CHARTERS, FRAMEWORKS AND POLICIES FOR REVIEW

15th February 2021

Notice is hereby given that a meeting for reviewing Frameworks and Policies of FNB Moçambique will be held via Microsoft Teams (electronic means), On 15th February 2021 at 14:30.

APOLOGIES: None

New Governance Documents

Frameworks and Policies Summaries

1. Information Governance Committee Charter

Comment	Approving Committee	Status	Page
The purpose of this Charter is to communicate the primary responsibilities and delegated authority of the IGC, ensuring that all relevant stakeholders optimally manage their information resources effectively in support of the Bank´s objectives and strategies.	MRCC	New	n/a

2. Information Governance Framework

Comment	Approving Committee	Status	Page
This framework is a sub framework of the Business Performance and Risk Management Framework and is a management tool to ensure business success through the use of reliable information with the aim of optimizing information value and supporting effective management and mitigation of information-related risks. The purpose of the IGF is to: • create a common reference and stipulate key information governance requirements across the Bank; • ensure that FNBM´s information and records are maintained to a level of integrity and quality sufficient to ensure regulatory compliance and effective operation of the business; • create a framework for the establishment and management of information management principles, policies, standards, processes and guidelines; • define key roles and responsibilities involved in the management of information and oversight thereof within the organization; • oblige management to adopt and adhere to a set of minimum standards and criteria for the management of information; and assist the board and senior management to discharge their duties in relation to information management in accordance with legal and regulatory requirements	MRCC	New	n/a

3. ESRA Policy

Comment	Approving Committee	Status	Page
ESRA (Environmental and Social Risk Assessment) forms part of the	MRCC	New	n/a

"Desirability Test" of the credit approval application process. Environmental and social risks are risks that relate to specific activities and sectors which increase the probability that commercial and industrial activities and human intervention will cause and lead to degradation of the environment or have a significant social impact. This assessment ensures the management of the environment and the consequential risk to the business of the client and, ultimately to the bank. These risks are managed through conducting a due diligence process through the Environmental and Social Risk Assessment (ESRA) tool, in alignment with The Equator Principles (EP). The benefits of implementation of an environmental and social risk assessment process will provide the bank with protection against typical risks associated with investment and lending This policy is an extension and not a substitution of the FirstRand Guideline for the Management of Environmental and Social Risks in financing but is specific to FNB Mozambique.			

4. Monitoring Operating Procedures

Comment	Approving Committee	Status	Page
The monitoring standards and operational procedures are applicable to the FNBM, it's as they establish the minimum standards and implement the operating standards to which a monitoring function must adhere. These operating procedures are developed in support of the FNBM Monitoring Standards as approved in line with the RCRM Manual. Should additional procedures or a deviation from the monitoring standards and/or operating procedures be required, this must be tabled at the Monitoring Centre of Excellence (MCOE) Work Group. FNBM Monitoring Standards and Operating Procedures recommendations are discussed, agreed and approved by the Monitoring Centre of Excellence (MCOE) Work Group. The LMT Sub Committee are informed for ratification. The standards will be updated accordingly in line with the annual revision of the CCRC Frameworks Committee. Where it is established, that the deviation is only applicable for a single instance, such a deviation must be approved by the (MCOE) Work Group, the standards will not be amended, and no referral will be done to LMT Sub Committee.	MRCC	New	n/a

5. Write-off Process

Comment	Approving Committee	Status	Page
The purpose of this document is to outline the write-off process – relating to: • Mandatory / regulatory (i.e. Aviso 16) write offs • Dormant account write-offs (negative balances) • Debt relief/settlement agreement write offs	MRCC	New	n/a

6. PIP Management Process

Comment	Approving Committee	Status	Page
The purpose of this document is to create awareness on the process of management of property in possession, from purchasing processes and requirements to the step by step guidance on the maintenance of property in possession	MRCC	New	n/a

Notices

Below the list of notices for the perusal of the committee

1. CCTV Notice
2. Customer Notice
3. FNB Employee Notice
4. Supplier Notice
5. Cookie Notice

INFORMATION GOVERNANCE COMMITTEE CHARTER

Document information	Responsibility		
Owner:	*Name, Surname* *Role* *Physical Address* *e-mail*	Monica Souto Chief Risk Officer Prédio JAT, 1º Andar Av. 25 de Setembro, n.º 420, C. Postal 4339, Maputo-Moçambique Monica.souto@fnb.co.mz	
Review and Approval:	*Committee*		*Approval/ Review Date*
	Management Risk and Compliance Committee		
	FNBM Executive Committee		
Chairman´s signature:	Peter Blenkinsop		
Previous approvals	Not applicable as this is the first approval		
Date of next review:	February 2022		
Document version:	1.0		

INTRODUCTION

Reliable information is the backbone of any effective corporate governance system as it is central to decision making, growth, risk management, internal control and reporting systems in FNB Moçambique (*FNBM*).

Information governance is a co-ordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimising information value.

Information governance is an integral part of corporate governance and is ultimately the responsibility of the Board of Directors. In exercising their duty of care, the Directors should ensure that prudent and reasonable steps have been taken with regards to information governance.

To successfully discharge this responsibility, FNBM must be guided not only by relevant Frameworks and Policies and supporting reporting system, but also by an appropriate information governance committee with the purpose of providing the Board and Management with a comprehensive and transparent view of the effectiveness of the information governance mechanisms in the Bank.

The scope of the herein proposed Information Governance Committee (henceforth referred to as "*IGC*" or the "*Committee*") includes specific information governance strategy, policies, reporting and risk requirements, relevant legal and regulatory requirements and select best practices for information asset management.

The purpose of this Charter is to communicate the primary responsibilities and delegated authority of the IGC, ensuring that all relevant stakeholders optimally manage their information resources effectively in support of the Bank´s objectives and strategies.

1. CONSTITUTION OF THE COMMITTEE

The Information Governance Committee is constituted as an in-country Committee with the objective of assisting Management in monitoring information risk by effectively controlling the overall information management and governance within the Bank, as such, serve as a medium of communication and co-ordination with the other risk and governance committees and relevant stakeholders, both local and at Center.

Escalation matters will be reported to the Management Risk and Compliance Committee (henceforth referred to as "*MRCC*").

2. ROLES AND RESPONSIBILITIES

The FNBM Information Governance Committee's primary objective is to discharge responsibilities relative to the governance of information related matters within the Bank.

Specifically, it is the responsibility of this committee to:

- Report to the MRCC on the state of information governance and management;
- Ensure that governance structures are in place to oversee information risk management in the Bank;
- Guarantee inclusion of relevant representation from the business in oversight structures;
- Set and agree on measures and metrics to track the progress of implementation of information governance in FNBM;
- Ensure a strategic approach to and facilitation of the integration of information management into business strategic thinking;
- Ensure that the information processes within the scope of its authority remain appropriately funded;
- Ensure better management of information for the benefit of the business units and functions, risk types, branches, customers, staff in general and other relevant stakeholders;
- Monitor the implementation of appropriate information governance frameworks, policies, standards and guidelines and recommend the framework for approval; and
- Facilitate and monitor the development and implementation of the Bank´s data strategy, and report to the MRCC on the status of implementation;
- Establish sub-committees, forums and/or working groups as specific focus on data management functions is required;
- Ratify decisions made by any sub-committee and act as the point of escalation for any disputes that cannot be resolved by any of the sub-committees, forums or working groups under its oversight;
- Approve any exceptions or waivers from compliance with information governance requirements;
- Maintain a schedule of material breaches or non-compliance to governance, and report these to the MRCC.

3. MEETINGS AND PROCEEDINGS

- The IGC shall meet quarterly, and as and when deemed necessary for the purpose of discharging its obligations as recommended by the chairperson;
- Meeting agendas shall be prepared and distributed in advance, together with the appropriate information to enable IGC members and invitees to prepare for meetings;
- The chairperson shall set the agenda for and preside over meetings;
- The chairperson will ensure that comprehensive minutes are taken at all meetings and that they are approved by the committee and kept on record for future reference or inspection;
- A proper attendance register of the meetings shall be kept; and
- A report on material issues discussed at the meetings shall be submitted to the MRCC.

4. MEMBERSHIP

Committee membership shall be comprised of Senior Management from the Business, Operations and IT.
The Chairperson will be the Chief Risk Officer, with an alternate chair as the Chief Information Officer.

The Committee will count on the permanent membership of the following stakeholders:

- Chief Risk Officer
- Chief Operating Officer
- Chief Information Officer
- Head of Internal Audit
- Chief Compliance Officer
- Enterprise Risk Manager
- Operational Risk Manager
- Business Representative (CCIB)
- Business Representative (Retail and SME)

The following individuals attend the IGC meetings by invitation:

- Head of Human Capital
- Chief Financial Officer

5. QUORUM AND VOTING

A quorum of members must be present before a meeting can proceed. A quorum shall be at least five permanent committee members.
Non-permanent members and invitees present in the meeting are considered non-voting attendees.

6. REVIEW PROCESS

This charter is approved by the Executive Committee. The charter and the effectiveness of the committee will be reviewed at least annually.

7. SECRETARIAT

The Chief Risk Officer shall indicate the resources for secretarial duties, which will consist of the following:

- Schedule the meetings, adequately inviting members and invitees;
- Ensure agreement of agenda items with the Chairperson;
- Document discussions in accurate and concise meeting minutes
- Ensure timely circulation of meeting packs (agenda, approved minutes, main deck and supporting/additional documents) to members and invitees;

*Minutes and actions logs are distributed within 21 days after the meeting.

GLOSSARY

ACRONYM	DEFINITION
FNBM	FNB MOCAMBIQUE
IGC	INFORMATION GOVERNANCE COMMITTEE
MRCC	MANAGEMENT RISK AND COMPLIANCE COMMITTEE

INFORMATION GOVERNANCE FRAMEWORK

(IGF)

Document Version Control

Policy level:	FNBM
Effective date:	16th March 2021
Number of pages:	
Recommended by:	Management Risk and Compliance Committee
Date	March 2021
Approved by:	FNBM Risk, Capital Management & Compliance Committee
Framework Owner	Monica Souto Chief Risk Officer Monica.souto@fnb.co.mz 420, 25 de Setembro, JATI, 1st Floor
Board approval date:	March 2020
Version number:	1.0
Signature	_____ John Macaskill (Chairman)

TABLE OF CONTENTS

1. INTRODUCTION

Information, whether internally generated or that entrusted into our care by our customers, staff or business partners, is a valuable and strategic asset and essential to our business. The information landscape is complex, and it is expected that it will become ever more complex, considering the exponential growth in information, the availability of information on a vast range of devices, big data, advanced analytics, advances in digitization, personalized experience expectations and compliance with ethical use of information.

Laws and regulations are there to guide us around privacy and the use of data, defining to a certain degree the current “no-go” area. However, recent advancements in analytics and data technologies has widened the gap between what is possible and what is legally allowed, changing the balance of power between individuals and the data collectors and processors. Within this gap there are new opportunities as well as risks of public relations disasters and other unintended consequences. And it is within this gap where the ethical questions around what is acceptable are raised.

As data and analytics become a core part of digital business and data is increasingly recognized as an asset, new roles are required and executives and employees’ ability to communicate and understand conversations about data is becoming an integral aspect of most day-to-day jobs. Competency development in the field of data literacy is required support digital strategies and improve business outcomes and employee engagement. This, together with the requirement that boards of directors are held accountable for the governance of information, the use of information as a strategic enabler by competitors and the increased focus on information from a regulatory perspective, reinforces the need to formalize and embed the governance and management of information.

Not all information is equally important . Therefore, we must ensure that we maintain and protect all the information we use and/or store in accordance with its value, sensitivity and the risks to which it is exposed. This must be done in a manner, consistent with business objectives as well as all legal, regulatory, contractual, environmental and operational requirements.

Information governance is FNBM’s coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. Information governance is a corporate governance responsibility, focusing on and directing the management of information by helping to ensure that:

- information principles, policy and standards are set;
- information ownership and accountability are clearly defined and allocated;
- governance structures are in place to set information strategy, information management maturity levels and to monitor key information risks and root causes specific to the data itself;
- legal and regulatory requirements are identified and met;
- sufficient independence is maintained and that proactive and coordinated decisions about information are made for the benefit of the overall Bank;
- data literacy and an information management aware culture is promoted to support effective and ethical use of information;
- information governance workplans are reviewed periodically (at least annually) to confirm that they continue to meet the Group’s and FNBM´s business priorities and needs as they evolve. These workplans must be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities and must be established with the structure, direction, resources, and accountability to provide reasonable assurance that the set objectives will be achieved;

- material data sources are identified and managed as information assets;
- key metrics and key data elements (KDE) are defined clearly and consistently aligned with the Group;
- data flows for material risk data processes are documented, maintained and authoritative and trusted data sources identified;
- information is appropriately classified;
- fit-for-purpose information controls are identified and embedded in business and IT processes;
- vital records are identified and retained in line with regulatory and business requirements;
- material data quality issues are identified, root causes assessed and remediated timeously and sustainably;
- master and reference data are appropriately managed to support effective consolidation, aggregation and integration of shared data across the Bank; and
- information security, data privacy and records management requirements are embedded in all processes.

To manage information effectively, both **proactive** and **reactive** components must be considered when implementing information governance:

- reactive components must deal with deficiencies that are inherent in data and records in the existing databases, data stores and/or paper stores; and
- proactive components must deal with business and IT change and must focus on preventing information issues (e.g. data quality issues, records retrieval issues, unclear business rules and definitions, etc.) when new data, processes and applications are introduced in the Bank.

The Board of Directors (the board) is ultimately responsible for the effective governance of information within the Bank. This Information Governance Framework (IGF) is a policy of the board and prescribes the governance and monitoring structures, key roles, responsibilities and principles which must be implemented and adhered to in order for the board to discharge its obligations in this regard.

The diagram below is a graphical representation of the IGF, making provision for strategic enablers, agreed information management domains, key outcomes, scope and operational enablers.

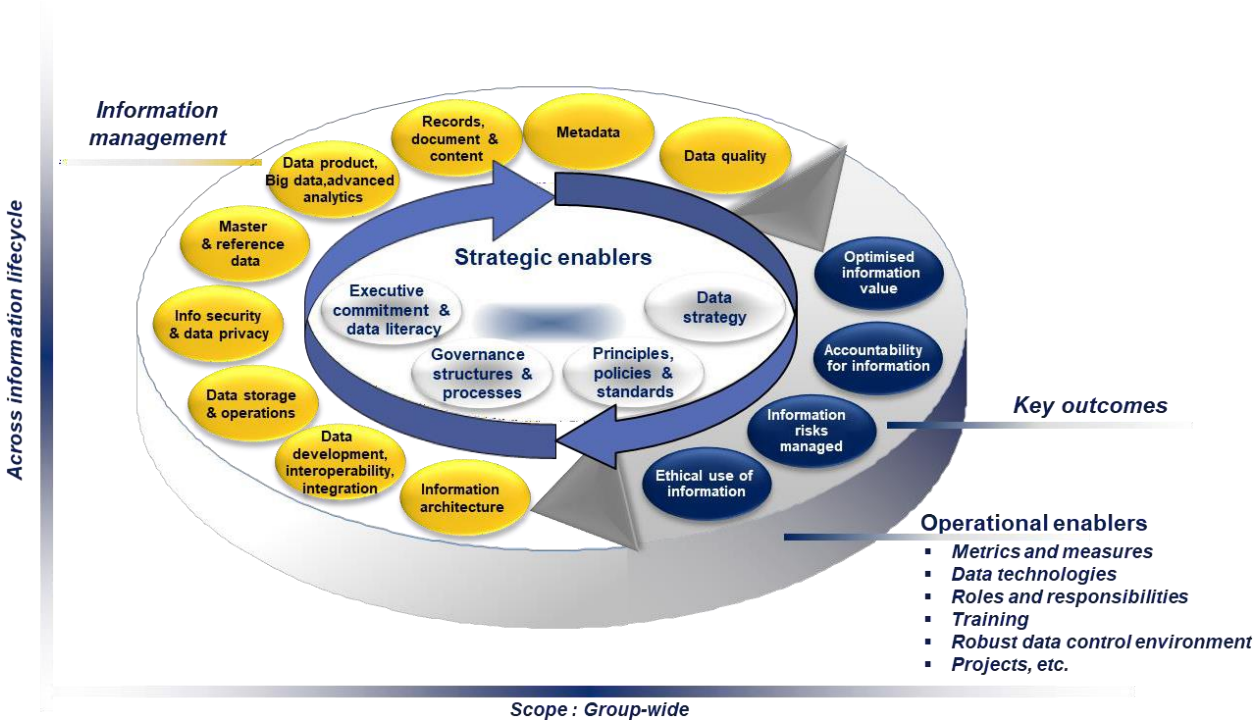


Figure 1: Information Governance Framework

Strategic enablers: The successful implementation of information governance is underpinned by data literacy, which is the ability to locate, read, write, evaluate and communicate data and to derive meaningful conclusions from data. Additionally, this implementation is also underpinned by executive commitment, and directed and enabled by data strategy, sustainable governance structures and supporting processes, information management roles, principles, policies and supporting standards.

Information management: The IGF makes provision for several information management domains to ensure the holistic management of information over time. Please refer to section on *Definitions and key principles* for every domain. Each Business Area must be able to assess and determine a feasible implementation approach. However, the essential nature and the fundamental principles of information management remain the same across FirstRand. Implementation priorities will be discussed and agreed by the information governance committee.

Operational enablers: Efficient operational practices are essential to support and enable effective information management. Operational enablers include training and awareness interventions, metrics and measures, information technologies e.g. data profiling tools, data integration tools (please refer to the Information Architecture Policy and Data Integration Policy), information-related initiatives and projects in support of the information strategy, etc.
Operational enablers are ultimately required for all components of the framework. Implementation across FNBM must be in an incremental fashion, driven by risk appetite, data and business strategy and monitored at information governance committees:

- **Training and awareness**. Targeted information management training and awareness programmes must be developed and monitored to develop and embed required skill sets and improve data literacy;
- **Operating model.** Establish and entrench an operating model(s) to support FNBM´s as well as Group´s business and data strategies. Effective operating models will make provision for the required functions, roles, responsibilities, skills, processes and information forums required on the operational, tactical and strategic levels of the Bank;

- **Controls.** Define and document "fit-for-purpose" controls for all material information assets to ensure appropriate control ownership, escalation, implementation and maintenance of controls;
- **Data stewardship**: Allocation of accountability (i.e. data ownership) for information assets to business leaders, business data stewards and IT custodians of data. Various data stewardship models may be considered for implementation, e.g. by data theme, process, system, function, etc.;
- **Information risk landscape**. Compile a consolidated view of the risks impacting the data landscape e.g. information related audit findings (internal and external), conformance review results, self-assessments, gap assessments, security incidents, policy dispensations, material data quality issues, records retrieval failures, etc. The consolidated information risk profile must inform the overall risk profile of FirstRand;
- **Data technologies**. monitoring the identification and implementation of required technologies by brands to support information governance and management processes, i.e. data profiling and cleansing tools, meta data and master data management tools, BI applications, etc. Data technologies must be rationalized and re-used across brands where it makes technical and business sense;
- **Initiatives and projects**. Identification and monitoring of information related initiatives and projects in support of the data strategy; and
- **Audit and conformance reviews**: Identification and implementation of governance processes to:
  - monitor and report on data control design and effectiveness,
  - collect metrics and success measures and report them to data stakeholders;
  - results of conformance reviews, compliance to legislation and standards, etc.

Key outcomes:
The outcomes of the governance and management of information must ultimately be in line with the business and data strategies of FNBM and cannot be achieved in isolation. These outcomes must be aligned and driven in conjunction with other important business imperatives. Outcomes are not limited to what is mentioned in the IGF and not all outcomes are discussed separately in the IGF, but key expected outcomes include optimized information value, accountability for information, managed information related risks and the ethical use of information. A successful information governance and data management approach, which builds trust and meets legal requirements, must also lead to improved decision-making, operational efficiency, understanding of data and regulatory compliance.

- **Ethical use of information:** Information ethics is concerned with ethical standards, moral code, legal and societal aspects of using information (relationship between the origination, creation, organization, dissemination and use of information) and communication technologies. It's about honest and genuine transparency in data management.

The following must be considered as part of ethical awareness[8] from a data perspective and must inform the development and formalization of principles for the ethical use of data in the near future:

- **Context** – For what purpose was the data originally collected? For what purpose is the data now being used? How far removed from the original context is its new use? Is this appropriate?
- **Consent and choice** – What are the choices given to an affected party? Do they know they are making a choice? Do they really understand what they are agreeing to? Do they really have an opportunity to decline? What alternatives are offered?
- **Reasonable** – Is the depth and breadth of the data used and the relationships derived reasonable for the application it is used for?
- **Substantiated** – Are the sources of data used appropriate, authoritative, complete and timely for the application?

