is maintained. The board monitors the implementation of the risk strategy, approves the risk appetite and ensures that risks are managed within tolerance levels."	"The risk governance and management structure is set out in the group's risk management framework. As a policy of the board, the group risk management framework delineates the roles and responsibilities of key stakeholders in business, support and control functions across the group. “	"The board of directors has the ultimate responsibility for the group's business strategy, financial soundness, governance, risk management and compliance and has allocated oversight of risk governance to the Group Risk and Capital Management Committee (GRCMC). This includes, among other things, the overall effectiveness of the process relating to corporate governance, internal controls, risk management, capital management and capital adequacy."	"Our risk management system is governed by appropriately mandated governance committees and fit-for-purpose governance documents. Governance committees are in place at both a board and management level. These committees have mandates and delegated authorities that are reviewed regularly. Members have the requisite skills and expertise to manage risk."
6	Compliance	Complying with rules, laws, and guidelines set by the national regulator.	"Manage the funding and high-quality liquid assets (HQLA) position in line with the Board-approved framework and ensure compliance with regulatory requirements."	"We believe that RDARR is more than a compliance requirement and that mature RDARR capabilities add value to our understanding and management of risk."	"A programme is in place to implement RDARR requirements within the agreed compliance timelines, and regular updates are provided to the Prudential Authority (PA). The Group's implementation of BCBS 239 resulted in enhanced risk management and decision-making processes, and risk data maturity. Focus has shifted from remediation of	"RDARR compliance for the bank's key tranche 3 risk types. (AML risk, Conduct risk, and cyberrisk) met the RDARR compliance requirements for the December 2022 deadline. This follows compliance already having been met in December 2019 for the bank's key risk types (credit risk, market risk, operational risk, liquidity risk, investment risk and IRRBB). The RDARR compliance journey	"Risk management reports comply with the standards set out by BCBS239."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
					compliance gaps to maintaining compliance."	does not end with regulatory compliance, with the focus now shifting to maintaining compliance through BaU operations."	
7	Three Lines of Defence (3LoD)	An effective governance operating model that enables the banks' Board of Directors and management to carry out and monitor the affairs of the group to meet the obligations of the group to its depositors, regulators and shareholders with the aim of creating and protecting value sustainably. The 3LoD defines risk management, risk oversight and assurance roles across businesses and functions of the group.	"The Group applies a three lines of defence model in support of the combined assurance model to govern risk across all businesses and functions. The ERMF assigns specific responsibilities to each line of defence."	"the focus remained on improving the risk maturity and clearly delineating the lines of defence in our risk management framework. • 1st line of defence is Risk ownership. • 2nd line of defence is Risk control. • 3rd line of defence is independent assurance (internal audit)"	"The group obtains assurance that the principles and standards in the operational risk management framework are adhered to by the three lines of defence model, which is integrated in operational risk management. In this model, business units own the operational risk profile as the first line of defence. In the second line of defence, ERM is responsible for consolidated operational risk reporting, policy ownership and facilitation, and coordination of operational risk management, measurement and governance processes. GIA, as the third line of defence, provides independent assurance on the adequacy and effectiveness of operational risk management processes and practices."	"The 3LoD Model forms an important part of the ERMF, which provides the structure in which the group operates. If risks taken are not managed and controlled effectively, it can prevent the group from achieving its strategic objectives. The roles and responsibilities of the 3LoD Model provides a structure for considering risk and control, to ensure that they are appropriate and managed effectively. The 3LoD Model provides guidance as to the appropriate organisational structure to be implemented, assigning roles and responsibilities to parties that will increase the effective management of risk and controls."	"The three lines of defence model is leveraged to maintain a strong risk culture with an emphasis on doing the right business, the right way."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
8	Accuracy	Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.	"The objective of risk reporting is to provide timeous, accurate, comprehensive and useful information to the Board and senior management to facilitate informed decision-making."	"Ensure reports are accurate, convey aggregated risk data and are reconciled and validated"	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"The Group has acted in good faith and has made every reasonable effort to ensure the accuracy and completeness of the information contained in this document,"	"Risk information is subject to strong data and reporting controls. It is integrated into all business reporting and governance structures. Our governance structure enables oversight and accountability through appropriately mandated board and management committees. "