- **Owned** – Who owns the resulting insight? What are their responsibilities towards it in terms of its protection and the obligation to act? Are mechanisms in place to ensure responsibility and accountability for analytics and its outcomes, both before and after development, deployment and use?
- **Fair** – Is advanced analytics free from bias, ensuring fairness and avoidance of unfair discrimination? How equitable are the results of the application to all parties? Is everyone properly compensated?
- **Considered** – Have you considered and is the data subject aware of the consequences of the data collection and analysis?
- **Access** – What access to data is given to the data subject?
- **Accountable** – Do we sell data to third parties? Do we sell data aggregated or as personal identifiable data? How are mistakes and unintended consequences detected and repaired? Can the interested parties check the results that affect them? When do you anonymize personal data? Is the information owner aware of the use of data?
- **Transparency** – Are data processing activities and automated decisions truly transparent and explainable? Does the individual understand the purpose and interests of data processing in terms of risks, as well as social, ethical and societal consequences? In which country is the data stored? Where is the storage solutions provider headquartered?

2. PURPOSE

This framework is a sub framework of the Business Performance and Risk Management Framework and is a management tool to ensure business success through the use of reliable information with the aim of optimizing information value and supporting effective management and mitigation of information-related risks.

The purpose of the IGF is to:

- create a common reference and stipulate key information governance requirements across the Bank;
- ensure that FNBM´s information and records are maintained to a level of integrity and quality sufficient to ensure regulatory compliance and effective operation of the business;
- create a framework for the establishment and management of information management principles, policies, standards, processes and guidelines;
- define key roles and responsibilities involved in the management of information and oversight thereof within the organization;
- oblige management to adopt and adhere to a set of minimum standards and criteria for the management of information; and
- assist the board and senior management to discharge their duties in relation to information management in accordance with legal and regulatory requirements.

3. REGULATIONS APPLICABLE

This framework is based on the best practices and principles contained in national and international standards and has been tailored to reflect the Mozambican business and regulatory environment. Regulations considered include Basel risk data aggregation and risk reporting principles, GDPR, and local regulations as listed below:

- Law 15/99 of 1 November – Law of Credit Institutions and Financial Corporations and their amendments brought by Law 9/2004 of 21 July;
- Decree 54/2004 of 10 December - Regulation of the Law on credit institutions and financial corporations with the amendments brought by 30/2014 of 5 June; and
- Notice 4/GBM/2013 - Risk Guidelines

4. SCOPE

Information management concerns every person in the Bank and forms an integral part of the FNBM´s business activities. This framework and its underlying policies are, therefore, applicable to all business units or departments and all employees in the Bank. The level of application of this framework within the Bank is dependent on the size, nature and complexity of operations within the Bank and subject to the minimum requirements for the application of the BPRMF. The level of application decided upon must be agreed, in consultation with Group information governance, and approved by the information governance committee.

For purposes of this framework, the term 'information' includes records, data, information and knowledge owned or processed by or on behalf of FNBM. The framework applies to information assets, whether electronic, paper or in other forms. Information assets may consist of structured or unstructured information. The Bank must identify and classify those information assets that are key to the sustainability of their operations and include them in the scope of their information governance activities.
The IGF supersedes any other information-related policies in the Bank and mandates the minimum levels of information management practice that must be put in place.

5. FRAMEWORK APPROVAL

The IGF is owned and documented by Enterprise Risk Management, approved annually at the MRCC and recommended for final approval at the Risk, capital management and compliance committee (RCCC).

6. COMPLIANCE

6.1 Non-compliance to IGF requirements

Non-compliance with this framework may expose the Bank to breaches of legislation/regulation, possibly leading to litigation or regulatory censure, which could result in:

- payment of financial compensation in the event of litigation or compensation claims which cannot be adequately defended;
- fines by Regulators and/or imprisonment;
- reputational damage resulting in loss of business;

Any suspected breach of this framework or its supporting frameworks and policies will be referred and investigated under the relevant disciplinary processes and procedures; and may constitute a criminal offence.

Non-compliance with this may result in appropriate actions by ERM as set out in the Operational Risk Management Framework (ORMF).

6.2 Dispensation

Any business area wishing to apply for a dispensation/waiver, (where a dispensation is a temporary/special consideration or permission granted for non-compliance and a waiver being a permanent permission granted) on any element of this framework must provide a reason for non-compliance, which must be supported by the associated risks and mitigating actions to manage risks, and in the case of a dispensation, the timelines for achieving compliance.

BAs must, therefore, keep a list of dispensations and/or waivers which must be timeously updated. The dispensation/waiver request must be completed in the relevant template and submitted to the IGC for consideration.

Requests for waivers or dispensations are considered and assessed on a case-by-case basis.

7. CORE INFORMATION PRINCIPLES

The core principles and generic guidelines with respect to information governance in the Bank can be summarized as follows:

Table 1: Core information principles

Principle	Statement
The board is responsible for information governance	The Board exercises its information governance responsibility through the Risk, capital management and compliance committee (RCCC). The RCCC and the Platform exco delegate its information governance responsibility to the information governance committee (FNBM IGC).
Information governance is a subset of corporate governance	Information governance is a subset of corporate governance and will be incorporated into the existing governance and risk management processes of the Bank.
Information is managed as a strategic asset	Information is a valuable and strategic enterprise asset and will be managed in line with legal and regulatory requirements, the Bank-wide business and data strategies and policies, it will also be managed in line with its value, sensitivity and risks.
Optimal value is derived from information, whilst legal and ethical use of information is preserved	Selected processes, people, data analytics and technology capabilities will be identified, prioritized and applied to enhance and leverage information, ensuring optimal business value is extracted for the Bank
Information is appropriately shared and readily available, whilst adhering to FNBM policies and in compliance with requisite legal and regulatory requirements	To improve operational efficiency, enhance reporting, competitive advantage and accelerated decision making, data and information must be appropriately shared and leveraged across business units and must be readily accessible to all, except where confidentiality, legal or security restrictions apply.
Information management is a shared responsibility between IT and business	Information management is a shared responsibility between business and IT management and will be actively managed at all levels of the Bank.
Information is classified so the degree of control applied is proportionate to the risks	The origin, location, business use, value and risk profile of information dictate its classification, and hence the degree of management, protection and security required.
Information ownership is clearly allocated	Data and information must have designated and assigned ownership with accountability for integrity as close to the source as possible.
Information is secure and privacy rights are protected	All access to important information and information processing facilities is controlled based on business and security requirements. Information security and privacy controls address relevant people management, physical security and IT security risks. Privacy rights of people to which personal information belong will be protected.
Information risks, issues and incidents are reported transparently	Information security risks, incidents or events, records issues, data quality issues and control weaknesses are identified and communicated in a manner that allows timely corrective action to be taken.
Data quality is fit for purpose	Data produced and reported must be fit for purpose, e.g. ensuring completeness, accuracy, timeliness and integrity, proportional to its use and cost of collection and maintenance.

Master data is a strategic shared asset	Master data is recognized as a shared data asset and must be managed and governed diligently to drive increased business value through the availability and use of consistent, trusted and shared master data.
Data analytics, including big data, machine learning and advanced analytics, is 'ethical by design'	Ethical data use principles will be embedded in the development, deployment and use of analytical solutions from the start.
Data literacy is entrenched	Data literacy and an information management aware culture is promoted to support effective and ethical use of information. Deliberate data literacy competency development to improve executives and employees' ability to communicate and understand conversations about data and support digital dexterity strategies.

8. GOVERNANCE STRUCTURES

Information governance reporting is the responsibility of Information Owners and Information Governance Owners. The FNBM information governance structure and how it relates to other committees is depicted in the figure below.

8.1 Board of directors and RCCC

The board has overall responsibility for the effectiveness of the information governance processes. It is responsible for the establishment of formal information governance management and governance structures, duties and responsibilities and for the discharge of this responsibility through the RCCC.
The RCCC delegate their information governance responsibilities to the IGC.

8.2 Executive management committees

The Executive management committee is responsible for all aspects of management of their businesses, including the management of information. There are requirements designed to ensure an Information Management Framework is established, executive management is aware of and protects important information assets, sufficient resources are allocated to optimize the use of information and ensure that information risks are adequately managed.

As a minimum the executive committees must ensure:

- strategic information management strategy and a budgeted commitment;
- nomination of a information governance owner or an appropriate governance body accountable for providing strategic information management direction, reporting and sanctioning risk acceptance. This includes oversight and delegation of responsibility to:
  - debate and ensure that business strategies appropriately provide for information management initiatives; and
  - decide on the Group's appetite for information governance and risks associated with the management of information;
- procedures are in place to ensure contacts related to information risk management with relevant authorities and regulators are maintained;
- that identification, assessment and management of data quality risks are part of its overall risk management framework. The framework must include agreed service level standards for both outsourced and in-house data-related processes; and
- the effectiveness of the internal organization for managing information must be reviewed independently at risk assessed intervals.

8.3 Information Governance Committee (IGC)

The IGC objective is to assist Management and Board in discharging its responsibilities relative to the governance of information-related matters within the Bank.

FNBM IGC is responsible for the strategic information management and, as such, information governance owners, business area heads and information owners will be guided and directed by this forum from an information strategic perspective.

It is the responsibility of this committee to:

- report to the Exco, The Risk Committees, the Combined Assurance Forum and the audit committees (with regard to specific requirements) on the status of information governance and management;
- ensure that appropriate structures are in place to oversee information management. The committee must debate and consider the appointment of a chief data officer or appropriate alternative;
- ensure that business units are appropriately resourced to execute information management initiatives;
- ensure that relevant interdependencies are managed;
- ensure inclusion of relevant representation from the business in oversight structures;
- ensure a strategic approach to and facilitation of the integration of information management into business strategic thinking and planning;
- ensure that the information processes within the scope of its authority remain appropriately funded;
- ensure effective management of information for the benefit of Bank, customers, staff and other stakeholders;
- initiate such actions and the issuing of instructions as may be appropriate, in order to improve the status of information governance;
- ensure that information governance workplans are reviewed at least annually and confirm that they continue to meet the business priorities and needs. These workplans must be based on a comprehensive assessment of information-related practices, requirements, risks, and opportunities and must be established with the structure, direction, resources, and accountability to provide reasonable assurance that the set objectives will be achieved; and monitor the communication and implementation of the IGF.

9. KEY INFORMATION GOVERNANCE ROLES

The fluidity of data (it flows through and is updated and stored via several business processes across the Bank) complicates the allocation of accountability for information, which often results in data quality issues, records retrieval failures, and disparate and inconsistent controls across the information supply chain. To mitigate this risk, key data themes, aligned with selected organizational functions, have been identified and is used to prioritize implementation and clarify responsibilities**:**

- finance data;
- risk data;
- procurement data;
- tax data;
- HR data;
- customer data;
- product data;
- IT data;
- audit data;
- treasury data; and
- company secretarial data.

Data themes are approved at the Group IGC and must be consistently used across the Group. In cases where additional data themes may be required in-country, the relevant information owner must engage with ERM and table a motivation and request for approval at the IGC. Additional sub-data themes may only be added with the consent of the relevant Group Information Owner and ERM Information governance. Given the impact on classification effort, navigation and maintenance, a maximum of three sub- data theme levels will be allowed.

9.1 Information Governance Owner

The information governance owner is appointed by the Exco to carry out on the following responsibilities:

- be a senior manager with relevant experience and decision-making authority, preferably an exco member;
- represent a single point of accountability at for information governance such as interfacing with in-country and Group governance structures (audit, board, information governance committees) and executive management;
- chair the IGC;
- ensure that information ownership and accountability is clearly defined and allocated. As a minimum, segment and brand information owners for relevant data themes must be identified and responsibilities allocated;
- promote data literacy, understanding and reuse of information assets and metadata (i.e. via a common business taxonomy and use of metadata repositories); and
- ensure the communication, implementation and adherence to the requirements of this framework.

9.2 Information owners

The concept of an information owner is intended to convey a fiduciary (or trust) level of responsibility towards information. As the name implies**,** information ownership refers to both the possession of and responsibility for information; it recognizes, formalizes and operationalizes a set of responsibilities specific to the management of information. Ownership implies power as well as control. The control of information includes not only the ability to access, create, modify, package, distribute, derive benefit from, buying, selling or removing data, but also the right to assign these privileges and responsibilities to others.
The Bank assigns responsibility for information assets associated with a data theme to information owners.

These information owners exercise FNBM´s rights and interests in the data theme. The allocation of information owner roles will be monitored at the IGC.
Information ownership must be cascaded down into business areas and information owners may choose to allocate certain responsibilities to other roles, e.g. data stewards, etc.

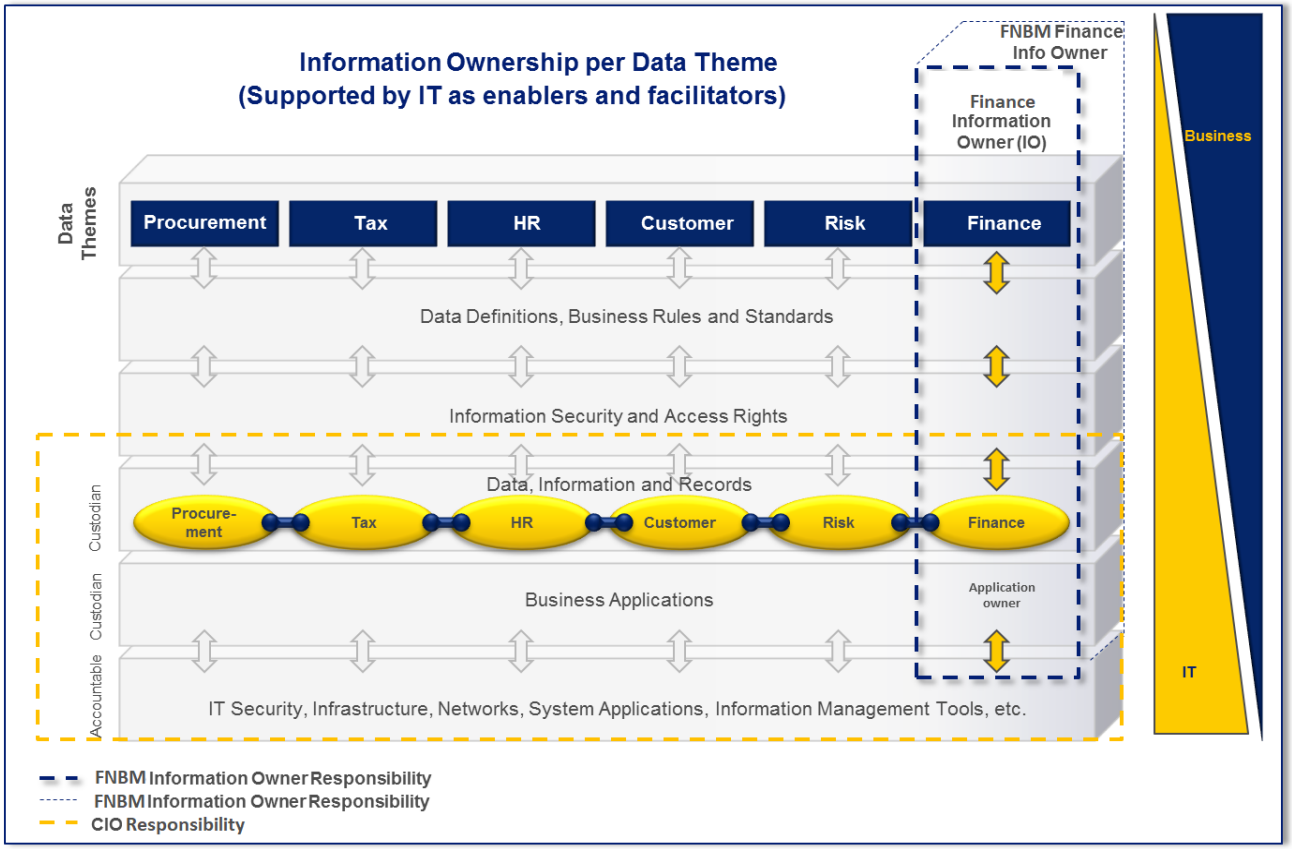


Figure 3: FNBM information ownership per data theme

Information owner responsibilities will follow the owner-manager principles and include:

- communication and implementation of IGF requirements to relevant stakeholders;
- ensure the implementation of policies and standards to control information-related risk for the data theme;
- identify and develop supporting data theme specific standards where required (e.g. risk data standards, etc.) and ensure adherence thereto;
- compliance with legal, regulatory and contractual information requirements;
- classify and define information so the degree of control applied is proportionate to the value and risks;
- Group and segment/brand Information owners are responsible to agree information boundaries and scope for the **data theme**. Responsibilities include:
    - Information governance strives to govern a manageable set of data elements per data theme. Accountabilities must be assigned to (i) standardize these data elements for the data theme, (ii) specify and enforce valid values, and (iii) address data quality and records requirements.
    - Establish integrated data taxonomies (dictionaries), which include information on the characteristics of the data (metadata), as well as use of single identifiers and/or unified naming conventions for data including legal entities, counterparties, customers, products, accounts, etc.
    - Establish business rules, verify data quality and target measurable improvements in data quality for important sets of information.

- Information controls must be designed, documented and implemented in business processes (in line with operational risk management requirements) to adequately address relevant people management, physical security, information privacy and security risks.
- Records are identified and managed in accordance with legal, regulatory and corporate governance demands;
- Cost-effective delivery of consistent, integrated data for all business intelligence and reporting activities;
- Businesses must have procedures in place to ensure ongoing capability development and maintenance of professional and business skills related to information management;
- Information risks, incidents/events, issues and control weaknesses are identified and communicated in a manner that allows timely corrective action to be taken; and
- Promote transparency in the processing and use of information and ensure that this is within legal and ethical boundaries.

– Demonstrable compliance with the above and act to address gaps.

9.3 The Chief Information Officer

The chief information officer (CIO) supports and enable business success by providing IT services in the most strategically sound, secure and cost-effective manner possible. However, the ownership and accountability for the quality of business information moving in, out and around the IT environments is not a CIO responsibility. refer below to the responsibilities:

- Business remains accountable and responsible for the quality and integrity of their data, irrespective of where and by whom it is processed;
- The CIO is responsible for the accuracy, completeness and integrity of IT's own data (e.g. application portfolio, access information, IT asset registers, IT contracts, system logs, etc.);
- The CIO must ensure that IT general controls have been designed, assigned and are operating effectively for all systems owned by their respective brands;
- The CIO is required to ensure design and architecture that provides a systematic model for defining data and for managing the process of creating, moving, modifying, storing, archiving, securing and deleting data. They can take on a gatekeeper as well as a service provider role, ensuring that the IT needs of the business units they serve comply with the requirements of this framework;
- Ensure appropriate consideration of information requirements when technology solutions are acquired, developed, maintained and implemented, the CIO must:
  - designate members of the IT leadership team to participate in the information governance and management committees (and related forums); and
  - communicate the requirements of the IGF to all IT stakeholders, including external service providers where relevant.

9.4 Regulatory and conduct risk management compliance officers

Risk management activities within FNBM are overseen by the two independent, central risk control functions, (i) Enterprise risk management (ERM) and (ii) Regulatory and conduct risk management (RCRM). These two functions are part of the second line of control.

RCRM's roles and responsibilities relative to information governance include:

- ensuring that Risk Management Plans (RMP) reflect relevant legal and regulatory requirements for all information management domains (in consultation with Group ERM);
- The Privacy Framework forms the basis for the achievement of data privacy and protection within the Bank and sets out the roles and responsibilities that are required by each line of defense to implement, sustain and monitor privacy compliance, and mitigate the risks related to the processing of personal information.

To ensure that the control environment sufficiently covers all legal and regulatory requirements, compliance officers must:

- provide input into the risk assessment process (PRCIA) in business by identifying and assessing the regulatory risks and controls related to information management;
- ensure that business include relevant information controls as documented in their RMPs; and
- must provide guidance on the implementation of the RMPs and monitor that fit-for-purpose information controls are designed and implemented by all business areas.

9.5 Enterprise Risk Management

ERM is responsible for the independent governance and oversight of all types of risk affecting the Bank, including risks associated with information.

9.6 Deployed risk managers

In the second line of control, business heads are supported by deployed risk management functions that are involved in all business decisions. These risk managers are responsible for information risk identification, measurement and control.

Deployed risk managers' roles and responsibilities relative to information governance include:

- facilitating information risk management processes on all key information projects (as defined by each business area);
- assisting management and information owners in identifying and assessing information risks and propose actions or mitigating controls to adequately and effectively manage these risks in accordance with the IGF and ORMF and its related sub-policies, e.g. ensure that the PRCIAs are completed and adequately provide for information governance requirements;
- confirming the adequacy of the design and effectiveness of information-related controls through control self-assessments; and
- monitoring the implementation of data quality and records management processes and resolution of identified issues.

9.7 Group internal audit

Group internal audit (GIA) plays an integral part in the information management processes by providing a 3rd line of control independent and objective assurance on the overall adequacy and effectiveness of information governance, information risk management and control established by the first and second lines of control.

GIA's responsibilities relative to information governance include:

- providing assurance with regards to the compliance of business units with this framework and supporting policies, standards and procedures as part of audit assignments;
- assessing the adequacy and effectiveness of information controls and confirming the completeness, accuracy and validity of key internal controls over information in accordance with this framework and its related policies and standards;
- ensuring that audit staff is sufficiently skilled in the respective information management domains to support appropriate identification and classification of audit findings;
- ensuring that audit findings are classified to effectively report on audit findings per information management domain (e.g. data quality, records management, etc.); and
- ensuring that GIA access to information systems via data analytics tools (e.g. data extraction and manipulation tools for CAD purposes, etc.) is controlled to prevent any possible misuse or compromise of information.

10. INFORMATION MANAGEMENT

Information management entails the establishment and deployment of roles, responsibilities, policies, and procedures concerning the acquisition, maintenance, dissemination, and disposition of information to support the business and to maximize the investment in data and content.

This component of the framework highlights key principles for every one of the following information management domains :

- data quality management (completeness, accuracy, etc.);
- metadata management (definitions, business rules, data catalogue, etc.);
- content, document and records management (vital and operational records);
- data product, big data and advanced analytics (reporting, analytics, modelling, etc.);
- master and reference data management (authoritative source of central and shared data entities);
- information security and data privacy management (data protection and access control);
- data storage and operations management (technical support for data processes);
- data development, interoperability and integration management (software development, SDLC, etc.); and
- information architecture management (data flows, information requirements, data models, Information Architecture Framework, etc.)

Implementing information governance and information management requirements is a journey and executive management in all entities must oversee senior management's accountability in respect of assessing and implementing the prioritized information management principles within an agreed timeframe.

10.1 Information categorization and classification

Information classification's goal is to categorize information by value, legal and sensitivity requirements in order to enable targeted use, remediation and protection. The information being stored and managed by FNBM can deliver value or simply consume valuable resources. It would be unwise and costly to submit every single piece of information to the same level of governance and it is, therefore, imperative to identify and classify those information assets that are key to the sustainability of the Bank´s operations. The classification of information applies to all information that is on-premise, off-premise, on-shore, off-shore, etc. The location of data must be noted and be in line with residency requirements.

Information must be classified according to its importance and agreed FirstRand information classification categories to ensure that appropriate controls are applied during its creation, storage, processing and disposal. The classification criteria are to be used for all information, whether electronically stored, paper based, or mentally retained:

- **Sensitivity classification**: Information must be classified in accordance with requirements to maintain or protect its confidentiality, integrity or availability (refer to the Information Security Policy);
- **Legal and regulatory classification**: Classification must reflect regulatory and legal requirements;
- **Records categorizations**: Business records must be identified and categorised as either vital or operational (refer to the Records Management Policy):
  - **vital records**: records, regardless of medium, necessary to ensure the continuity of normal business operations and/or in the event of disasters or business interruptions. These records protect the legal and financial position of the Bank and must be disposed of as defined by local regulatory retention requirements;
  - **operational records**: records which have no mandatory-related retention requirements and must be disposed of as defined by the business unit retention schedule disposition authorities and processes**;**

- **Location classification:** geo location of data to support data legal and regulatory as imposed by the local jurisdiction;
- **Origin classification:** Information can originate through various methods and systems. The origination of information needs to inform the potential use and consent requirements of information and must be classified using the following classification categories:
  - provided – information originally obtained directly from the customer or entity;
  - observed - information obtained through observing the customer or entity e.g. social media;
  - derived – information that is derived from other information, e.g. computational (creation of new data elements through an arithmetic/algorithmic process) or notational (new data elements created as being part of a group based on common attributes shown by members of the group); and
  - inferred – information is the result of a probability-based analytic process, e.g. advanced analytics using correlation rather than causation, etc.); and
- **Data theme**: data must be classified to reflect the appropriate data theme.

The following types of data must be considered for classification, and as a minimum, important information must be included in the scope of **business continuity and disaster recovery plans**:

- unstructured data - any document, file, graphic, image, text, report, form, video or sound recording that has not been tagged or otherwise structured into rows and columns or records – can include emails, internet data streams, customer interactions, call centre data, corporate intranet portals, security footage, minutes of meetings, PDF files, etc.;
- transactional data - business transactions that are captured during business operations and processes, such as sales, invoices, purchase records, etc.;
- metadata – refer metadata management;
- master and reference data – refer master and reference data management;
- hierarchical data - stores the relationships between data, e.g. company roll-up structures, client hierarchies, etc.;
- analytical data - derivations of the business operation and transaction data used to satisfy reporting and analytical needs. Data is stored in data product, including data warehouses, data marts, spreadsheets and other decision support applications; and
- cloud and off-shore data - business objectives and regulatory requirements calls for the classification of all information residing or provided in any cloud computing[12] and offshoring arrangement. Offshoring of data refers to the storage and/or processing of data outside the borders of Mozambique. The information classification pertains to location (residency - where information is stored), jurisdiction of information, service and deployment model, etc. The information classification is to be applied to data at rest, data in motion (transmission), encrypted for offshore and cloud computing. Please refer to the Cloud Policy for more detailed requirements.

10.2 Important information and information assets

'Important information' include data or information contained in systems, paper documents, applications and other end user developed applications (e.g. business-critical spreadsheets - refer Critical Spreadsheet Policy) that is regarded to be of high importance or are required for the business to operate and continue operating effectively.

The information asset register (IAR) helps to drive clarity and consistency about which data sources are important for the Group. It covers the data sets across the Group that are important to drive strategic outcomes such as minimising risk, reducing the cost of operations, improving the customer experience, and driving growth.

Information assets must be recorded in the information asset register (this may comprise consolidation of one or more registers or catalogues), including data, IT assets, systems, processes and the location of the data (to

be in line with data residency requirements). Agreement about which data sources are information assets allows the Bank to focus the following activities on its information assets: data management, compliance and value engineering / data monetization. The respective data theme owners and information governance owner must work together to identify the sources that represent valuable or important data for their business areas. This implies that information assets are identified by data theme and by business area

While FNBM maintains its own IAR, The FirstRand IAR is a register of registers and will identify important information assets and their associated metadata (base set).

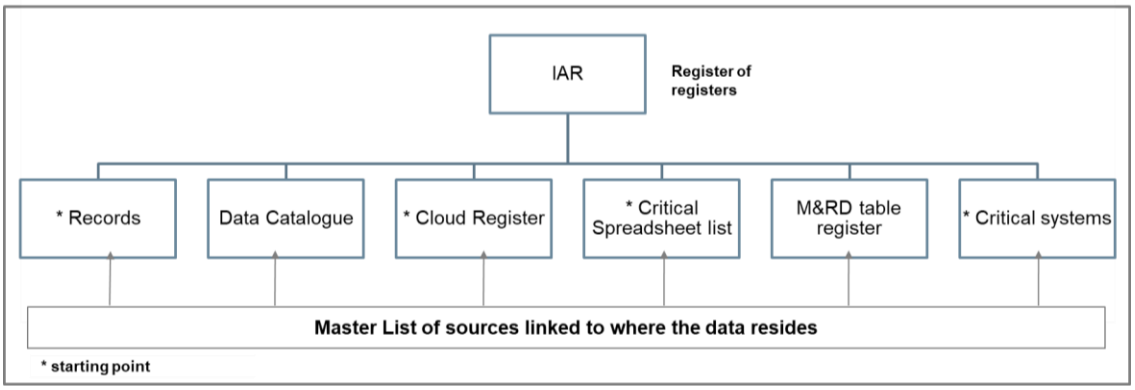


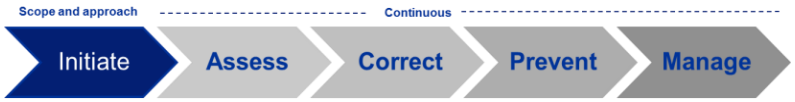
Figure 4: High-level depiction of Information asset register (IAR)

The information asset register must as a minimum, capture the following metadata: Entity name, name of the register or list, its purpose, owner, what type of metadata it covers (i.e. business or technical), link to where register\ list is available and maintained.

For the purposes of this register the information asset is the information and not the media it is stored on. For clarification, the information asset may be stored and managed on a business system; but a business system is an application asset not an information asset.

10.3 Data quality management

Data quality management is the combination of organisational structures, methodologies, tools and activities (planning, control, development and operational) that exist for the purpose of reaching and maintaining the required levels of data quality within the Bank. The data quality management process is a collection of ongoing activities involving developing an understanding of data processed, identifying and resolving data quality issues, enhancing data and monitoring the status of data quality.



FNBM is expected to produce information that is reliable, and which takes proper account of the different users of the information produced (customers, shareholders, regulators and other market participants).

To ensure that important information is maintained to a level of integrity and quality sufficient to ensure effective operation of the business, data quality management must be formalized, and the following data quality principles must be adhered to:

- apply data corrections at original source, if possible. If it is not possible to correct data at source, forward data corrections to the owner of original source for appropriate action;
- data quality issue ownership must be clearly allocated;
- information must be sourced from authoritative or trusted data sources;

- information integrity will be maintained throughout the information supply chain, including when staging and transforming information. Business must be able to demonstrate that data quality is maintained throughout the end-to-end process from initial capture (or import from an external source) through to use in calculations, reporting, collections, etc. Where the data is transformed, transformation must be documented;
- data must be fit for purpose;
- data must be sufficiently accurate to avoid material distortion of the outcome;
- information owners must ensure that measurable quality targets are set for those subsets of important data where quality must be improved, and that adequate controls and processes are in place to verify and preserve the quality of data in the following dimensions:
  - accuracy: data is correct within the precision required and refers to the degree of confidence that can be placed in the data. Accuracy refers to how close the measured values are to the actual correct value;
  - completeness: requisite information is available;
  - conformity: data is in the correct format;
  - integrity: freedom of data from unauthorized alteration and manipulation that compromises its accuracy, completeness and reliability;
  - consistency: data is not in logical conflict with other data across systems/processes and the degree to which data with the same definition has the same value wherever it is stored or displayed;
  - precision: data is provided with sufficient precision;
  - timeliness: data is known to be sufficiently current, up to date and available;
  - uniqueness: no entity exists more than once in the dataset;
  - risk data specific:
    - adaptability: ability of risk data aggregation capabilities to change (or be changed) in response to changed circumstances (internal or external);
    - approximation: a result that is not necessarily exact, but acceptable for its given purpose;
    - clarity: ability of risk reporting to be easily understood and free from indistinctness or ambiguity;
    - comprehensiveness: extent to which risk reports include or deal with all risks relevant to the Bank;
- businesses must regularly review (at least annually) all categories of important data to measure and monitor the accuracy of data, develop appropriate escalation channels and ensure clear action plans to be in place to rectify poor data quality;
- assess and profile data quality against defined business rules;
- data quality issues must be appropriately classified per data theme and type of error (error in processing, error in business process, error in source system, error in expectation and error in semantic consistency);
- data quality issues must be appropriately risk rated (refer to data quality risk rating guideline);
- all material data quality issues must be logged, at intervals agreed at the IGC, on a central data quality issue register. Initial focus will be on material data quality issues impacting on risk reporting;
- in addition to identification of materiality, attention must be given to the number and classification of data quality issues reported to ascertain the reliability of material data sources;
- auditability and traceability will be maintained when retaining and archiving information;
- accuracy of reporting will be maintained through:
  - defined requirements and processes to reconcile reports to the risk and finance data;
  - testing of accuracy of input data, including reconciliation at a sufficiently detailed level so that, together with other available evidence, reasonable assurance that data input into models (risk, finance, etc.) and rating systems is accurate, complete and appropriate. Input data fails the required standard if it gives rise to a serious risk of material misstatement in reporting either immediately or subsequently;
  - defined automated and manual edit and reasonableness checks, including an inventory of validation rules that are applied to quantitative information;
  - all material data aggregation processes, whether automated or manual, must be documented. Documentation must include an explanation of the appropriateness of any manual workarounds, description of their criticality to the accuracy of risk data aggregation and proposed actions to

reduce the impact (data aggregation refers to the processes that combine and summarize atomic data); and
  - integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exception reports;
- businesses must confirm quarterly to the segment/brand information governance owner that there is reasonable cause to believe the quality of the remaining important data is fit for purpose.

10.4 Metadata management

Metadata management is the management of processes, technologies and people that create, control, integrate, access and analyze metadata. Metadata forms a foundation for clear communication within FNBM, as well as with customers, partners and other stakeholders. Metadata management is key to a successful information strategy, without it, navigation of the data landscape is inaccurate and highly cumbersome, the data models are potentially inaccurately mapped, reports or the interpretation thereof may be incorrect, business processes may be imprecise and the entire currency of data / information transformation, migration, integration and tracking systems of the group will lack certifiable accuracy.

Metadata is literally data about data. Metadata allows for an information asset to be useable, verifiable, traceable and reliable for its entire life cycle. It defines and describes the characteristics of data and information contained in databases (electronic) or paper documents and is used to improve both business and technical understanding of data and data-related processes.

Metadata categories:

- business metadata is logical in nature, as it reflects an abstract or business view of the data. It includes names and business definitions of subject areas, entities and attributes, attribute data types and other attribute properties, range descriptions, valid domain values and their definitions;
- technical metadata includes physical characteristics of data found in a database, including physical names, data types, lengths, precision and scale of numeric data elements, statistics, source locations (lineage) and code values. It may also include data about programs and other technology;
- operational metadata describes details of the processing and accessing of data including logs of job execution and errors, audit trails, version control etc. Operational metadata is active in nature. It is captured and stored on a continuous basis as part of day-to-day operations and is more volatile than technical and business metadata. Operational metadata is mostly automatically created by systems;
- process metadata is data that defines and describes characteristics of other system elements (processes, business rules, programs, jobs, tools, etc.);
- records metadata provides more information about records e.g. data created, origin and retention; and
- data stewardship metadata is data about responsibilities, stewardship processes and responsibility assignments.

Metadata capabilities:

In achieving usability, traceability and data reliability across the life cycle for all the types of metadata, a core set of metadata capabilities must be prioritized for implementation, including: metadata governance, data catalogue, metadata repository, business glossary, metadata capture, metadata integration, data lineage analysis, impact analysis and meta data reporting:

- The data catalogue is at the heart of the metadata management capabilities. A data catalogue assists in finding, inventorying and analysing vastly distributed and diverse information assets. An appropriate data catalog must be implemented as part of the central meta data repository to:
  - ensure that the Bank´s data platforms do not become data swamps;
    - help scale the appropriate use of data within the Bank by making it easy to find, understand, trust,

use and reuse for self-service analysis and to activate the data to deliver business value;
  - limit and discourage the use of siloed data catalogues that do not connect to the enterprise metadata repository;
  - shorten data discovery and improve business user, data engineer and data scientist productivity improvement due to easy-to-use self-service solutions;
  - cost and effort saving from faster onboarding of data consumers and providers;
  - cost and effort saving from faster onboarding of resources;
  - enhance and enable collaboration around data and ultimately improve data literacy;
  - increase data transparency and reuse to improve the accuracy of analysis;
  - create a central platform to document data and data usage guidelines, define best practices, and determine the standard data sets for further use; and
  - encourage and document user interaction about information assets, their use, and best practices;

- Other metadata management capabilities include:
  - technical data lineage: The foundational capability of metadata management that provides the functionality to determine where data comes from, how it is transformed, and its target destination. It enables visibility into the lifecycle of data between different systems;
  - business glossary: a comprehensive directory of business terms, definitions, and taxonomies that can be used across disparate business processes and systems. The ability to create, enrich, govern and grow FNBM's business concepts and terminology, and associated relationships and definitions between them;
  - metadata enrichment: The consolidation of metadata from disparate tools and sources, including business intelligence (BI), data integration, relational databases, modeling tools, and third-party metadata into a single repository.
  - rule management: the ability to support definition and evaluation of business rules and the ability to provide reports in case of exception to these business rules
  - impact analysis: The prediction of potential impacts that changes in one system may have on other inter-dependent systems. These changes may include the deletion or change to a specific standard data element, changes to a system of record or poor data quality measures in one of the subsystems.
  - metadata sharing and delivery: using mechanisms (e.g. semantic tier) to expose curated metadata for analytics, data science and other operational use cases; or the ability to invoke data catalogs directly (e.g. APIs) in a downstream analytics/BI or data science platform
  - metadata governance: provides the ability to setup an appropriate governance structure (information owners/ stewards) and automated workflows to govern metadata as well as the ability for stakeholders to collaborate on the authoring and management of metadata;
  - data classification: involves the ability to classify (tag) data to make it easily searchable and traceable and to organize data by relevant categories (refer section 10.1) so that it may be used and protected more efficiently. On a basic level, the classification process makes data easier to locate and retrieve.

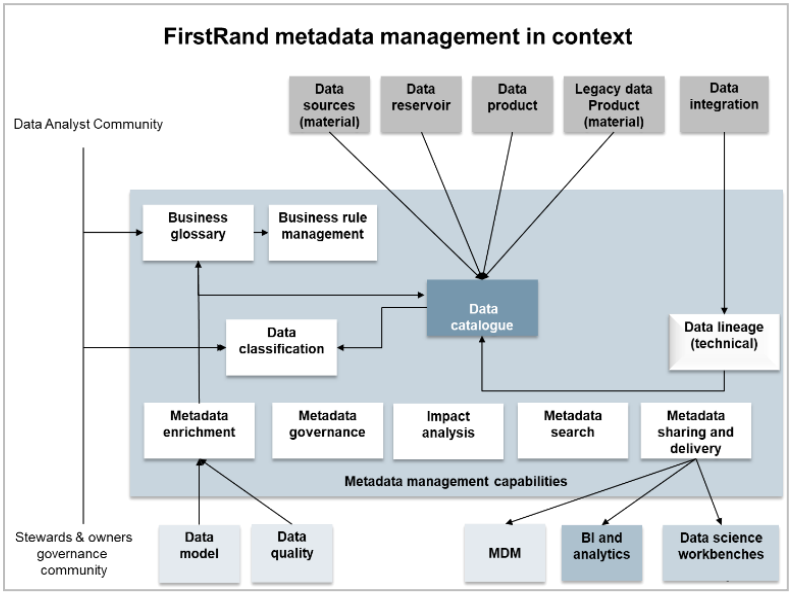


Figure 5: Metadata management in context

Key requirements:

At a bare minimum, metadata must be captured for material data sources, key data elements and vital records as identified across FNBM. The following must be considered:

- metadata repositories must be designed from established metadata sources, rather than reinventing these elements from scratch;
- guidance on how and where to find the data must be easily accessible;
- a key metadata consideration is to take a group-wide perspective to ensure future extensibility, flexibility, usability and reusability but implemented through iterative and incremental delivery;
- metadata systems must allow for extensions so that needs of a given application can be accommodated within the group;
- ensure alignment with the FirstRand data strategy before evaluating, purchasing and installing metadata management products;
- enterprise metadata repository to house and maintain metadata associated with all strategic data architecture components (e.g. data reservoir, data products, etc.), material data sources and key data elements. The use of an enterprise metadata repository will enhance accessibility to metadata and promote efficient use of data:
  - A central metadata repository is preferred; however, segments and brands must decide on a metadata repository solution that is fit for purpose for their data management needs. Motivation for use of brand specific meta data repositories must be tabled for discussion at the IGC and recommended for approval at the Exco. Board approval will be required for any new metadata solution components.
  - FirstRand elected to implement Ab Initio as the strategic solution for meta data management on the FirstRand data platform. Existing FNBM metadata repositories must integrate into the FirstRand Ab Initio repository for relevant meta data. The data integration design must be tabled and approved at the FirstRand Information architecture committee.
- metadata standards need to be established to ensure interoperability, consistency of use and execution of metadata management within FNBM;
- establishment and maintaining business involvement in data stewardship will allow assigning accountability for metadata throughout its life cycle. **Owners of both business and technical metadata must be identified**. Their roles and responsibilities pertaining to metadata data must be clearly articulated and

tracked to ensure that there is accountability for the capture, curation and maintenance of metadata for data elements that are critical in decision making for the Bank;

- Information owners must ensure that metadata is defined, recorded and captured on the relevant meta data repository for those information assets included in the scope of the IGF for the particular data theme. As a minimum:
  - a dictionary of key concepts used must be established - this is not an abstract data vocabulary, but an actual operational data vocabulary that defines the data flowing through the organization in a consistent way; and
  - key data elements must be defined clearly and consistently in alignment with the Group;
  - quality metadata is the crucial component for the proper identification, classification and management of data assets and processes within a defined business, while enabling accountable group wide transmission of those information assets;
- information governance and information management structures must define metadata-related processes and promote meta data awareness, within FNBM and provide guidance to owners on how to capture and maintain the metadata. This will ensure consistency in monitoring and measuring sound metadata management discipline across all brands and subsidiaries;
- metrics need to be defined to measure metadata management maturity. Metrics will enable brands and subsidiaries to understand the maturity level of metadata management and guide data owners and custodians;
- all metadata will include considerations pertaining to privacy, security and regulatory requirements. The capturing of relevant privacy, security and regulatory requirements as part of the metadata will promote transparency and provide guidance in driving compliance;
- metadata requirements must be considered when information management technologies (data quality, records, master data management, data models) are implemented and be used as sources of metadata to be integrated in the metadata repository: e.g. data quality metrics, records management metadata, etc.

10.5 Content, document and records management

Enterprise content management (ECM) - Is the strategies, methods and tools used to capture, manage, store, preserve, and deliver *content and documents* related to FNBM´s processes and business goals. It is an umbrella term that covers document management, web content management, search, collaboration, records management, digital asset management, workflow management, capture and scanning.