9	Comprehensiveness	Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.	"The ERMF includes risks taken by the Group that are foreseeable and material enough to merit establishing specific Group-wide control frameworks. These are grouped into eight principal risks1 that account for the vast majority of the total risk faced by the Group. • Financial principal risks – Credit risk – Market risk – Capital and liquidity risk – Insurance risk • Non-financial principal risks – Operational and resilience risk – Compliance risk • Risks straddling both financial and non-financial risks – Model risk – Strategic and sustainability risk	"The risks we manage • Credit risk • Operational risk • Market risk • Capital and liquidity risk • Reputational risk Operational risk consists of the following categories: • Fraud risk • IT risk • Information risk • Compliance and legal risk • Conduct risk • Model risk • Supplier and third-party risk • Environmental risk. Market risk consists of the following categories: • Interest rate risk • Insurance risk • Equity and currency risk • Hedging risk. "	"The following table illustrates the core competencies that form part of the group's risk management processes across key risk types and components. Risk limits for all risk types are integral to risk management and are instrumental in constraining risk taking within appetite. Qualitative risk appetite principles are designed to support a strong risk culture in the group and provide a foundation to ensure appropriate behaviour and conduct. The risks, and the roles and responsibilities of the various stakeholders across business, support and control functions are described in the group's risk management framework. • Liquidity risk ▪ Funding liquidity risk ▪ Market liquidity risk • Credit risk ▪ Settlement risk	"For 2023 our top 10 risks, indicated below, are selected as top-of-mind risks rather than business-as-usual principal risks. 1. Business Risk (Including Geo-Political and Country/Sovereign Risks) 2. Credit Risk 3. Cyberrisk 4. People Risk 5. Strategic Execution Risk 6. Organisational Resilience Risk 7. Operational risk (including emerging-IT, digital transformation and data risks) 8. Climate Risk 9. Reputational and Conduct Risks 10. Capital Risk In addition to major traditional risks, various emerging risks continue to grow in importance and include those with impacts that have not yet significantly materialised in the organisation, notwithstanding that they are very real and increasingly relevant. The group remains vigilant in	"Our risk universe represents the risks that are core to our financial services business. We organise these into strategic, financial and non-financial categories and biennially identify key enterprise risks. Strategic risks • Strategy position risks • Strategy execution risks • Reputation risks • Financial risks • Credit risks • Country risks • Market risks • Insurance risks • Funding and liquidity risks Non-financial risks: • Business disruption risks • Compliance risks • Conduct risks • Cyber risks • Environmental, Social and Governance (ESG) risks • Financial accounting risks • Financial crime risks • Information risks • Legal risks • Model risks • People risks

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
			The Board annually reviews and approves the ERMF on recommendation by the GRCMC. The Group Chief Executive grants authority and responsibility to the GCRO to ensure the principal risks are managed under appropriate risk control frameworks and within the Board-approved risk appetite and risk budget."		▪ Country risk ▪ Credit default risk ▪ Concentration risk ▪ Securitisation risk ▪ Large exposure risk • Counterparty credit risk ▪ Pre-settlement risk • Traded market risk ▪ Interest rate risk in the trading book ▪ Traded equity and credit risk ▪ Foreign exchange risk ▪ Commodity risk • Non-traded market risk ▪ Interest rate risk in the banking book ▪ Structural foreign exchange risk • Equity investment risk ▪ Price risk ▪ Equity investment liquidity risk • Climate risk ▪ Physical risk ▪ Transition risk • Operational risk (including information technology (IT) and cyber risk) ▪ Internal and external fraud risk ▪ People risk ▪ Information technology risk ▪ Information risk ▪ Legal risk ▪ Business resilience risk ▪ Process risk ▪ Cyber risk ▪ Third-party risk	monitoring the potential impact of these risks, constantly scanning global and local environments for flags or triggers, as the evolution of the potential impact of these risks is highly uncertain and our response is critical to ensuring survival and sustainable growth."	• Physical assets, safety and security risks • Tax risks • Technology risks • Third-party risks • Transaction risks "

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
					• Compliance and conduct risk ▪ Compliance risk ▪ Conduct risk ▪ Financial crime risk • Other risks ▪ Insurance risk ▪ Model risk ▪ Tax risk ▪ Strategic risk ▪ Business risk: • Margin and volume changes • Expansion activities ▪ Environmental and social risk: ▪ Social risk • Nature and biodiversity risks ▪ Step-in risk ▪ Reputational risk"		
10	Clarity and usefulness	Risk management reports should communicate information clearly and concisely. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Reports should include meaningful information tailored to the needs of the recipients.	"Reports provide key insights into developing industry, sector and product trends and incorporate agreed management actions to modify behaviour and strategy in accordance with specific findings."	"Risk reporting is clear, concise and puts management and the board in a position to make informed risk decisions. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements"	"The group's robust and transparent risk-reporting process enables key stakeholders (including the board and senior executives) to get an accurate, complete and reliable view of the group's financial and non-financial risk profile and enables management to make appropriate strategic and business decisions."	"These enhancements to Group's modelling and risk management tools allow the bank to stay ahead and respond to a crisis appropriately. More specifically, they enable the bank to make informed strategic decisions in these unprecedented times through: • delivering analysis and insights to enable well-informed decision-making; • enabling us to update stress-testing models in a tightly controlled manner to ensure they are reflective of the new reality; • enabling us to upgrade forecasting tools and management information to facilitate management response; and	"Risk information is subject to strong data and reporting controls. It is integrated into all business reporting and governance structures. Our governance structure enables oversight and accountability through appropriately mandated board and management committees. The three lines of defence model is leveraged to maintain a strong risk culture with an emphasis on doing the right business, the right way."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
						• facilitating production of future information so that outcomes are as accurate as possible and without undue procyclicality."	