- **Capture**:
  - When converting information from paper documents into an electronic format through scanning business must adhere to the Bank´s standards and ensure that the processes and procedures are clearly documented;
  - Business must ensure that the minimum set of metadata (index values) that describe characteristics of the information for easy location through search technology are created; and
  - If technologies are used to automate the creation of metadata, (e.g. OCR/ICR/HCR/OMR/Barcode) business must ensure that they are certified and compliant.
- **Manage:**
  Includes the following traditional application areas -
  - document management (DM) - check in check out; versioning; search; organizing;
  - collaboration (or collaborative software such as groupware);
  - web content management (including Web portals);
  - workflow - production & ad-hoc; and
  - business process management - integrates all of the affected applications within an enterprise, monitoring processes and assembling all required information.
- **Store** component is divided into three categories:
  - repositories such as file systems; content management systems; databases; data warehouses;

  - library services which is the administrative service of the ECM; and
  - storage media and location premises, cloud (including vendor cloud)
- **Archive:**
  - involves the long-term, safe storage and backup of business-critical information (e.g. vital records);
  - storage media; and
  - inclusive of preservation, migration and emulation strategies.
- **Deliver c**omponent is divided into three groups: transformation technologies, security technologies, and distribution:
  - transformation must always be controlled and traceable;
  - security includes electronic signatures, digital rights, watermarking, etc.;
  - distribution output and media include but is not limited to: the internet, extranet, intranet, portals, e- mail, data transfer; mobile devices, paper, etc.

Records management (RM) is the lifecycle management of designated significant (vital records) of the Group. It is a collective term, including both the management of paper and electronic records, regardless of medium.

The purpose of records management principles is to prescribe records management direction, policy, processes and procedures within FNBM. The principles drive both business and functional capability for effective records management, which is comprised of people, processes and technologies harnessed to achieve effective records management. Please refer to the Records Management Policy.

Information owners must ensure that records are identified, classified and captured on a records register and that implementation roadmaps are constructed to ensure adherence to the following RM principles:

- accountability, responsibility and activities for RM must be assigned to appropriate employees with the adoption of the policy and procedures to ensure that it can be audited;
- RM processes and activities must be documented in a manner that is open, verifiable and available to all employees and appropriate parties;
- records must be protected from unauthorized alteration irrespective of whether inadvertent or deliberate. By retaining records in a manner that preserves complete content, context, integrity, authenticity and metadata, especially the metadata indicating origin and context;
- all records that the Bank manages, and stores must be securely protected. Records storage systems must provide information security controls and capabilities to protect the system and its content from alteration, corruption, inaccessibility, loss, compromise of confidentiality and privacy;
- relevant legal and regulatory requirements must be complied with; by managing records economically and responsibly by exercising good corporate governance and monitoring compliance;
- FNBM must be able to access records in a timely, trustworthy and cost-effective manner at any time during the record life cycle and use those records as required;
- FNBM information owners in cooperation with Group information owners, must compile a records register and retention schedule for all vital records used in brands. The FirstRand regulatory records retention standard can be used as reference when compiling the retention schedule; and
- RM solutions must provide the capability for proper disposal or destruction of records once no longer required. The procedure for disposing of paper and electronic records must be detailed in the records retention schedule, which must be adhered to.

10.6 Data product, data analytics, big data and advanced analytics management

Business value must ultimately be derived from all the effort and investment in data. Data products are the pinnacle of data-driven business, bringing insight and intelligence into the customer experience, getting better with every use, and enabling new ecosystem-based business models. Products fuelled by trusted data and artificial intelligence (AI) can be a powerful way to solve users' needs and deliver business value.
This section of the framework starts unpacking some of the information management requirements for data

products, data analytics, big data and advanced analytics and will be enhanced over time as the understanding the topics matures. All these components of the architecture must be managed in line with Information governance requirements. Please also refer to the FirstRand Information Architecture Policy for further clarification regarding information architectural requirements and positioning.

Data Product:
Data product is a component of the FirstRand data platform, supporting core functions to leverage data, be they physical products, software, or services. Fit-for-purpose sets of curated data, including data warehouse, marts, cubes, ODS, etc., can all be regarded as data products. A data application that acquires its value from the data itself, and creates more data as a result, is also a data product. Data products can be physically instantiated on any technology platform as a building block component, however data products would selectively be enabled in the integrated data foundation.

Characteristics of the data product are:
- data product contains trusted data to be used for reporting and decision support and enables the sharing with other business partners and internal systems. Data products must be the preferred sources for decision-making as opposed to the data reservoir that must be used for exploratory purposes;
- data products contain data that adds value and will be stored aligned to retention policies and requirements.
- data products are developed per segment and/or business unit but must be aligned and merged into the logical enterprise data model (EDM);
- data product data is modelled and curated and more tightly governed than any of the other layers of the information architecture to ensure data integrity. Not all data products are currently aligned to the EDM, alignment is preferred and must be considered where it makes business sense;
- the structure of the data stores is optimized for specific use cases e.g. to support operational use cases that have low latency requirements;
- machine learning (ML) models and applications are also data products. These applications are fueled by data and generate more data as a result which can be used to create more data products; and
- data is featurised and used as input into reinforcement machine learning models. The featurised data becomes a re-usable data product that can be used by multiple machine learning models.

The strategic data architecture, including some components of data product, is still being defined and implemented. Following is a set of high-level principles for the management of existing business intelligence and data warehouse environments:

> **Data warehouse (DW) management** incorporates management processes, integration technologies, data stores and conceptual, logical, and physical models to support business goals and end-user information needs. Creating a DW requires mapping data between sources and targets, then capturing the details of the transformation in a metadata repository.
>
> **Business intelligence (BI) management** is the management of hardware, software and organizational support for business intelligence activity that enables knowledge workers and modelers to access, analyze and manipulate data. It generally includes the business intelligence software, user interfaces, associated infrastructure hardware and software, data mart databases and multi-dimensional data cubes.

- data stores must be classified (e.g. operational data store, data mart, etc.) according to its characteristics;
- think and architect globally, act and build locally; (any systems must be designed and planned with the big picture and end-state in mind - for a greater and wider coverage yet build and implemented

incrementally within optimal benefits within the “global” design perspective – Group benefits rather than individual solutions.)

- data ownership for sourced, transformed and newly created information must be clearly allocated;
- one size does not fit all (No one solution in an organisation can be “lifted” and used to provide a solution in another – deployment considerations and constraints may be similar but may not fit another - make sure we find the right tools and products for each of your customer segments.);
- DW and BI design must:
  - support agile development;
  - start with the end in mind – let business priority and scope of the end-delivery drive the BI creation and DW content;
  - ensure user-friendliness and minimize chances for data replication and inconsistency;
  - ensure information controls are included on a proactive basis through all layers;
  - promote and ensure data classification, integrity, integration and standardization;
  - promote and ensure visibility of available data in the warehouse;
  - separate analysis workload from transaction workload and enables the Group to consolidate data from several sources;
  - summarize and optimize last, not first; build the atomic data and add aggregates as needed for performance, but not to replace the detail.

Data analytics, big data and advanced analytics:
As data and advanced analytics become a core part of digital business, data is more and more recognized as a strategic asset, with increased emphasis on the ethical use of information, data management practices, methods, use of cloud services and use of data resulting from big data and advanced analytics. FNBM must formalize the definition, management and governance of the required capabilities for advanced analytics and big data over time to ensure that optimal business value is derived and that associated emerging risks are understood and adequately managed.

Trustworthy analytics should be a foundational ambition for FNBM and for this reason it is important to appropriately position the various components in the Information Architecture Framework (e.g. Data platform, data labs, enterprise data warehouse, data reservoir, etc.) and to start unpacking associated model, data quality, metadata, privacy, etc. requirements. Please also consider the Model management framework, the Information Architecture Framework and Cloud Policy for further context regarding models and positioning of data product in the FirstRand Information Architecture Framework.

Following is a set of definitions for key analytic terms to ensure consistent interpretation and use across the Group. Whilst many definitions exist across the world, FirstRand adopted the following definitions from the European commission[17] and the European banking authority (EBA)[18] and will refine these for FirstRand purposes over time as the disciplines mature. It is recognized that the definitions of fast-evolving phenomenon such as big data must remain flexible to accommodate the inevitable need for future adjustments:

- **Advanced analytics** can be defined as ‘the autonomous or semi-autonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence’; it is often based on machine learning (ML), ‘to discover deeper insights, make predictions, or generate recommendations. Advanced analytics techniques include those such as data/text mining, machine learning, pattern matching, forecasting, visualization, semantic analysis, sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, simulation, complex event processing, neural networks.

  Different types of advanced analytics include: diagnostic analytics, predictive analytics, autonomous and adaptive analytics.

- **Data science** is an interdisciplinary field involving extracting information and insights from data available in both structured and unstructured forms, similar to data mining. However, unlike data mining, data science includes all steps associated with the cleaning, preparation and analysis of the data. Data science combines a large set of methods and techniques encompassing programming, mathematics, statistics, data mining and ML. Advanced analytics is a form of data science often using ML.

- **Artificial intelligence** - Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.

  As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)."

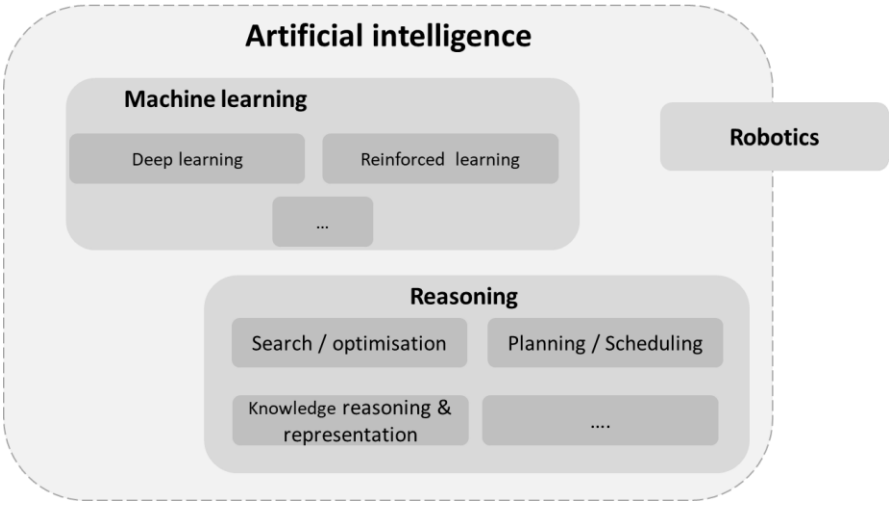
  An artificial intelligence system is regarded as any AI-based component, software and/or hardware. Indeed, usually AI systems are embedded as components of larger systems, rather than stand-alone systems. Humans design AI systems directly, but they may also use AI techniques to optimize their design.

- **Machine learning:** This group of techniques includes machine learning, neural networks, deep learning, decision trees, and many other learning techniques. These techniques allow an AI system to learn how to solve problems that cannot be precisely specified, or whose solution method cannot be described by symbolic reasoning rules

  - **Deep learning:** This approach refers to the fact that the neural network has several layers between the input and the output that allow to learn the overall input-output relation in successive steps. This makes the overall approach more accurate and with less need of human guidance.
  - **Reinforced learning**: Another useful kind of machine learning approach is called reinforcement learning. In this approach, we let the AI system free to make its decisions, over time, and at each decision we provide it with a reward signal that tells it whether it was a good or a bad decision. The goal of the system, over time, is to maximize the positive reward received. This approach is used, for example, in recommender system (such as the several online recommender systems that suggest users what they might like to buy), or also in marketing;
  - Neural networks are just one machine learning tool, but there are many others, with different properties: random forests & boosted trees, clustering methods, matrix factorization, etc.;

- **Reasoning/information processing and decision making**: At the core of an AI system lays its reasoning/information processing module, which takes as input the data coming from the sensors and proposes an action to take, given the goal to achieve. This means that the data collected by the sensors need to be transformed into information that the reasoning/information processing module can understand.

The figure below depicts most of the AI sub-disciplines mentioned above, as well as their relationship. It is important however to notice that AI is much more complex than this picture shows, since it includes many other sub-disciplines and techniques. Moreover, as noted above, robotics also relies on techniques which fall outside the AI space.



- **Big Data**: Technological change is leading to increasing amounts of data being collected, processed, shared and used in digital form at lower cost and on a larger scale. Managing data is not new but the ability to store huge amounts of data in any format and analyse it at speed is. The growing volume and increased analysis of data have led to the emergence of Big Data

  Big Data refers to large volumes of different types of data, produced at high speed from many and varied sources (e.g. the internet of things, sensors, social media and financial market data collection), which are processed, often in real time, by IT tools (powerful processors, software and algorithms). It is often characterized by the increased volume, velocity and variety of data being produced (the three Vs) and typically refers (but is not limited) to data from the internet. In addition, increased variability with respect to consistency of data over time, veracity with respect to accuracy and data quality, and complexity in terms of how to link multiple datasets are characteristics of Big Data.

The successful development, implementation and adoption of Big Data and advanced analytics is dependent on at least the following four areas and will require cross-functional engagement and commitment. The components interact with each other, are not mutually exclusive and are the preconditions for the effective implementation of the advanced analytics process:

- data management
- technological infrastructure
- organization and governance
- analytics methodology.

The role of information governance and information management will largely focus on the data management (e.g. information architecture, data quality, meta data, etc.) and governance aspects, whilst FNBM model governance and model management communities will be mainly responsible for the analytics methodology and development of models. IT is responsible for technology infrastructure and assistance with the model deployment in production.

10.7 Master and reference data management

Information sharing and operational collaboration has become a differentiating factor for organizational success and to use that information for both operational and analytical processes. Master and reference data management refers to a collection of business and technology capabilities that together enable the management and usage of master and reference data to support effective data sharing and use. These capabilities must be consistently leveraged across both the operational and analytical environments. Please refer to the Master Data Management Policy for more information.

Master and reference data management comprises the business processes, applications, repositories, methods, and tools that implement the policies, procedures and infrastructure to ensure accuracy, consistent use and control in the on-going maintenance and application of master and reference data:

- master data is a commonly agreed authoritative or trusted source of core data which is shared across many lines of business, processes and applications and requires consistent understanding and usage. Master data results from data integration, consolidation and de-duplication processes where multiple versions of data are transformed (mastered) into a single, trusted version; the latter which may also have been enriched or augmented. It represents the most accurate, consistent, complete and uniform set of unique identifiers and extended attributes, associated hierarchies, metadata, definitions, roles, connections and taxonomies that describe the shared data to be managed as master data.
- reference data is focused on defining and managing collections of slow changing common values to ensure consistent use within the Bank. Reference data can be defined internally, such as market segments, product categories, transaction codes, lookup tables (e.g. gender, marital status, etc.), status codes, role codes, etc. Reference data can also be defined externally by government, industry and standards authorities, such as currency codes, countries, tax rates, date/time zones, etc.

FNBM must explore, define and agree on why and where business users rely on master and reference data, the scope and management requirements thereof. Additionally, the Bank may require different views of master data; the definition of master data thus needs to consider the context in which the master data itself is used. Where business goals drive the need for master data to be managed on a FirstRand level, FNBM must decide what master data are to be considered as enterprise master data and handled as such.

Information owners must consider the following principles to assess the extent to which master data management is relevant and must be implemented per data theme. Master and reference data management must:

- be driven by business and developed in the context of business drivers that considers improvements in business process efficiency, innovation, information value and information risk mitigation;
- provide continued value delivery over the solution's lifecycle to better accommodate change in the definition, use, management and governance of master and reference data;
- ensure that accountability and ownership for master and reference data management is clearly defined throughout the master and reference data lifecycle. Individuals, groups, and their structures together with their responsibilities for authoring, managing and consuming master and reference data must be identified and documented;
- ensure that appropriate governance structures are implemented to facilitate effective decision making, controls and data sharing between cross-functional lines of business decouple master and reference data from silo-based business lines, processes and applications, making it available as a shared strategic data asset;
- ensure that roles are clearly defined with well-defined rules with regards to quality measures and procedures to govern the timing, resolution of conflict and maintenance of integrity across all applications where master and reference data is required to be synchronized across one or more consuming location;
- establish an environment where master and reference data management decisions and actions are in support of different lines of business, processes and applications;
- define processes for creating, validating and sharing of master and reference data;
- be an on-going data quality improvement effort, managed proactively and with the capabilities to improve the quality at source and thereby the trust in the master and reference data entities for the entire business. There must be a focus on on-going data quality management processes, whereby master and reference data is routinely profiled to determine its quality;

- support accurate and reliable data aggregation;
- maintain related data hierarchies over time;
- cater for versioning, synchronization and audit trails of changes;
- enable and support effective classification, change management and maintenance of the different metadata types;
- be protected from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability;
- ensure that changes are implemented in a timely and controlled manner, aligned to the needs of the business, architecture principles as well as regulatory or policy requirements; and
- accommodate existing application infrastructures in ways that are minimally disruptive yet provide a standardized path for transitioning to the synchronized master.

10.8 Information security management

Information security management controls whether the right individuals have access to the right information at the right time. Data must be protected while in transit as well as at rest, and authentication, authorization, access and auditing of information assets is managed in line with policy requirements:

- authentication: validated users are who they say they are;
- authorization: authenticated users are authorized with privileges that allow them access to specific and appropriate views of data, information or records;
- access: enable access rights based on their authorized privileges in a timely manner;
- audit: review of security actions and user activity to ensure compliance with regulations and conformance with policy and standards.

The information governance component of information security is limited to the principles related to the people and process components of information security and specifically excludes technology security. Please refer to the Data Protection Policy - suppliers, Information Security Policy, Data Privacy Framework and the requirements listed below.

- **People information security requirements**

People, whether internal or external, play a key role in the management and use of information and information systems. Special care must be taken to ensure that human resources information is accurate, information responsibilities are clearly understood, and information is sufficiently protected:

Prior to employment:
The following requirements are designed to ensure people understand their information and record management responsibilities and are suitable for the roles under consideration:

- information management roles and responsibilities of prospective employees, contractors and third-party users must be defined and documented; and
- successful job applicants must complete pre-employment screening in accordance with the relevant standards and policies.

During employment:
The following requirements have been designed to ensure people continue to understand their information management responsibilities and are suitable for the roles they hold:

- management must require employees, contractors and third-party users to apply information management controls in accordance with established policies and procedures;
- management must implement procedures to ensure employees, contractors and third-party users are trained and competent to use any important information processing facilities to which they have access; and

- all employees, contractors and third-party users must receive updates on relevant business policies and procedures and relevant information risk awareness materials.

Termination or change of employment:
The following requirements are designed to ensure information management objectives are not compromised as a result of people exiting the organization or changing roles:

- responsibilities for performing employee termination or change of employment procedures must be clearly defined and assigned; and
- responsibility must similarly extend to contractors and temporary staff.

10.9 Data privacy management

All personal information must be treated with the utmost care and responsibility whenever and however it is processed by FNBM or its partners. The collection, processing, storage, dissemination and destruction of personal information must be done in accordance with the records management and the Privacy Framework and supporting data privacy policies.

the Privacy Framework identifies four key deliverable sets, enabling the Bank to achieve and maintain compliance to data privacy and protection legislation and regulations:

- artefacts that drive privacy governance for the Bank, including the Privacy Framework and the supporting privacy policies;
- deliverables that deals with the rights of a data subject as described in privacy legislation. These deliverables will be focused mainly on conduct related matters, which includes data subject rights (such as consent/non-consent to direct marketing, which has been specified in the Marketing Policy).
- deliverables that relate to information governance matters, including but not limited to: data classification; records management and data quality.
- deliverables that relate to information security policies and standards; and information security risks and practices managed by the information security community.

In respect of the third set, the data privacy community, which includes the Data Privacy officers(as set out in the Privacy Framework), is required to contribute and provide input to information governance related deliverables such as data classification, records management and data quality, enabling compliance to certain privacy principles and requirements(as set out in privacy legislation and regulation) relating to records retention and destruction; processing of personal information limitations; and data quality and accuracy of personal information.

The data privacy community is expected to identity and define the privacy risk profile for the FirstRand Group (including the privacy risk profiles at a segment and brand level), and same will be reported to the Information governance committee.The applicable privacy principles are as follows:

- Privacy Principle 1: Accountability
- Privacy Principle 2: Processing Limitation
- Privacy Principle 3: Purpose Specification
- Privacy Principle 4: Further Processing
- Privacy Principle 5: Information Quality
- Privacy Principle 6: Openness
- Privacy Principle 7: Security Safeguards
- Privacy Principle 8: Data Subject Participation
- Privacy Principle 9: Cross Border Transfer of Personal Information

- Privacy Principle 10: Third Party / Operator Management

Please refer to the FirstRand Internal Privacy Policy for

detail.

10.10 Data storage and operations management

Data operations management provides support from data acquisition to data purging, and includes database support and data technology management:

- business must ensure that all important information and physical assets associated with important information processing facilities are owned by a responsible individual or a designated part of the business;
- on a risk-assessed basis, selected duties and areas of responsibility (IT and business) must be formalized and segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Bank's information;
- development, test and operational facilities for material processes must be separated to reduce risks of unauthorized access or unwanted changes to operational information.
- Data that is stored must be in accordance to the FNBM information architecture components storage standards (please also refer the Information architecture and Data integration policies):
  - data duplication must be avoided where possible within the data platforms;
  - data types and formats must be optimized efficiently to avoid data storage infrastructure wastage
  - temporary data used in data integration or transformation must be programmatically removed as soon as the data is no longer required. Temporary data is subject to the same security and risk controls as permanently stored data;
  - data must be secured based on the IT and Data Security Policy requirements.
  - data storing must have defined and implemented controls, monitoring, alerting and reporting.

10.11 Data development, interoperability and data integration management

This section of the framework covers key requirements and references to relevant FNBM policies and standards related to the management of software development processes and introduces key concepts from a data interoperability and data integration management perspective.

Data development management is the analysis, design, implementation, deployment and maintenance of data solutions to optimize the value of information to the Group. It includes the subset of project activities within the software development life cycle (SDLC) focused on defining data requirements, designing the data solution components and implementing these components.

Please refer to the requirements set out in the Information life cycle management section of this framework under the sub-title ´change the business´ and the Project Risk Management Framework.

Data interoperability is the ability for systems and organizations to work seamlessly together, based on common standards; systems and services that create, exchange and consume data have clear, shared expectations for the contents, context and meaning of that data.
Interoperability is a characteristic of good quality data, and it relates to broader concepts of value, knowledge creation, collaboration, and fitness-for- purpose. Before any decisions can be made on the degree to which a dataset must be made interoperable, careful consideration must be given to what the intended and anticipated use case of a dataset or system will be.
Maximum levels of interoperability are not always desirable and can in fact be harmful or even unlawful (e.g., if they result in the unintentional disclosure of personal data). A significant data interoperability challenge relates to how the structure and description of data and metadata can be organized consistently. Interoperability is highly

dependent on data and metadata modelling decisions and practices. To expose data without ambiguities and ensure semantic interoperability, it is crucial to focus on the adoption of standard vocabularies and classifications early on, starting at the design phase of any new data collection, processing or dissemination system.

Application program interfaces (API) are highly-reusable pieces of software and are at the heart of enabling multiple applications to interact with an information system. They provide machine-to-machine access to data services and provide a standardized means of handling security and errors. APIs must be designed with the needs of application developers in mind, focusing on helping them create information products that satisfy the requirements of end users and provides the ability for systems to seamlessly work together based on common standards. In this context, APIs need to be well documented, easy to understand, and easy to integrate with other systems in order to support effective data interoperability.

Interoperability has a close connection to data 'integration' which is the act of incorporating two or more datasets into the same system in a consistent way. Data integration is one of the possible outcomes of data interoperability.

Data integration enables and controls the movement of all data at differing speeds between systems and data stores. Movement of data, in its purest form, means transporting of data to storage locations in the overall data landscape reflecting any security, compliance, and other standards. Data cleansing, matching and other data related processing tasks are performed by this component. Data Integration deals with all internal and external systems, cloud offerings and 3rd party services and APIs.

The goal of information and data integration management is to establish a holistic and congruent capability to direct management effort and its data resources in an integrative manner to realize maximum information benefit to the Bank.
Integration efforts are redirected as leveraging of the various available technologies in the Group becomes more prevalent. Information and data integration does not imply one single repository or source. This contributes and enables the fulfilment and increased focus on the data strategy and the formalization of the overall management of information as a strategic enabler. Integration of information and data is architecturally dependent on the deployment considerations of the brands internal resources and technology capabilities, these
architecturally components are to be maintained and management to provide optimal efficiencies and make available the information and data as key strategies. Please refer to the Data Integration Policy for a set of principles that have an impact on the data integration landscape. Notably, the Integration Policy aims to navigate the shift from batch/ ETL driven integration to more real time integration patterns, by introducing real time integration patterns as preferred. This creates new possibilities in the exploitation of the data for real time decision making and analytics.

10.12 Information rchitecture management

Architecture describes how a diverse set of components fit together and interact to fulfil a purpose or meet needs. In the same way, information architecture describes, through a set of requirements, principles and models how information is shared and exchanged. It provides a view of the current and future state architecture.

Information architecture management defines the sources and destinations of information, its flow through the organization, as well as the rules for persistence, security and ownership. The focus of information architecture management is on information assets that are deemed to have recognized significance and are necessary to achieve effective business change and management.

Management must design, build and maintain information architecture and IT infrastructure which fully supports its business strategy, operations, regulatory requirements, including data aggregation capabilities

and reporting practices, not only in normal times but also during times of stress or crisis. The Information Architecture Policy defines the essential components of information architecture, design approach, minimum standards as well as the relationships between these components.

Apart from the information management principles already stated, architects, developers and business users who develop applications or models must ensure alignment with the following information architecture principles:

- information architecture is driven by business requirements and strategy;
- promote reuse through architectural patterns and master data management;
- information flows of material data elements or business processes must be documented - for both internal and external data;
- information modelling must be an integral part of information system development effort;
- align business information and technical architectures; and
- development of information services (such as business applications, data warehouses, directory services, etc.), available across the Bank is preferred over the development of information silos which are only provided to a particular department or group of departments.

Data gravity is defined as the economic pull of data to its most natural resting place. As the locational creation of data shifts from internal to external data sources there will be a corresponding shift of data gravity from on-premise storage to off-premise storage. The applications used to do transactions, queries, analysis, etc. usually work best when located close to the data. Because the greater the network distance between data and application, the longer each interaction takes – i.e., the greater the latency. As operational source systems pivot into the cloud, analytic repositories will follow suit. Application performance is why we care about gravity and latency and why this must be carefully considered when choosing cloud implementations.

A spirit and culture of collaboration and the sharing of information for the greater corporate good shall pervade all decision making, especially relating to the selection and prioritization of programmes, projects and their approval points.

11. INFORMATION LIFECYCLE MANAGEMENT

To ensure the appropriate identification, selection and design of information controls, management must ensure that the requirements stipulated in this framework are considered when business processes are designed, enhanced and implemented.

Roles must be established for ownership and quality of data for both the business and IT functions to ensure adequate controls throughout the lifecycle for the data and for all aspects of the technology infrastructure:

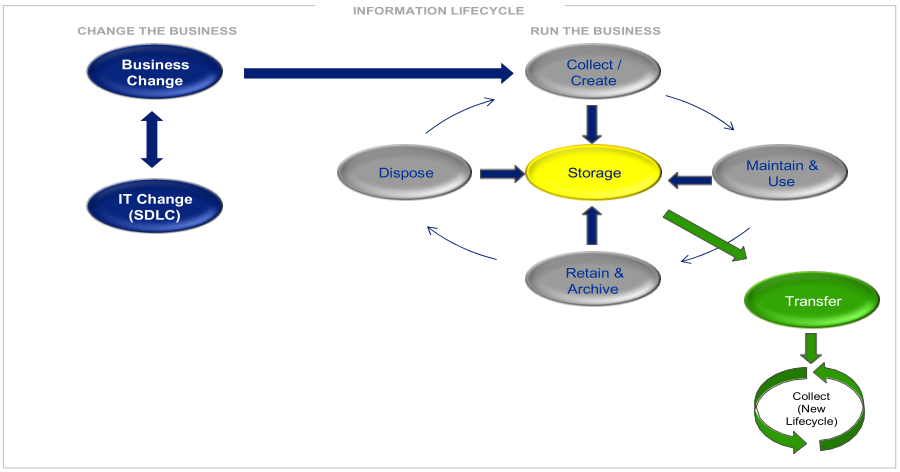


Figure 6: Information lifecycle

11.1 Change the business

Business and IT management must ensure that information-related risks associated with business and IT changes are managed and that change management processes and procedures are in place:

- **Requirements analysis**: Business and IT changes are confirmed, defined and assessed for impact on data paths and information assets prior to approval of changes (this includes legal, regulatory and policy requirements related to information);
- **Design**: Information requirements are refined and adequately captured in architectural and process designs prior to changes to business and/or IT environments. The impact on existing or need for new information management roles have been articulated and included in the design specification;
- **Development and testing**: Software development and testing is managed in such a way that integrity, security, usability, maintainability, retention and disposition of information is aligned with business, regulatory and legal requirements;
- **Training**: Staff is trained to understand the context and importance of key information assets and how it impacts the usage and interpretation within the business and application thereof; and
- **Post-implementation review**: Business stipulated information requirements for changes made to the business and/or IT environments are adhered to and the implemented system conforms to the architectural designs. Monitoring and assurance of information related requirements against legislation and policies.

11.2 Run the business

Business management ensures that key information management controls are identified and implemented across the information lifecycle to support the effective day to day running of their business as follows:

- **Create and collect**: Downstream impact on business operations is minimized by ensuring that quality thresholds and system validations are implemented at the point of data collection/creation.

- **Maintain and use**: Information can be accessed and updated in a timely, reliable and cost-effective fashion. Additionally, the integrity and confidentiality is maintained and the detection of failed transactions does not disrupt the processing of valid transactions.
- **Retain and archive**: Information assets are retained securely, in line with regulatory requirements (refer to the Records Retention Standard) and remain accessible while maintaining the integrity and confidentiality thereof.
- **Store:** Information assets are stored in a stable, reliable, secured and controlled environment in order to maintain their integrity, usability and accessibility, also for business continuity and disaster recovery purposes.
- **Dispose:** Information assets that have been authorized for destruction are disposed of securely in accordance with the applicable confidential methods of destruction.
- **Transfer (exchange of information)**
  - data is not copied, unless for good reason. Creating a persistent copy of data will only be undertaken when all other avenues have been exhausted;
  - data lineage is clearly documented;
  - data transfers adhere to policy and regulatory requirements;
  - information is checked for authenticity of origin and integrity of content, before and after the transfer process ;
  - agreements must be established for the exchange of information and software between the organization and external parties (customer/clients or third parties); and
  - media containing important information is protected against unauthorized access, misuse or corruption when transported beyond the Bank's physical premises.

12. POLICY LIFECYCLE MANAGEMENT

The objective of this section of the framework is to outline how the policy and standard hierarchy for information governance and management within the FNBM fits together and defines the maintenance requirements that must be in place to ensure supporting policies and standards remain up to date, meet regulatory requirements and remain in line with the business needs.

The Information Governance Policy Framework establishes the expected control environment for the management of information within FNBM. It details how the IGF and related Information Management policies and standards will be structured and implemented in order to ensure the ongoing quality and protection of records and information:

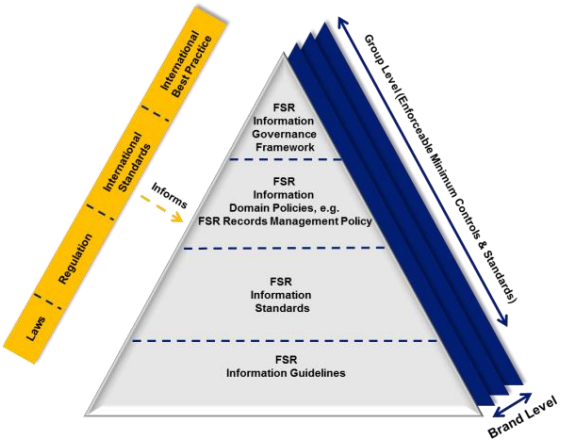


Figure 7: Information Governance Policy Framework

Table 2: Layers of the Information Governance Policy Framework

Layer	Responsibility	Final approval
Tier 1 –Information Governance Framework	MRCC	RCCC
Tier 2 –Information Domain Policies Information Domain Policies support the implementation of the IGF and other relevant policies by providing a framework of principles, objectives, control statements, key processes and roles per information management domain (e.g. records management) to enable consistent management of the domain within the Group. A policy is typically a document that states specific requirements or rules that must be met. Brand level policies must only be created in exceptional cases.	IGC	MRCC
Tier 3 –Information Standards These standards promote consistency and further extend FNBM information policies for specific areas of focus (e.g. imaging) in relation to information management domains. It includes information specific requirements or rules that must be met by everyone. Standards do not include information on *how* standards must be met.	Information Governance Owner	IGC
Tier 4 –Information Guidelines To provide guidance on how to implement and ensure compliance to information policies and standards. Guidelines are not requirements to be met but are recommended best practice in the Bank´s context.	Information Governance Owner	IGC for noting

The management and maintenance of the policies is important in ensuring thesecontinue to address the risks that FNBM faces. Failure to ensure that policies and standards remain up to date will result in information policies and standards preventing the mitigation of information risks.

Information policies, standards and guidelines must be reviewed annually. The following actions must be carried out to maintain the IGF policies and standards:

- version control and change management;
- policy and standard maintenance;
- change management;
- review cycles;
- decommissioning of existing policies and standards;
- identification and management of dependencies; and
- publication and communication of standards and policies.

ANNEXURE 1: ACRONYMS

Acronym	Description
AI	Artificial intelligence
API	Application program interfaces
BCBS	Basel committee for banking standards
BI	Business intelligence
BPRMF	Business Performance and Risk Management Framework
CAD	Computer aided design
CDO	Chief data officer
CEO	Chief executive officer
CIO	Chief information officer
CM	Content management
CTO	Chief technology officer
DAMA	The Data Management Association
DM	Document management
DMBOK	Data Management Body of Knowledge
DW	Data warehousing
EBA	European Banking Authority
Entity	Refers to any legal and/or management entity, division, business unit or activity under the umbrella of FirstRand Limited, including committees and subcommittees thereof
ERM	Enterprise Risk Management
ETL	Extract, transform, load
Exco	Executive committee
FirstRand	FirstRand Limited
GDPR	General data protection regulation
GIA	Group Internal Audit
GIG	ERM Information Governance
GISO	Group information security officer
Group	FirstRand Limited
FirstRand IGC	FirstRand information governance committee
IAR	Information asset register
IGF	Information Governance Framework
IT	Information technology
ITAB	Information technology architecture board
KDE	Key data elements
ML	Machine learning
ORC	FirstRand operational risk committee

ORMF	Operational Risk Management Framework
PI	Personal information
POPIA	Protection of personal information act
PRICA	Prevention and combating of corrupt activities act
RCCC	FirstRand risk, capital management and compliance committee
RFC	Request for comments (relevant for frameworks, policies, etc.)
RM	Records management
RMP	Risk management plan
RRM	Regulatory Risk Management
SDLC	Software development life cycle
SPI	Sensitive personal information

ANNEXURE 2: EXTERNAL FRAMEWORKS, METHODOLOGIES AND STANDARDS

Listed below are the key external references that were used to compile this document.

Ref no	Description
1	King IV Code of Governance Principles
2	King IV Report on Governance
3	BASEL Principles for effective risk data aggregation and risk reporting (BCBS 239)
4	The DAMA Guide to the Data Management Body of Knowledge (DAMA- DMBOK Guide)
5	European commission report: A definition of AI: Main capabilities and discipline
6	European banking authority: Final report on big data and advanced analytics
7	European commission: Ethics guidelines for trustworthy AI
8	Select ISO standards
9	Gartner CDO Circle participation – Data literacy
10	IBM “Ethics and big data analytics” report
11	The information accountability foundation (Martin Abrahams) – The origins of personal data and its implications for governance

ESRA Policy

First National Bank Mozambique – February 2020

TABLE OF CONTENTS

ESRA POLICY

1. INTRODUCTION AND PURPOSE

1.1 What is ESRA?

ESRA is the acronym used for an '**Environmental and Social Risk Assessment**'. ESRA forms part of the "Desirability Test" of the credit approval application process. Environmental and social risks are risks that relate to specific activities and sectors which increase the probability that commercial and industrial activities and human intervention will cause and lead to degradation of the environment or have a significant social impact.

Through its lending and investment practices, FNB Mozambique ("the bank") is subject to environmental and social risks. These risks pertain to sector specific activities that could potentially yield environmental degradation and significant social impact. The assessment of these risks ensures the management of the environment and the consequential risk to the business of the client and, ultimately to the bank. These risks are managed through conducting a due diligence process through the Environmental and Social Risk Assessment (ESRA) tool, in alignment with The Equator Principles (EP).

For the bank, environmental risk mainly manifests itself as a credit risk e.g. if the client is unable to pay its debts because of environmental liabilities or actions by authorities, a legal liability or criminal sanction as a result of a statutory provision, or reputational risk as a result of negative publicity or public perception. Social risks include labour issues, occupational health and safety, community involvement, human resettlement, indigenous people rights, including human rights. These risks could lead to criminal sanctions, termination of operations, production losses and subsequently a financial or credit risk to the bank.

In 2009, the Environmental and Social Risk Assessment (ESRA) process was implemented across FirstRand South Africa (FirstRand), which was aligned with its adoption of The Equator Principles (EP) in July 2009. The Equator Principles is an internationally recognized best practice related to the management of environmental and social risks as credit risks in larger investment banking financing transaction types. The full text of The Equator Principles can be found at www.equator-principles.com.

ESRA, which encompasses the application of EP is the review conducted by lending officers, when reviewing a loan or credit application, of the direct environmental and social risks that may be associated with a client of the bank or their activities, in order to determine what indirect environmental and social risks the bank may face by lending to the client and how well the client manages these risks.

1.2 Guideline Governance

This policy is an extension and not a substitution of the FirstRand Guideline for the Management of Environmental and Social Risks in financing but is specific to FNB Mozambique. The FirstRand guideline is an operational tool of the FirstRand Environmental Risk Framework, a sub-framework of the FirstRand Regulatory Risk Framework and the FirstRand Credit Risk Framework. The main policy related to these guideline documents is the FirstRand Environmental Sustainability Policy.

To avoid frequent reviews, the FNB Mozambique ESRA policy will be subject to periodic updates as and when required, as well as a comprehensive review annually to view its suitability, appropriateness and effectiveness. The policy will further be reviewed by the FirstRand Rest of Africa Environmental and Social Risk team and approved by the Senior Credit Risk Committee and appropriate governance structures.

1.3 Benefits of Implementing the ESRA Process

The benefits of implementation of an environmental and social risk assessment process will provide the bank with protection against typical risks associated with investment and lending, such as:

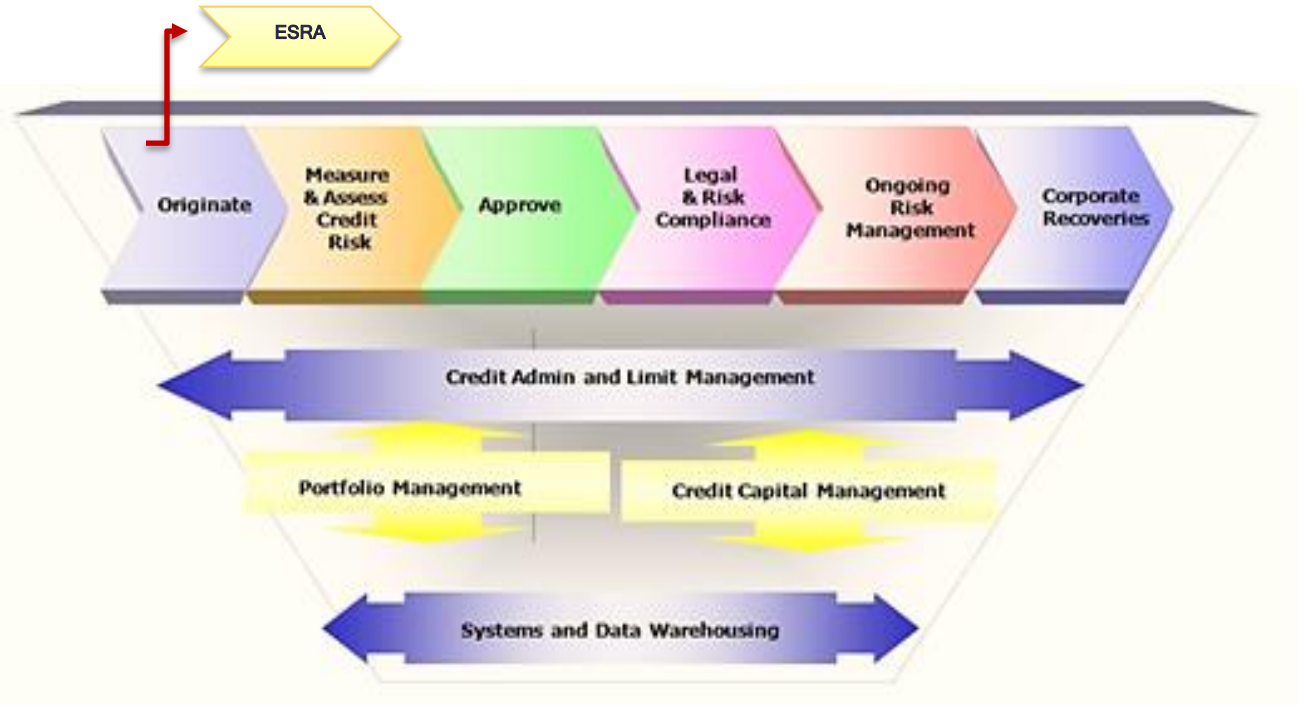
The prevention and mitigation of environmental and social risks by clients reduce the possibility of:

- Increased costs to the client; including costs due to regulatory fines or third-party lawsuits (e.g. for contamination clean-up)
- loss of revenue and/or share value due to unsafe or unsustainable activities;
- The client defaulting because of environmental or social liabilities

- The value of the banks security being reduced or incorrectly valued as a result of contaminated property;
- The bank incurring potential loss of assets associated with the transaction;
- Damage to reputation for negatively impacting society through the association of providing facilities to clients whose activities have negative impacts on the environment and society; and
- Through the ESRA process, the identification of environmental and social risks may result in opportunities for the bank by providing facilities to clients which may result in positive E&S impacts on society. This might include, projects that promote sustainable environmental practices or empowering communities, leading to increased profitability and longevity of business activities due to sustainable business practices

1.4 Structure

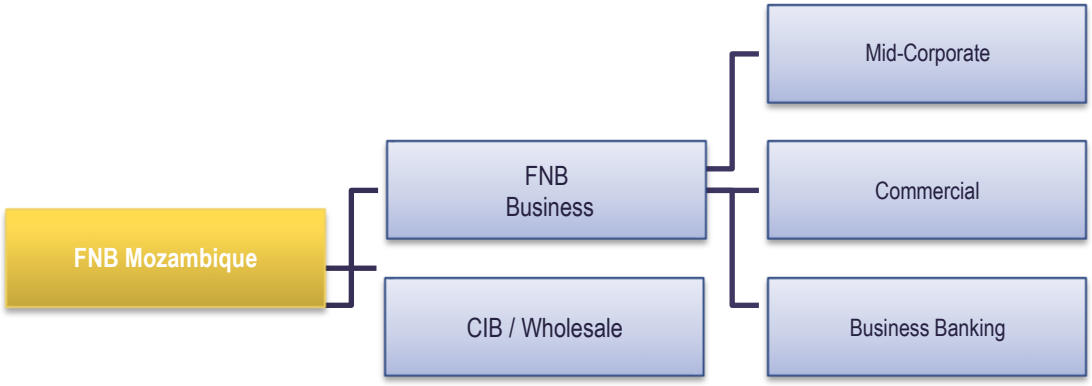
The diagram below is a high-level representation of the credit process and credit model applied. The ESRA process is an integral part of the credit approval process and is applied at credit origination prior to credit approval.