11	Frequency	The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.	"Board and senior management risk committees determine their requirements in terms of content and frequency of reporting under both normal and stressed conditions."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under Basel Committee on Banking Supervision (BCBS) Standard number 239. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements."	"'Regular risk reporting enables the board, senior management, the risk, compliance and capital committee (RCCC) and relevant subcommittees to evaluate and understand the level and trend of material risk exposures and their impact on the group's capital position, and to make timely adjustments to the group's future capital and strategic plans."	"The risk appetite, risk profile and risk exposures are reported regularly to the board and senior management through various governance committees and reviewed annually as part of the three-year group business plan."	"Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
12	Distribution	Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.	"Risk reporting processes flow from the business unit and relevant risk committees to the ERC and thereafter to Board committees."	"To ensure we report the right risks to the right people at the right time, the group adopted the Basel principles for effective RDARR practices under Basel Committee on Banking Supervision (BCBS) Standard number 239. Risk reporting practices ensure reports are comprehensive, clear, useful and set at a frequency which meets the recipients' requirements."	"Reporting of risk information follows the governance structure. Specialist risk committees and segment/ operating business risk and compliance committees report to the RCCC and its subcommittees. Relevant executive committees receive reports on the risk profile, material risk exposures, risk-adjusted business performance and key risk issues. The RCCC submits reports to the board and highlights control issues to the audit committee."	"The board of directors has the ultimate responsibility for the group's business strategy, financial soundness, governance, risk management and compliance and has allocated oversight of risk governance to the Group Risk and Capital Management Committee (GRCMC). The group's sound governance and risk management are underpinned by the Three-lines-of-defence (3LoD) Model, based on 'function' rather than 'location' in the organisation."	"Risks are reported and discussed in the risk governance structures and executive management committees. Risk reports are prepared for the board committees, the regulator and other stakeholders on a regular basis."
13	Risk appetite	A description of what type and how much risk the group is willing to take on or keep taking on in executing its strategy. The group expresses risk appetite both quantitatively, using risk measures such as economic capital and risk limits, and qualitatively in terms of policies and controls.	"The Group's risk appetite: • Specifies the level of risk the Group is willing to take in pursuit of its strategy. • Considers all principal and material risks individually and, where appropriate, in aggregate. • Consistently measures, monitors, and communicates the level of risk for different risk types, expressed in qualitative and quantitative terms. • Describes agreed parameters for the Group's performance and	"Our risk appetite is the level of risk we are willing to accept while pursuing our objectives. As expected from a banking group, our highest exposure is in the credit risk environment, where we define the risk appetite level through our pricing model and pursue a targeted Return on Equity (ROE) on all credit products. For operational risk events, we have a low-risk appetite, which means that the group will not knowingly expose itself to such risk. However, for risk events related to discrimination,	"The Group's risk appetite is the aggregate level and the type of risks the group is willing and able to accept within its overall risk capacity in the execution of its strategy. It is captured by a number of qualitative principles and quantitative measures. The risk appetite framework, in conjunction with the risk-return framework, aims to ensure that the group maintains an appropriate balance between risk and reward. Return targets and risk appetite limits are set to ensure the group achieves its overall strategic objectives, namely to: • deliver long-term franchise value;	"Risk appetite is an articulation and allocation of the risk tolerance or quantum of risk the group is prepared to accept in pursuit of its strategy. Risk appetite is integrated into the group's strategic and business planning process and is approved by the board and monitored by varying levels of senior management, with ongoing oversight and coordination by Group Risk. Risk appetite is guided by the group's Risk Appetite Framework (RAF), which sets the principles for decision-making and risk-taking that are aligned with our strategic focus areas."	"Risk appetite is an expression of the amount or type of risk we are willing to take in pursuit of our financial and strategic objectives, reflecting our capacity to sustain losses and continue to meet our obligations as they fall due, under both normal and a range of stress conditions. Risk appetite guides strategic and operational decisions and is reviewed annually."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
			resilience under varying levels of financial stress and volatility to earnings, capital adequacy, leverage, and liquidity. Is considered in key decision-making processes, including business planning, mergers and acquisitions, new product approvals and business change initiatives. "	we adopt a zero-tolerance attitude."	• deliver superior and sustainable economic returns to shareholders within acceptable levels of volatility; and • maintain balance sheet strength.”		