2. SCOPE AND APPLICATION

This policy applies to all corporate, commercial and business transactions, employees and operations undertaken through FNB Mozambique. All FNB Mozambique transactions with impending environmental and social risks shall be reviewed as per the ESRA review process prior to processing for credit approval. Employees will be required to adhere to the latest approved version in circulation.

The ESRA process is applicable to the following business units and services within FNB Mozambique:



2.1 Excluded/Exempted Transaction Types

The ESRA review process is **not** applicable to the following transaction types across the bank:

- Personal loans
- Insurance products
- Overdrafts approved for working capital purposes
- Contingent Facilities
- Settlement and Pre-settlement Facilities
- Share Based Lending and Preference Shares
- Retail Business
- Category C classifications (as determined by the ESRA automated tool)

2.2 Annual Reviews / Renewals

- Straight annual reviews/renewals are excluded from the ESRA process.
- All annual reviews with changes to the facility must be loaded on the ESRA tool with the required note (deal notes on the ESRA tool) confirming that it is an annual review with facility changes. This will assist the ESRA specialist in determining if a review will be required based on the nature of the facility changes or client operations.
- Annual renewals / reviews for activities falling within the FirstRand exclusions list and sensitive industry matrix will be applicable for an ESRA review and credit/credit committee must ensure that the transaction is referred for an ESRA review upon the annual review/renewal.

NB: The following principles apply to excluded transaction types (2.1 above) and annual renewals/reviews (2.2 above) as follows:

1. All transactions are still subject to the desirability matrix, excluded activity list and sensitive industry matrix
2. Credit / Credit committee or the ESRA specialist has the discretion to request that an ESRA review be performed on any transaction (irrespective of the transaction type) including category C where the assessment of the client's activity or the property valuation (collateral) indicates that there may be an environmental or social risk attached to the lending.
3. Credit is further responsible to ensure that the categorisation and activity selection as per the ESRA questionnaire results is accurately selected in relation to the client's activities and funding requests. This is an important check for credit to undertake especially for category C transactions where ESRA reviews are not required.
4. Credit/ Credit committee must ensure that all transactions which fall within the excluded and sensitive industry matrix are referred for an ESRA review to ensure that facilities are provided in line with the position statements where applicable.
5. The ESRA specialist has a discretion to review transactions on high risk activities (category A) irrespective of the nature of the transaction.
6. If there is any doubt about a transaction, guidance should be sought from the ESRA specialist/team.

3. THRESHOLD AND COMMITMENT

FNB Mozambique is committed to the management of the ESRA process through:

- Managing all identified environmental and social risks as a result of the bank's lending activities through an Environmental Social Risk Assessment (ESRA) due diligence process.
- Periodically reviewing transactions and trends and systematically reducing transaction thresholds through a management plan until a zero threshold is achieved. The transaction threshold for the roll-out of the ESRA process is as follows:

4. REGULATORY/ LEGAL PRINCIPLES

4.1 Environmental Law (Law n.º 20/97, of 1 October) , 1997 of Mozambique and Environmental Impact Assessment Regulation (Decree 54/2015, of 31 December)

Although the act does not make direct reference to lender liability, the bank faces continual exposure and can be indirectly affected through financing of clients with identified potential environmental and/or social risks. Sound practice and proactive risk management will require the bank to ensure the following environmental management principles as detailed as per the act are not compromised by clients. These include:

- Non-renewable resources must be used on a sustainable basis for the benefit of present and future generations;
- Community involvement in natural resources management and the sharing of benefits arising from the use of the resources, must be promoted and facilitated;
- Assessment, licencing and registration must be undertaken for activities which may have a significant effect on the environment or the use of natural resources;
- Sustainable development must be promoted in all aspects relating to the environment;
- Mozambique's cultural and natural heritage including, its biological diversity, must be protected and respected for the benefit of present and future generations; the option that provides the most benefit or causes the least damage to the environment as a whole, at a cost acceptable to society, in the long term as well as in the short term must be adopted to reduce the generation of waste and polluting substances at source;
- The reduction, re-use and recycling of waste must be promoted;
- A person or entity who causes damage to the environment must pay the costs associated with rehabilitation of damage to the environment and to human health caused by pollution, including costs for measures as are reasonably required to be implemented to prevent further environmental damage;
- Where there is sufficient evidence which establishes that there are threats of serious or irreversible damage to the environment, lack of full scientific certainty may not be used as a reason for postponing cost-effective measures to prevent environmental degradation; and
- Damage to the environment must be prevented and activities which cause such damage must be reduced, limited or controlled.

5 THE ENVIRONMENTAL AND SOCIAL RISK ASSESSMENT PROCESS

The bank embraces sustainable development practices in its financing and lending process by integrating social and environmental management principles into its credit decision-making processes and commits to promote environmental and social management and sustainability by:

- Defining the requirements for environmental and social risk assessment and monitoring on transactions;
- Developing and communicating environmental and social performance standards that clients will be expected to meet within an acceptable time frame; and
- Defining environmental and social roles and responsibilities for both the bank, and its clients.
- Providing continuous/ periodic training to relevant stakeholders (i.e., credit, business, Exco, board of directors etc.) on environmental and social risks and developing trends in regulation.

The environmental and social risk assessment should be appropriate to the nature and scale of the activities involved in the transaction and proportional to the level of environmental and social risks and impacts. For transactions, which meet the criteria of The Equator Principles, or relevant corporate loan criteria as per DFI funding requirements, the bank

requires adherence to the International Finance Corporations (IFC) Performance Standards and makes use of their sector specific Environmental, Health and Safety (EHS) Guidelines together with the World Bank Guidelines as prescribed by The Equator Principles.

For all other corporate or commercial related lending and investment transactions where the use of the proceeds is known, the bank requires compliance by our clients against all relevant local and national environmental, health and safety legislation, impact assessment, permitting and public commentary processes etc.

6 EXCLUDED & SENSITIVE ACTIVITIES AND INDUSTRIES MATRIX

The Excluded & Sensitive Activities and Industries Matrix was developed to provide guidance to key stakeholders in the negative/exclusionary screening process which forms part of the ESRA process. Activities listed on the matrix potentially raise significant environmental and social issues which require a position to be taken by the bank regarding potential lending to these industries. FNB Mozambique is required to adopt the sensitive industry matrix in line with requirements of local Mozambique laws.

The matrix and respective supporting documents define the industries which the bank and the wider FirstRand Bank group will not finance/ or invest in or provides restrictions on the financing and investment available to sensitive industries. Restrictions are primarily based on the following principles:

- Activities may be illegal in terms of national or international laws and treaties;
- The bank or group has agreed to financing restrictions imposed by financing agreements with development funding institutions (DFIs);
- The bank or group has made an ethical/moral decision not to be involved in certain industries which may be controversial and may suffer reputational damage as a result of association;
- Internal risk appetite; and
- Alignment with approved bank or wider group strategy.

The updated excluded & sensitive activities and industries matrix together with detailed position statements governing the sensitive industries/ activities is located on the ESRA tool and can be accessed using the following link: https://FirstRandgroup.sharepoint.com/sites/FCCESRA/ESRA%20documents/Forms/AllItems.aspx?FilterField1=Categories0&FilterValue1=Sensitive%20and%20Excluded%20Industries&FilterType1=Choice&viewid=97e9bafa%2D134b%2D4d25%2D825a%2D67bb991a0985

6.1 Application of the Excluded & Sensitive Activities and Industries matrix

ESRA applicable transactions: The industry or client activity is screened by using the ESRA online application together with position statements governing the industries/activities. Excluded activities are prohibited and will not be financed

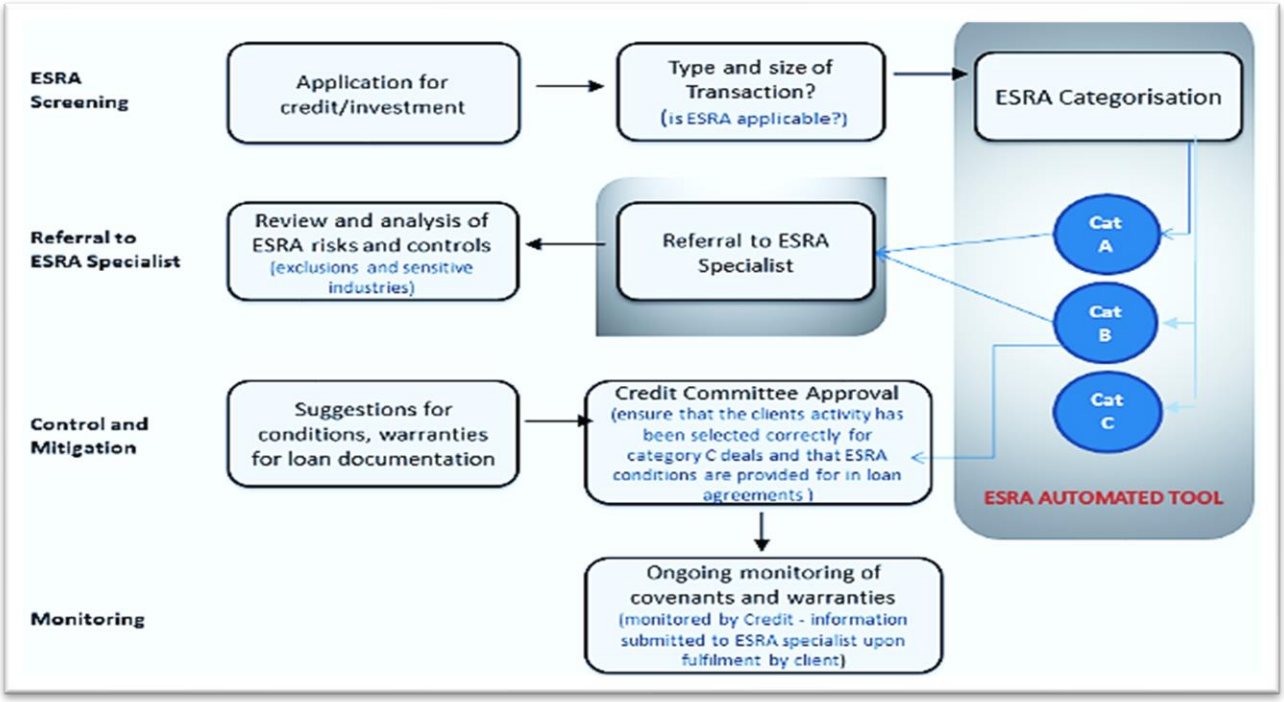
whilst activities identified as sensitive or restricted are referred to the ESRA Specialist as part of ESRA review process for enhanced due diligence and suitable recommendations if approved.

Non-ESRA applicable transactions: In cases where transactions are exempted from the ESRA process, the relationship manager/ transactor and credit managers are also responsible to ensure that where facilities are requested for activities that fall on the excluded and sensitivity activity and industry matrix, this is referred to the ESRA specialist for review where required.

Where a client's activity falls within the excluded and sensitive industries and activities matrix and where concerns have been noted by the ESRA team, the credit team or any other stakeholder involved, the process of escalation must be followed. (see 7.8 below).

7 THE ESRA PROCESS

The generic ESRA process can thus be summarized in the following generic ESRA process diagram.



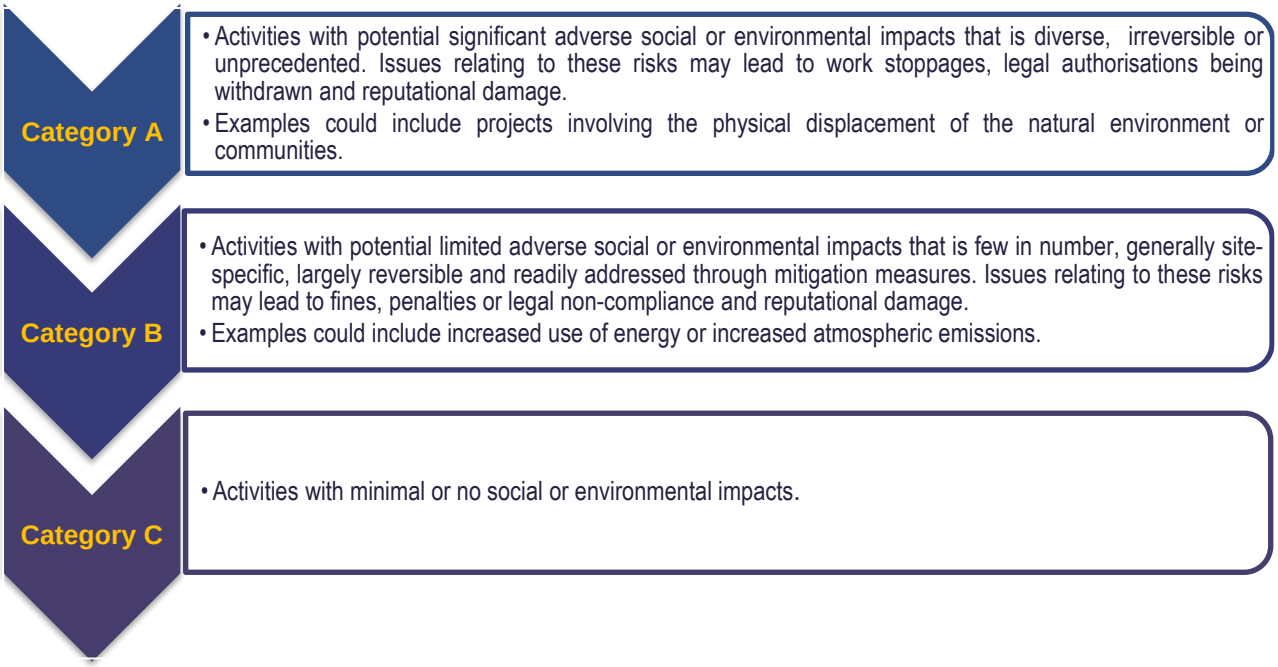
7.1 ESRA transaction categorization & screening

Assessment and management of environmental and social risks associated with a particular credit application or investment proposal is integral to the credit decision-making process. The timely and correct identification of environmental and social risks will assist the bank in making the correct credit decision and will reduce the risk of

incurring direct or indirect liability and lender liability and / or attracting potential negative publicity. The main objectives of screening transactions and conducting an environmental and social risk assessment (ESRA review) are as follows:

- To ensure the clients activities for which financing is being provided follow the banks environmental and social requirements;
- To identify both risks and opportunities and to ensure that all relevant risks have been considered in providing finance or investment by the bank; and
- To avoid potential environmental and social liabilities that could affect the longevity of the client and/or the facility being provided to the client.

As part of the screening of a transaction's potential environmental and social impacts, FNB Mozambique uses an online tool (ESRA tool) for environmental and social categorization to reflect the magnitude of potential impacts identified on a specific transaction. The screening and categorization process is initiated by the bank's transactor/relationship manager by completing the ESRA tool with specific transaction related information (i.e. client request, facility type, amount, sector, activity etc.) and submitting the online request for categorization. Transactions are categorized into 3 categories based on the level of environmental and social risk associated with a specific transaction:



Once a transaction has been submitted on the ESRA tool for categorization, the online tool produces a "pdf" document that defines the ESRA categorization for the specific transaction. The tool and the "pdf" document will also indicate whether any of the following apply to the transaction:

- Whether the transaction is an Equator Principles related transaction type (which will require stricter screening);
- Whether the transaction involves an activity that is included on the bank's exclusions list; and

- Whether the transaction involves an activity which is considered a sensitive industry in terms of the bank's sensitive industry and activity list.

All identified excluded activities within the online tool will automatically be categorized by the tool as a category A transaction and will be referred to the segment ESRA specialist/team for further action.

In the event that a transaction is categorized as a category A or B transactions, the "pdf" document and the online record within the ESRA tool of the transaction will indicate the possible initial documents to request from the client in order to mitigate generic environmental and social risks associated with that particular activity. If the transactor/relationship manager has any of the documentation requested at hand, this can be loaded onto the ESRA tool for the ESRA specialist/team to review. Documentation requested will vary per transaction based on the activity being screened and the categorization of the transaction and the ESRA specialist/team may request further information and documents via the transactor/relationship manager to obtain from the client when undertaking the risk mitigation and compliance review.

7.2 Referral to ESRA Specialist / Team

Once a transaction has been logged on the online tool and submitted for categorization, the online tool will automatically notify the relevant ESRA specialist that a transaction has been logged via the ESRA tool:

- If the transaction is a Corporate /CIB transaction, and the transaction will be booked on the South African balance sheet, it will be referred to the appropriate group ESRA specialist for assessment.
- All Corporate/ CIB transactions that are booked on the in-country balance sheet will be screened by the FNB Mozambique ESRA specialist/team.
- If the transaction is a Commercial or business transaction, it will be referred to the FNB Mozambique ESRA specialist/ team for screening.
- If the transaction is an Equator Principles category A or B transaction, it will be referred to the appropriate group ESRA specialist and an independent Equator Principle's compliance report must be submitted by the client to the bank;

The transactor/relationship manager is to submit via the online tool, the draft credit application or alternative (i.e. pre-screen document, forum paper or any other transaction related note/document) for that specific transaction as well as any environmental and social documentation obtained from client as requested by the ESRA specialist for consideration and review. Once submitted, the transaction is logged and saved in an online database on the ESRA tool and can be accessed by the transactor/relationship manager who logged the transaction, as well as by the ESRA Specialist. The transactor/relationship manager can view only their own transactions logged, whilst ESRA specialists have an overview of all the transactions captured on the system for the bank.

Where it is identified that the transaction has been categorized aggressively by the tool based on various factors and where a transaction appears to have a lower risk depending on the nature of the transaction, then the ESRA specialist/team may allocate, at their discretion, the correct category in line with the risk associated. Where significant material changes are made, then the ESRA specialist will consult with the Head of Credit (or his/her alternative) and the CRO accordingly. **NB:** This rule will only apply where the ESRA specialist makes a judgmental decision to change the risk category and not in instances where the transactor/relationship manager has selected the wrong information (i.e. transaction type, monetary amount, sector and activity etc.) on the tool leading to the incorrect categorization of the transaction.

7.3 ESRA Risk Mitigation and Compliance Review (ESRA Review)

This step involves the ESRA specialist/team applying their expertise to the types of environmental and social risks applicable to the specific activity for which finance or investment is being requested. In considering a new credit application for finance or an upgraded facility or extension, the following aspects must be considered by the ESRA specialist/team:

- Potential environmental and social risks and impacts which may lead to liability or risk for the client and the bank if associated with the activity for which finance is being provided. These may include:
    - *Environmental factors*: Release of air pollutants (air emissions), release of liquid effluents or contaminated wastewater into local water bodies or improper wastewater treatment, generation of large amounts of solid waste and improper waste management, improper management of hazardous substances, excessive energy use, excessive water use, high or excessive noise levels, improper or excessive land use, destruction of areas rich in biodiversity etc.
    - *Social factors*: Occupational health and safety issues (i.e. physical hazards, chemical hazards, biological hazards, ergonomic hazards exposure to employees etc.), labour issues (i.e. contract mismanagement, exploitation of workers, lack of freedom of association or grievance mechanisms, exploitation of young workers or student workers, discriminatory hiring and promotion practices etc.) and community related issues (i.e. release of pollutants and harmful dust into ambient air, strain on local water supply, exposure to hazardous substances, Increase of disease vectors from failure to manage liquid and solid wastes, release of unpleasant odors, excessive noise etc.)
- The commitment, capacity and appropriate mitigation measures taken by the client to manage these risks (i.e. by requesting reports/processes or documents relevant to environmental and social matters compiled internally by the client or by external stakeholders on behalf of the client, assessing client's websites (where applicable) for environmental & social related information and conducting internet based searches on the client taking into

account key environmental and social aspects to identify if there are any issues that were highlighted in the media etc.;

- The review of the facility or transaction in the light of present environmental legislation and receipt of the necessary statutory environmental certificates and social permissions, or the confirmation that these will be granted;
- The evaluation of the facility/transaction, design and technology, including verification of the technical and financial ability and willingness of the client and/or the project to comply with the applicable legal requirements; and
- In instances where an environmental or social risk has been identified, the ongoing evaluation of compliance with conditions imposed on the facility.