14	Risk exposure	Means how much risk being taken on, described in terms of how likely the risk event(s) are to happen and their impact on the goals.	"Key risk scenarios are a summary of the extreme potential risk exposure for each risk in the suite of operational and resilience risks and includes quantitative and qualitative assessments of the potential frequency of risk events, the average size of losses and extreme scenarios. The assessments consider internal and external loss experiences, key indicators, critical process assessments (CPAs) and other relevant risk information. Factors incorporated into the analysis of potential extreme scenarios include: • The circumstances and contributing	"The following tables contain an analysis of the credit risk exposure of loans and advances for which an Expected Credit Loss (ECL) allowance is recognised. The gross carrying amount of financial assets below also represents the group’s maximum exposure to credit risk on these assets. "	"The group’s risk exposure through its association with and usage of third parties, in particular vendors, remains an area of focus. Cyberattacks on and negative media coverage of third parties/vendors used by the group persisted during the year under review. While instances of poor vendor service was experienced and subsequently remediated, these did not have a material impact on service to group stakeholders. Ongoing monitoring and management of key vendors remains a priority."	"developing appropriate metrics to provide insight into risk exposure trends and building in escalation triggers to alert and prompt action via indicators [key risk indicators (KRIs), key control indicators (KCIs), key performance indicators (KPIs)];"	"Risk exposures are reported on a regular basis to the board and senior management through our governance committees."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
			factors that could lead to an extreme event. • The potential financial and non-financial impacts (e.g., reputational damage). • The controls and other mitigants that seek to limit the likelihood of such an event occurring, and the actions that would be taken if the event were to occur (e.g., crisis management procedures, business continuity or disaster recovery plans, etc.)."				
15	Risk universe	The complete picture of the risks across all business lines, functions, geographical locations and legal entities of the group. These risks are captured through the risk identification process. A qualitative list of the key risks that the group faces is kept.	"ERMF and frameworks include risk appetite and stress testing, as well as the 8 principal risks. These describe the high-level Group-wide approach for a specific risk and are mandatory for each of the principal risks identified in the ERMF. These are grouped into eight principal risks that account for the vast majority of the total risk faced by the Group. • Financial principal risks • Non-financial principal risks	"Our risk universe consists of 6 risk categories that are managed by the EXCO, the Risk and capital management committee (RCMC), the Risk committee (RISCO), the Retail bank credit committee (RCC), the Business bank credit committee (BCC), the Asset and liability committee (ALCO) and the Data Steerco. These committees report to the RCMC, which is mandated by the board to oversee risk management."	"A complete view of the group's principal and supporting risk universe is outlined below on this report: • Liquidity risk • Counterparty credit risk ▪ O Pre-settlement risk • Traded market risk • Non-traded market risk • Equity investment risk • Climate risk • Operational risk (including information technology (IT) and cyber risk) • Compliance and conduct risk	"The Group's risk universe is defined, actively managed and monitored in terms of the ERMF, in conjunction with the Capital Management Framework and its subframeworks, including the Economic Capital Framework. A summary table of the key risk types impacting the group highlights the mapping of the 17 key ERMF risk types to the 12 quantitative risk types of the Economic Capital [and Internal Capital Adequacy Assessment Process ICAAP)] Framework"	"Our risk universe represents the risks that are core to our financial services business. We organise these into strategic, financial and non-financial categories and biennially identify key enterprise risks. These top enterprise risks require focused management because they represent material impacts to the strategy. We regularly scan the environment for changes to ensure that our risk universe remains relevant. The risk universe is managed through the lifecycle from identification to reporting. Our assessment process includes rigorous quantification of risks under normal and stressed conditions up to, and including, recovery and resolution."

No.	Code	Code Description	Examples of codes from risk reports by the D-SIBs				
			Bank A	Bank B	Bank C	Bank D	Bank E
			• Risks straddling both financial and non-financial risks Credit, market, capital and liquidity, and insurance are collectively known as financial principal risks. Strategy and sustainability (including reputational) and model risk are known as principal risk types which straddle both financial and non-financial risk. The remaining risks are referred to as non-financial principal risks."		• Other risks “		
16	BCBS 239 Full Compliance	A status where a bank has received full compliance of the regulation BCBS Standard 239	Full compliance status not observed	Full compliance status not observed	"GIA validated the status of all material risk types and the group is fully compliant with the requirements of BCBS 239 for the standardised approach for measuring counterparty credit risk (SA-CCR), achieving full compliance by 31 December 2022 along with all other principal risk types."	"RDARR compliance for the bank’s key tranche 3 risk types. (AML risk, Conduct risk, and cyberrisk) met the RDARR compliance requirements for the December 2022 deadline. This follows compliance already having been met in December 2019 for the bank’s key risk types (credit risk, market risk, operational risk, liquidity risk, investment risk and IRRBB)."	Full compliance status not observed