Considering the factors above and depending on the nature of the transaction, the ESRA review may involve requesting the following types of documentation from the client to ensure compliance and mitigation. These include, but are not limited to:

- Environmental authorizations/ certificate / record of decision issued by the relevant department;
- Environmental Impact Assessments/ project briefs undertaken for specific projects/activities;
- Environmental management plans;
- Legal permits / authorizations;
- Occupational Health and Safety documentation;
- Other relevant internal environmental and social related policies / procedures
- Property valuations reports for indications of contamination or environmentally hazardous substances;
- Waste management plans;
- Labour related information i.e. employment/ human resources related documents;
- Community engagement procedures and record of community participation;
- Review of other relevant documentation such as reports from environmental authorities, or independent audit reports, or international and local certification bodies.

7.4 Transaction type vs the level of screening required

7.4.1 Equator Principles

If the transaction meets the thresholds and stipulations of the Equator Principles (EP), the pdf document will reflect that the transaction is an Equator Principles related transaction and also provide a categorization of the transaction. For Category A and B Equator Principle transactions, an Equator Principles Compliance Report compiled by an independent and competent environmental consultant, should be requested from the client. This review would be for the client's cost. It is the responsibility of the client to implement all material recommendations made in this Compliance Report within timelines prescribed by the consultant. An Equator Principles monitoring report on the project by the same or a similar

competent consultant is required on an annual basis post financial close. This is not only to ensure that recommendations and resulting actions as per the initial Equator Principles review are carried out appropriacy, but also to ensure that any new gaps in compliance to the Equator Principles or breaches in legal compliance are identified and closed out appropriately.

Transactions that meet the above criteria are required to be screened against the Performance Standards principle 1 to 8 to ensure that all related environmental and social risks are managed accordingly.

Transactions that would be classified as an EP transaction include:

Criteria	Level of screening required
Project finance activities which have capital costs amounting to or exceeding USD 10 million	Screening required against the IFC performance standards principle 1 to 8 by independent consultant
Project related corporate loans where the total facility amounts to or exceeds USD 50 million	Screening required against the IFC performance standards principle 1 to 8 by independent consultant

7.4.2 Corporate Loans

In line with commitments made under DFI funding agreements and as part of the ESRA review process, corporate loan transactions that meet the following criteria are required to be screened as follows:

Criteria	Level of screening required
Corporate loans with tenor of not less than 36 months and funding-defined assets as part of a project amounting to at least $10 million of total capital costs	Screening required against the IFC performance standards principle 1 to 8 (internal review)
Corporate loans provided to a single client exceeding $5 million, on an aggregated basis over a period of 36 months	Screening required against the IFC performance standards principle 1 to 2 (internal review)

7.4.3 All other ESRA applicable transactions

If the transaction does not fall into the equator principles or corporate loan threshold, then the normal ESRA process screening would apply:

Criteria	Level of screening required
All other ESRA applicable transactions	Standard ESRA review applicable taking into account clients, legal compliance (local and international laws), environmental & social factors attached to the activity, excluded & sensitive industries and activities etc.

7.5 Referral to Credit / Credit Committee for approval

Once the ESRA specialist/team is comfortable that all risks are suitably controlled, managed or mitigated, or in the process of being mitigated, the specialist may provide ESRA approval on the transaction. Where there are concerns of

environmental and social non-compliance, this will be highlighted in the ESRA specialist/ team ESRA review for credit consideration.

The ESRA review process should form an integral part of the credit approval process following the evaluation and documentation of environmental and social risk by the ESRA specialist/team, credit managers/credit committees will be in a position to reject a transaction on environmental and social grounds, or accept the environmental and social risks, subject to measures being taken by the client to control the risks. A transaction has an acceptable level of environmental and social risk where environmental liabilities do not present a significant threat to company viability, ability to repay loans or the value of security, or where FNB Mozambique would not be unduly exposed to risk arising from direct liability, credit risk or reputational damage.

NB: Credit/ credit committees have the discretion to request that an ESRA review be performed on any transaction including Category C where the assessment indicates that there may be an environmental or social risk attached to the lending.

When an exception or a dispute is raised with regard to a lending transaction, client activity or where there is doubt regarding legal compliance, where there are ethical and moral concerns, or non-compliance with the excluded and sensitive industries and activities matrix, the process of escalation must be followed. (see 7.8 below)

7.6 ESRA Covenants in Loan Documentation

An important strength of an effective Environmental and Social Risk Assessment process is the incorporation of covenants linked to compliance. Having assessed and documented any environmental and social risks or opportunities associated with a particular transaction, the ESRA specialist/team should then consider whether the bank should attach any specific environmental or social conditions to the transaction and financing agreements to reduce or mitigate the risk.

Based on the recommendations of the ESRA specialist/team, the legal department, credit fulfilment department and the transactor/ relationship manager will ensure that the condition is embedded within the loan agreement.

Examples of conditions are as follows:

- To comply with all relevant country environmental and social laws, regulations and permits in all material aspects.
- Any covenants, warranties or related conditions that may mitigate any specific environmental or social risks identified during the ESRA review phase.
- Where environmental issues are of concern, the facility agreement must stipulate that the client is obliged to inform the bank of non-compliance with environmental legal requirements or any of the conditions of the facility. Furthermore, the client must also be required to notify the bank of any claims against it or the operation arising out of non-compliance with environmental laws. Provision should also be made in the facility agreement for

termination of the agreement, at the discretion of the bank, if no adequate steps are taken to comply with environmental legal obligations or environmental conditions of the facility agreement, i.e. by way of a material adverse change clause.

Where the client is not in compliance with its environmental and social covenants, the bank will work with the client on remedial actions to bring the client back into compliance to the extent feasible. If the client fails to establish compliance within an agreed grace period, the bank reserves the right to exercise remedies as considered appropriate.

7.7 ESRA Transaction Monitoring

Monitoring is conducted on the transaction post disbursement to ensure that all the appropriate environmental and social risk management covenants, warranties or conditions included in the loan documentation have been fulfilled. These conditions, warranties and covenants will vary per transaction, and will be monitored in accordance with the credit monitoring processes on facilities. Continual monitoring of covenants, or warranties as decided, should be conducted over life of loan where appropriate to mitigating the risk.

In the event that a client is non-compliant with monitoring conditions, the escalation process detailed in section 7.8 below must be followed.

7.8 Escalation Process

When an exception or a dispute is raised regarding a lending transaction, then the process of escalation must be followed. This would include instances:

- where there is doubt regarding legal compliance,
- where there are ethical and moral concerns,
- where a client has not fulfilled an environmental and social related condition imposed by the bank, or
- if the client's activities fall within the excluded and sensitive industries and activities matrix where concerns have been noted by the ESRA team, credit area or any other stakeholder involved.

If the ESRA Specialist raises concerns regarding the environmental and social performance of the client in general or in specific relation to the transaction, the transactor/relationship manager, the Chief Risk Officer and the Head of Credit (or his/her alternative) should be informed. The final decision on the action to be taken per lending transaction will be taken by the above-mentioned stakeholders.

A disputed transaction will be reported to the banks Ethics & Market Conduct Committee and Persons of Interest Forum (POI forum) for noting and discussion purposes.

8 MONITORING OF THE ESRA PROCESS FOR EFFECTIVENESS AND COMPLIANCE

8.1 Internal reporting on the ESRA process

The ESRA process is a standard agenda item at the Ethics & Market Conduct Committee. All aspects of the ESRA process are reported to the committee on a quarterly basis in terms of changes, efficiency and compliance of the process. Qualitative information associated with breakdowns in the ESRA process, deals of a sensitive nature, etc. will be tabled at the Ethics & Market Conduct Committee for review and discussion.

8.2 Internal Audit

The reporting data related to ESRA and Equator Principles is subject to internal verification by the group Internal Audit area. This audit is essential to ensure the completeness, accuracy and reasonability of the data, as well as the on-going effectiveness of ESRA processes within the bank. This is an independent internal process and all documentation in relation to the Internal Audit review is maintained by the group Internal Audit department.
The FirstRand Environmental and Social Risk team together with the ESRA specialist provide technical input into the internal audit planning processes and audit plans.

9 ESRA PERFORMANCE REPORTING

The group produces various public annual environmental reports which set out how environmental and social issues are being addressed in its business and operations. Reports that relate particularly to ESRA and the Equator Principles are:

- The integrated FirstRand annual report
- FirstRand Divisional Reports to Society
- Environmental and Social Risk Monitoring Reports to International Development Funding Banks

All data reporting related to ESRA and the Equator Principles is governed by the FirstRand Environmental Data Reporting Guideline. Performance reporting will be managed by the FirstRand Rest of Africa Environmental and Social Specialist / Team together with key stakeholders within the bank.

10 TRAINING OF STAFF ON ESRA

10.1 Affected Staff Members

The online training is available on Oracle for all FNB Mozambique staff and can be accessed by individual staff members logging into the Oracle Learner Management Module and searching for the ESRA training available. Line Managers will need to ensure that all new employees affected by the ESRA process, complete the online training upon their employment.

10.2 ESRA Specialists

Training of the ESRA Specialists will be conducted on an ad-hoc basis by the FirstRand Rest of Africa Environmental and Social Risk Team. ESRA Specialists are encouraged to attend external update courses such as environmental legal courses, or ESRA related courses. This will be managed through the divisional learning and development programs.

11 RESPONSIBILITIES OF KEY STAKHOLDERS IN THE ESRA PROCESS

Stakeholder	Responsibility
Transactors/ Relationship Managers	○ Completing the ESRA tool for categorization and submission for ESRA review purposes. ○ Obtaining relevant documents from the client related to the ESRA review and sending them to the ESRA specialist/team reviewing the transaction; ○ Reporting to the relevant Credit/Investment Committee on the ESRA categorisation on a transaction and any potential credit/reputational, collateral, regulatory or legal liability risks related to the transaction identified during the ESRA review by the ESRA specialist/team. ○ Where relevant ESRA related monitoring conditions have been imposed in loan agreements, following up on conditions and completion of any outstanding actions expected from the client.
ESRA specialists/ ESRA team	○ Assessing the categorisation of the transaction by the online tool for appropriateness of categorisation. ○ Assessing transactions against position papers where applicable (i.e. sensitive industry matrix) ○ Assessing whether documentation received from the client (i.e. EIA reports, property valuations, legal compliance audit reports, etc.) is relevant in order to conduct a review of the risks concerned and requesting additional documentation if necessary. ○ Analysis and review of documentation received from transactor on behalf of the client to mitigate environmental and social risks ○ Imposing conditions in loan agreements to mitigate risks related to the transaction. ○ Review of environmental and social documents requested as part of the monitoring on transactions ○ Reporting of transactions wherein ESRA approval or concern is raised to the Chief Risk Officer and Head of Credit for decision making on the transaction. ○ Reporting on the ESRA process performance to the Conduct and Ethics committee.
Credit/ credit committees and Investment Committees	○ Decision making on the appropriateness of the transaction based on the ESRA related risk identified during the ESRA review, and the impact that these risks will have on the lending relationship between the client and the bank. ○ Credit managers/ Credit committee has the discretion to request that an ESRA review be performed on any transaction (irrespective of the transaction type) including category C where the assessment of the client's activity or the property valuation (collateral) indicates that there may be an environmental or social risk attached to the lending. ○ Credit managers are further responsible to ensure that the categorisation and activity selection as per the ESRA questionnaire results is accurately selected in relation to the client's activities and funding requests. This is an important check for credit managers to undertake especially for category C transactions where ESRA reviews are not required. ○ Credit managers/ credit committee must ensure that all transactions which fall within the excluded and sensitive industry matrix are referred for an ESRA review to ensure that facilities are provided in line with the position statements where applicable. This is an important responsibility for credit managers /credit committee for transactions that are exempted from the ESRA process. ○ Review that standard and additional ESRA related covenants are included into facility condition where recommended by the ESRA specialist/team and approve conditions identified by ESRA specialist before payout

Internal Audit	○ Conduct independent reviews and evaluations of the effectiveness and adequacy of internal controls; and ○ Ensure that the respective area timeously addresses any unsatisfactory audit findings.

12 EXTERNAL COMMUNICATION AND ENGAGEMENT

The bank has developed an external communications and grievance procedure which aims to manage, investigate and address environmental and social related queries and grievances received from external stakeholders resulting from the banks financing activities, particularly those relating to project finance. Through the implementation of this procedure the following objectives will be met:

- creating a formal channel for bringing external grievances to the immediate attention of the bank;
- increase transparency in our lending and investment processes;
- ensure consistency in the equitable handling and resolving of grievances;
- encourage the prompt and effective management of issues raised; and
- compliance with relevant DFI contractual agreements and international best practice standards.

To meet accessibility requirements the grievance mechanism is available on the bank's website and grievances can be channeled by using the email address provided on the website as follows: environment@FirstRand.co.za. A process guide setting out turnaround times and engagement with all relevant stakeholders on addressing these queries can be located on the ESRA tool. All external responses via this channel will be approved through FirstRand Investor Relations prior to being sent out.

13 ANNEXURE 1 – REFERENCES

- The Equator Principles, version 4, http://www.equator-principles.com
- Environmental Law of Mozambique
- Environmental Impact Assessment Regulation of Mozambique
- IFC Performance Standards: http://www.ifc.org

REGULATORY AND CONDUCT RISK MANAGEMENT
MONITORING OPERATING PROCEDURES

Document control

Document Details	Responsibility
Document owner	<table><tr><td>Policy</td><td>Regulatory and Conduct Risk Management Monitoring Monitoring Standards</td></tr><tr><td>Origin:</td><td>Regulatory and Conduct Risk Management (RCRM)</td></tr><tr><td>Signature</td><td></td></tr></table> <table><tr><td>Name:</td><td>Yolanda Braga</td></tr><tr><td>Position:</td><td>Chief Compliance Officer</td></tr><tr><td>Contact:</td><td>(+258) 21356917</td></tr><tr><td>Email:</td><td>yolanda.braga@fnb.co.mz</td></tr></table>
Approval	<table><tr><td>Committee</td><td>Approval date</td></tr><tr><td>Executive Committee (EXCO)</td><td>_____August 2020</td></tr></table>
Date of Last approval	New document
Effective date	
Date of next approval	September, 2021
Signature	_____ Peter Blenkinsop (Chairman)
Group version	1.0
Version	1.0
Number of pages	52
Implementation date:	The directives and minimum requirements set out in this policy should continue to be implemented across FNB Moçambique by November 2020

GLOSSARY

Abbreviation	Description
BU	Business Unit
BUCO	Business Unit Compliance Officer
CO	Compliance Officer
CoE	Centre of Excellence
CRP	Compliance Risk Profiles
HOM	Heads of Monitoring
KCI	Key Compliance Indicator
KRI	Key Risk Indicator
LOD	Line of Defence
MCOE	Monitoring Centre of Excellence
PRCI&A	Process Risk Control Identification & Assessment
PI	Personal Information
RMP	Risk Management Plan
SDI	Self-Disclosed Issues
SME	Subject Matter Expert
SPI	Special Personal Information
WPs	Working Papers
QA	Quality Assurance

Table of Contents

1. BACKGROUND

Regulatory and Conduct Risk Monitoring is a process used to assess the adequacy and/or effectiveness of controls implemented within business to mitigate the risk of non-compliance to legislation, regulation and supervisory requirements. It is an assessment of business activities to assist management and the board of directors to understand whether business is conducted in compliance with relevant regulatory and ethical requirements. Regulatory and Conduct Risk monitoring is a requirement of Regulation 49 of the Banks Act, amongst others, which requires continuous compliance-related monitoring to be performed.

Regulation 49 (4) of the Banks Act 94 of 1990 states that:

As a minimum, the compliance manager of a bank shall –

f) be responsible for establishing a compliance culture in the bank that contributes to the overall objective of prudent risk management by the bank;

g) establish a line of communication to line management, in order to monitor continuously compliance with laws and regulations or supervisory requirements by the bank;

h) require line management to monitor compliance with laws and regulations or supervisory requirements as part of their normal operational duties;

i) require regulatory requirements to be incorporated into operational procedure manuals when appropriate; and

j) make recommendations whenever necessary in order to ensure that there is compliance with laws and regulations or supervisory requirements;

In order to execute on the requirements of Regulation 49(4)(i) of the Banks Act, these monitoring standards seek to provide a consistent approach to risk-based monitoring.

In line with Notice nº04/GBM/2013 - Risk guidelines, the Bank must risk management function and conduct independent review (section 1.5.8.)

2. OBJECTIVE and PURPOSE

The objectives of monitoring are to:

- Identify and recommend improvement for areas of compliance weakness;
- Ensure that controls designed to protect FNBM, against non-compliance are being properly implemented and that they are effective; and
- Review the integrity of the compliance system.

Once control measures have been developed, implemented, and embedded to ensure compliance with the regulatory requirements, these measures must be monitored to determine, firstly, whether they are adequate and secondly, whether they are effective.

The purpose of these operating procedures to:

- operate in line with the set minimum standards and operating procedures to support the Regulatory and Conduct Risk Monitoring Standard;
- contribute to mitigating the risk of FNBM exposure to reputational damage, potential fines, penalties, regulatory censure and/or punitive action, financial impact due to non-compliance with applicable regulatory and/or supervisory requirements;
- ensure that appropriate risk-based monitoring procedures are consistently applied/implemented, understood and adhered to across FNBM, including its local and foreign subsidiaries.

3. SCOPE

The monitoring standards and operational procedures are applicable to the FNBM, it's as they establish the minimum standards and implement the operating standards to which a monitoring function must adhere.

If a home jurisdiction has regulations which make it prohibitive for an operation to apply any of the requirements contained in the host FNBM Monitoring Standards, an application for a waiver must be submitted in accordance with the Monitoring Standards and be submitted to the Leadership and Management Team (LMT) Sub Committee for approval at the Compliance and Conduct Risk Committee (CCRC).

These operating procedures are developed in support of the FNBM Monitoring Standards as approved in line with the RCRM Manual. Should additional procedures or a deviation from the monitoring standards and/or operating procedures be required, this must be tabled at the Monitoring Centre of Excellence (MCOE) Work Group.

FNBM Monitoring Standards and Operating Procedures recommendations are discussed, agreed and approved by the Monitoring Centre of Excellence (MCOE) Work Group. The LMT Sub Committee are informed for ratification. The standards will be updated accordingly in line with the annual revision of the CCRC Frameworks Committee.

Where it is established, that the deviation is only applicable for a single instance, such a deviation must be approved by the (MCOE) Work Group, the standards will not be amended, and no referral will be done to LMT Sub Committee.

4. OWNERSHIP OF STANDARDS AND OPERATING PROCEDURES

The monitoring standard and operation procedures is owned by FNBM Assessment & Monitoring, who will facilitate and co-ordinate the implementation of these requirements. The Chief Compliance Officer (CCO) are responsible for the implementation of the minimum standards and operating procedures as set by these standards.

5. GOVERNANCE AND APPROVAL BODIES

The standard must be approved by Exco and the operating procedures would be updated on an annual basis as a minimum and/or on an *ad hoc* basis.

6. RELATED POLICIES

The operating procedures forms part of the FirstRand Monitoring Standards and must specifically be read in conjunction with the RCRM Manual and FNBM Monitoring Standards.

In order to execute the required controls, the RCRM teams can leverage tools and/or existing controls measures already developed in the Group, either by the RCRM function, for other risk types:

- ERM: BCBS 239 Standard as per the roles and responsibilities defined for RCRM in-country;
- POPIA / Confidential Information Guidance for Group Internal Audit.

7. PUBLICATION

The latest versions of the FNBM Monitoring Standards and Monitoring Operating Procedures must be published on the FNBM intranet. It is the responsibility of RCRM team to ensure that this operating procedure is distributed to all employees whose roles are impacted by it.

8. ADOPTION and SUPPORTING OPERATING PROCEDURES

FNBM must adopt the operating procedures in as far as this is required to give effect to the requirements contained in this FNBM Monitoring Standard and these Operating Procedures, which must be approved by its applicable governance forums.

9. MINIMIMUM OPERATING PROCEDURES FOR MONITORING

9.1 Archer Profile – Creation and Approval

Once the Compliance Risk Profile and the Monitoring Plan has been reviewed, discussed and approved by the relevant governance committees it must be loaded onto Archer. This includes confirmation of the process followed to achieve the risk profile and the creation of the engagements on Archer. This will be facilitated by the Program Team and will include:

- Loading the commentary on the creation of the profile;
- Updating the Compliance Risk Profile sections with all applicable authoritative sources;
- Rating of applicable authoritative sources'; and
- Loading of engagements per the Monitoring/Coverage Plan. This includes specifying the Engagement Name, potentially Monitoring/Review Manager and the dates for completion of the engagement. It should be noted that once the team are ready to begin their coverage plan, they will simply locate the specific engagement and complete the additional information as the base information has been updated to create the engagement. There is no reason to load another engagement. All Compliance Officers must first check the profile under monitoring engagements prior to loading their own engagement.

Once all information has been loaded onto Archer, the minutes confirming the approval of the governance committee must be obtained which specify that the Coverage Plan was submitted and discussed and noted as approved.

In terms of the FNBM RCRM Manual, the annual coverage/monitoring plan must at least ensure that low, medium, very high- and high-risk legislation has been addressed in the coverage plan. This will be monitored by the dedicated monitoring teams. The medium and low risk legislation may be included in coverage on a three (3) -year rolling plan. However, it is agreed that business unit compliance teams, to alleviate the pressure on the dedicated teams, will facilitate monitoring of medium and low risk legislation impacting their specific business units.

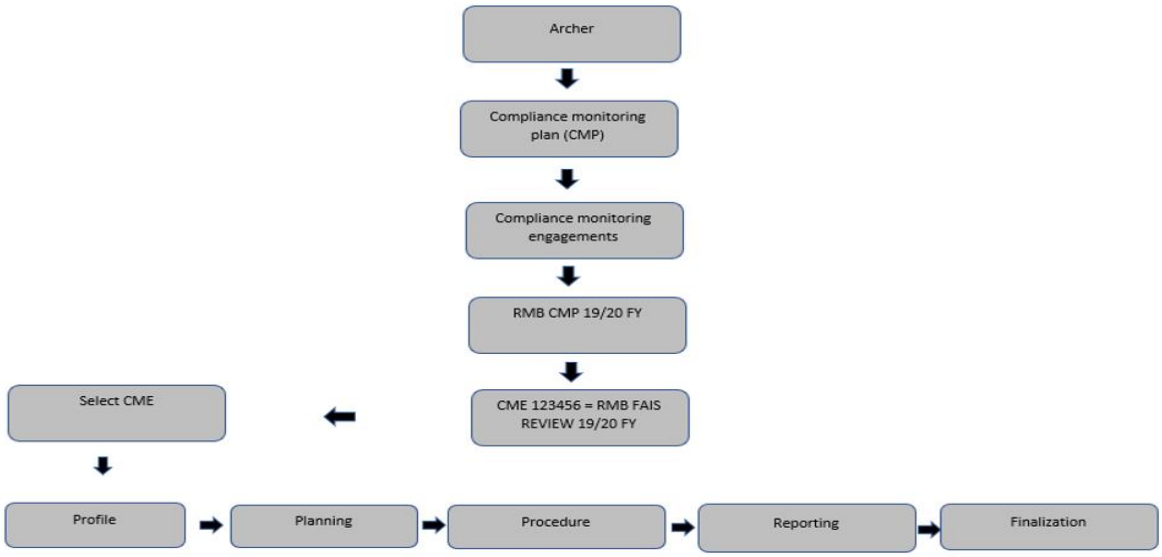
The functionality to create a regulatory universe versus a coverage plan has been segregated. While the use of the Compliance Monitoring Plan module on Archer still applies, you will now be required to select whether you are loading a regulatory universe or a coverage/monitoring plan with linked engagements. Only specific functionaries will have permissions to load the coverage plan with linked engagements. This permission is limited, and should you require such permissions, approval must be obtained from MCOE.

Number of Coverage Plans applicable:

- FNBM BU´s

9.2 Business Operations

Many laws, regulations, rules, standards and codes of conduct may impact a single business operation. Business processes are established to ensure all material regulatory risks and associated risk concentrations are identified, measured, prevented/limited, controlled, mitigated and reported as stipulated in the RCRM Manual. Regulatory Risks arise because of shortcomings or errors in the design, implementation or effectiveness of controls within the relevant business operations. The diagram below illustrates the monitoring workflow and expected outcomes:



Monitoring Phases	High Level Activities for engagement and Archer activities
Profile	Review and assess the information gathered (RMP/PRCI&A/RCRM, EA, BM, IA, and GIA Findings/SDI's), to establish key risks for the engagement
Planning	The engagement letter is drafted, discussed in the stakeholder meeting with BU management team. The engagement letter is updated and distributed for comments, finalised and signed with stakeholder and uploaded
Procedures (Fieldwork)	Select the related the RMP, load in line with the programme library, determine the test procedures and execute in line with Standards and Operating Procedures. Discuss findings with BU, send a list of findings to BU. Once accepted load onto Archer and mark as prepared on system, to the selected 'Engagement Reviewer' to send to the client.
Reporting	The selected 'Engagement Reviewer' will assess the application of procedures of the overall engagement and review the findings loaded by the Monitoring Manager based on the QA activities. The draft report is distributed to stakeholders, updated and finalised by the Preparer. Once signed by all parties it is uploaded to the system.

Finalisation	The overall management comments are added on to the system and sent via system notification to the client. The engagement is concluded when the Engagement Manager clicks on the signoff in Archer.

To comply with BCBS 239 Standards, the RCRM community must apply the second level of the Regulatory Risk Taxonomy which provides a link from the identified risks to which laws, regulations, rules, standards and codes of conduct that have given rise to them. The laws, regulations, rules, standards and codes of conduct are presented at three levels of granularity. Act Grouping and RCRM Pillars are important dimensions across which Regulatory Risk exposure is reported in the in-scope reports.

The elements on Archer that need to be applied to support the data controls that MCOE directly contribute to are listed in the table:

Element on Archer	Definition	Purpose
Authoritative Source	Named laws, regulations, rules, standards and codes of conduct which impose requirements on the regulated entity that must be complied with in order to avoid *the risk of legal or regulatory sanctions, material financial loss, or loss to reputation*.	The Authoritative Source drives the identification of the Compliance Risk Profiles (CRP) which, in turn, drive formal and informal compliance monitoring procedures from which Regulatory Risk issues may be identified. Each Regulatory Risk issue must be linked to the Authoritative Source.
Act Grouping	Applicable Legislation/Regulation is aggregated into Act Groupings. Act Groupings represent groups of laws, regulations, rules, standards and codes of conduct which address similar types of regulated activity or similar regulatory requirements.	Issues are aggregated into Act Groupings to understand the nature of the reporting entity's exposure to Regulatory Risk, and trends over time. Every Applicable Legislation /Regulation must be mapped to an Act Grouping.
Entity	Information relating to organisational entity recorded on ARCHER, reflecting Business Unit, Segment and Franchise. For example, if monitoring is being done by R&C Division as part of CoE coverage, within the Premium Segment specifically for the PCB business unit, then the entity specified **must** be FNB-Premium-PCB. Where monitoring is facilitated by the business unit compliance team, then on entity structure they **must**	Entity must be correctly applied. The applicable entity being reviewed is accurately reflected so irrespective of where monitoring takes place, the entity must reflect exactly where the engagement will occur. Ensure that there is full awareness of all engagements being facilitated across a BU regardless of who is facilitating the review/monitoring. All engagements must be linked to a Monitoring Plan, even ad hoc. This may be completed by the

Element on Archer	Definition	Purpose
	select the relevant Business Unit Entity, FNB-Premium-PCB.	creation of Divisional plans as well as Segment Plans. Where BU's within a segment are to facilitate monitoring, it must be incorporated into the segment plan for effective management of coverage and reporting.
Regulatory Risk Themes	Regulatory Risk Themes represent groupings of operational/business processes that are affected by distinct regulatory requirements defined in one or more laws, regulations, rules, standards or codes of conduct. The Regulatory Risk Themes are listed in the RCRM Manual. Regulatory Risk themes are an important dimension for aggregating information about Regulatory Risk exposure in the in-scope reports.	Regulatory Risk themes are used to organise regulatory risk monitoring activities. Regulatory Risk themes have been developed to alleviate the monitoring burden on compliance officers and eliminate duplication of control testing by both business and RCRM (first and second line) where regulatory compliance controls overlap with operational controls by catering for coverage of multiple pieces of legislation under thematic reviews

In addition, the Risk Monitoring responsibilities for MCOE and identified Subject Matter Experts (SME) are defined for the regulatory risk data aggregation capabilities. The focus of on controls and responsibilities are listed in the table below:

Risk Monitoring MCOE and SME Responsibilities as defined In BCBS 236 Standards

BCBS 239 principle	Paragraph	Requirement
Risk data aggregation capabilities – Timelines	Preamble	A bank should be able to generate aggregate and up-to-date risk data in a timely manner... The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank.

I. Risk identification → II. Risk assessment → III. Risk monitoring → IV. Risk reporting

Control	Source	Responsible	Frequency
The formal monitoring programme should be supplemented by informal monitoring procedures where the residual risk is High or Very High to enable the identification of Regulatory Risk on a timelier basis than the normal formal monitoring cycle.	New	BU RCRM Manager Franchise RCRM Head	Annual

The SMEs should make recommendations on appropriate analytics, wherever possible, to apply per RCRM Pillar. These recommendations should be catalogued through the FirstRand Regulatory and Conduct Risk Management Compliance Analytics Framework.	New	SME	Annual
BU and Franchise RCRMs should specify the analytics required to monitor the risks identified in the RMP/PRCIA. Consideration should take into account the Residual Risk level in the BU/Franchise, the availability and frequency of other monitoring activities and the cost versus benefit of applying analytics	New	BU RCRM Manager Franchise RCRM Head	Annual
The SME should review the analytics coverage across the enterprise and challenge the Franchise RCRMs in those areas where informal monitoring coverage is low relative to others.	New	SME	Annual
Tolerance levels should be established for each KCI and KRI.	New	SME	Annual
Exception reports should be produced where tolerance levels are breached.	New	1st LOD senior management	Varies (daily, weekly, monthly
The nature of exceptions should be investigated and, where necessary, Regulatory Risk issues should be logged on ARCHER.	New	BU RCRM Manager	Varies (daily, weekly, monthly)
KCI and KRI results and exception reports should be retained as risk data, which is subject to the requirements of BCBS 239.	New	BU RCRM Manager	Varies (daily, weekly, monthly)

9.3 Capacity Planning

In order to achieve coverage across FNBM it is imperative that effective capacity planning is implemented. In terms of the Capacity Management Model the following is required by Compliance Officers who have been identified through the coverage plan process to facilitate monitoring:

- All leave must be completed timeously on Oracle. This relates to all leave types including Annual, Sick, Maternity, Special Long, Sabbatical, etc. This will ensure that planning takes cognizance of availability of resources at any point in time

- All Training must be booked through Learning and Development so that this is also reflected on the Oracle record and may be considered for planning. On the job training must also be considered and provided to ensure that the hours applicable are considered within the model.

- Attendance of relevant industry forum, internally information and CPD sessions, as well as any attendance of meetings other than required, must be considered within the model.

- All employees involved in monitoring must complete the "Staffing Tab" on each engagement with the relevant details of the review. Once a Compliance Monitoring Plan has been approved and loaded onto Archer, all engagements linked to that plan will be loaded by the relevant resource, ensuring that all resources allocated to facilitate these reviews are included in the engagement details loaded. Thereafter employees affected may access the engagement and include all relevant details within the staffing tab relevant to that engagement. This includes adding tasks relating to the various phases of the review, specifically those related to Profiling and stakeholder engagement. This information will provide valuable data which will assist in ensuring that the model effectively utilizing the limited resources available. The key milestones that must be tracked for internal reporting purposes are as follows:

    - Start of administration and planning;
    - Date of scope document issued;
    - Start of monitoring fieldwork;
    - End of monitoring fieldwork;
    - Draft report/Findings sheet issued;
    - Close-out/Clearance meeting;
    - Final report issued; and
    - Monitoring work papers finalized and non-compliant issues

- Reference the "Annexure – Staffing Module Archer Appointment" for the capturing requirements onto Archer

9.4 Quarterly Meetings Regarding Coverage

On a quarterly basis monitoring teams must meet with their deployed compliance team to discuss monitoring for the quarter. These sessions must at minimum include a segment head of compliance with senior compliance resources to ensure that robust discussions are maintained.

The purpose of the meeting to provide the compliance team with the coverage areas for their business unit for the quarter, together with a view of the minimum that would be required by the monitoring team in order to facilitate these reviews.

The meeting will also allow for review and potentially adjustment of the coverage areas based on the risks identified by the business unit compliance team, together with other strategic and operational challenges and opportunities which may arise. Where coverage as per the approved plan is not able to be executed on, the monitoring plan needs to be adjusted to accommodate these changes and must be sent back to governance for noting and approval. As the plans are not static, these meetings become imperative in ensuring that we are all working towards a common goal of ensuring comprehensive control risk assessments and identifying areas of key regulatory concern.

9.5 Slippage on Engagements (Reporting Template)

The reporting template below is completed and referred to the MCoE Working Group and presented to the LMT Committee for approval of any adjustments/changes against the approved annual plan as table at the RCRM Frameworks meeting for the FirstRand Financial Year Monitoring Coverage Plan

No.	Engagement name	Q due	New due date	Rationale	Approving Committee	Approved/ Rejected

Monitoring – Profile and Planning

9.6 Risk Management Plans (RMPs)

Through the quarterly engagements noted above, the monitoring team will be aware of the availability or otherwise of the RMP. Where the RMP is not available, discussions must be had in terms of the time needed to ensure that this is completed, as this does have an impact on the facilitation of the engagement.

RMP's at a minimum must have been completed by the Compliance team to include:

- Confirmation of very high- and high-risk provisions of the legislation
- Documented controls as discussed with business
- Confirmed tests for such controls

- An adequacy assessment of the control (i.e. that the control exists and mitigate the risk, as applied)

All documented RMP's must be signed off by business confirming that the controls documented are an accurate reflection of their current control environment. Where applicable, be signed off by the business unit SME or a senior compliance officer.

The monitoring team will then perform adequacy and effectiveness reviews in line with the coverage plan.

9.6.1 Process to complete a Risk Management Plan (New and Existing)

New RMP's

- A workshop must be set up with all impacted (or potentially impacted) business unit compliance officers. An impact assessment of the provision must be completed to form the Master RMP which details business unit applicability. Where a provision is not applicable a comment must be included stating the reason for exclusion of the provision. Thereafter each Business unit compliance officer will filter for their specific provisions and create a BU RMP.

- Once the BU RMP provisions and RMP have been created the Compliance Officer together with Business will assess inherent risk rating (i.e. consequences and likelihood of non-compliance in the absence of any dedicated management controls being in place) for those provisions.

- A workshop **must** be set up with business to Identify and document Controls for the applicable provisions identified. (Controls must be completed by and in conjunction with senior management within the business area as business is the **ultimate owner of the controls**). Compliance must not document controls on behalf of business.

- Once controls have been documented and prior to monitoring being facilitated management (LOD 1) must sign off that the controls documented are an accurate reflection of the controls currently in place.

- After monitoring has been facilitated the adequacy and effectiveness of the controls must be rated in line with the outcomes of monitoring.

  N.B Adequacy and effectiveness of controls cannot be rated until monitoring has been conducted. Where this is rated it must be noted that this is based on business self-assessment, which will still be reviewed independently by Regulatory Conduct Risk Management (RCRM).

- Once completed and signed off the RMP must be sent to Program Team for transposing onto **Archer** template.

- Upon confirmation from the Archer COE that the RMP has been loaded, the compliance officer must complete testing on Archer.

Existing RMP's

- Where an RMP already exists, the Compliance Officer must assess the legislation in its current format and assess whether any amendments have been made to the Act.

- It is important that original version and date of the RMP be noted and not removed; the date of update must be noted in the applicable space.

- NB: No changes/amendments may be made to the standard wording within the RMP or to the RMP template as this will impact the linkages to the auto-upload functionality.

- For any changes/amendments to legislation the same approach must be followed as for new RMP where this must be workshopped with all impacted areas for assessment.

- Once all changes have been made, business must Sign off the updated RMP and this can then be uploaded onto Archer.

9.6.2 SME Sign off inclusive of preparation steps

It is important that where a SME exists for a piece of legislation, that the SME is provided with the RMP prior to monitoring being facilitated. Please note that the SME will not assess based on completeness and adequacy or effectiveness of the controls documented. The role of the SME is to assess risk mitigation in line with key risks identified across the Group/Segment and provide input in this regard.

A Group and/or a Deployed SME are required to follow the following procedural steps:

1. Update and review assigned RMP's during Q1 of each calendar year.
2. The Group generated RMP's will be considered "master" RMP's:
    a. These "master" RMP's will contain minimum suggested controls;
    b. The "master" RMP's will also contain suggested control testing and monitoring procedures as guidance to compliance officers across the group;
3. Any changes to RMP's due to significant changes to legislation ("trigger events") must be implemented timeously, with consultation with divisional Programme Heads and Divisional SME's;
4. Engagement with divisions should be strictly managed via the respective Segment Heads of Compliance, Head of Segment Programme Management, and the Divisional SME;

The list of Group and Deployed SMEs' is maintained by the RCRM Program Support and Enablement.

It is the responsibility of the BU Compliance Officer to ensure that RMP's are updated regularly and available for monitoring. The BU compliance officers must ensure that correct version of the RMP is used and this must be sent to the Archer COE for uploading to Archer. All Compliance Officers are required to conduct an annual review of RMP's to assess and confirm accuracy of the RMP. All RMP's must be reviewed annually, as a minimum to ensure that all applicable sections have been included, to confirm any legislative changes, to ensure that changes to business product, processes and structures have been taken in account.

9.7 Process Risk Control Identification and Assessment (PRCI&A)

The monitoring team must confirm whether a PRCI&A exists for the business unit being reviewed. Where applicable this may be used to confirm controls documented and approved by business and for any additional information, not available in the RMP.

The monitoring team is in no way responsible for the update and maintenance of the PRCI&A but where it is established that no document exists or the document applicable is outdated, the monitoring team may provide such information to the relevant Operational Risk resource. An email to confirm this will suffice.

9.8 RCRM and/or Internal Audit Findings

Before any engagement is scoped, it is imperative that the monitoring team review existing RCRM and Internal Audit findings. These may then be included (RCRM findings) as part of the scope to assess remediation action, i.e. findings assurance/validation (only where the estimated remediation date has passed). Where the estimated implementation date is still to be reached, this should be noted in the scope as an exclusion, to be reviewed once implemented through the finding's assurance/validation procedures.

For internal audit findings, these will be assessed in terms of scope exclusion and where applicable noted to business. Where a finding exists and has been effectively remediated this must be included in the scope for testing.

9.9 RCRM Self-Disclosed Issues (SDI)

RCRM self-disclosed issues are issues raised by Business Units on Archer immediately upon identification of actual non-compliance to a piece of regulation/legislation.

During the information gathering/profile stage, all SDI's on Archer should be assessed across all risk disciplines. These will be identified and included in the Engagement letter.

During stakeholder engagement these must be discussed and potentially this will illicit additional concern and emerging risks.

Formal SDI's will be established in the profiling stage and the emerging risks, "what's keeping you awake" conversation will take place during stakeholder engagement. This may encourage business to disclose any additional key risks for the team to include in review. These will then be noted in the engagement letter as areas of concern raised by business which becomes part of the scope of review. This is done during the "planning phase" at the engagement meeting or any other formal planning meeting.

Formal SDI's will follow a similar process to those obtained by Group Internal Audit and to qualify as an SDI it must have been raised at a governance committee, must have a remediation plan/action as well as implementation date and owner. The SDI must be documented during the "planning phase" and be confirmed by stakeholder and stated in the engagement letter based on the SDI, the impact and action plans in place to address this (i.e. confirm incident numbers on OpenPages, GIA findings, RRM issues and project or programmes underway).

The procedures to verify the adequacy and effectiveness of the compensating controls management have implemented to address the SDI in the interim should be established. Then the reviewer should consider extended testing if required in the "planning phase".

Once "Fieldwork" has been started, no further SDI's will be permitted. The individual performing the engagement will confirm with the stakeholder that Planning is now concluded, and no further SDI's may be submitted.

- Reference the “Annexure – Self-Disclosed Issues (SDI) template”

9.10 Risk Assessment and Scope determination

For all legislation forming part of the approved coverage plan, a further impact in terms of the risk-based approach may be followed. This takes the form of ensuring that the RMP formulated in terms of the legislation also follows a risk-based approach. This means, that the RMP should take cognizance of the very high- and high-risk provisions/sections impacting the business for prioritization and monitoring.

Further, where a Very High (VH)/High (H) risk provision has been reviewed over an extended period and has been noted as high assurance and there has been no change in business process, system, people or control environment, these may be excluded from the scope of the review on the basis that the control environment is effective. Additional risks may then be scoped in which ordinarily would have been excluded. These may be of a medium or low risk rating but may be included to ensure that a comprehensive assessment of the control environment is facilitated.

At this point, the individual performing the engagement has all the relevant information available to draft the engagement letter. The profile tab may then be populated prior to discussion with the impacted business unit.

9.11 Meetings with Key Stakeholders

Once the scope of the engagement has been confirmed (based on the information obtained/gathered) the monitoring team should meet with the relevant business unit management, risk officers, and compliance officers to obtain key risks identified by the dedicated business and risk teams for inclusion in the scope of the engagement. Minutes of these meetings may be compiled and provided to business as part of the engagement. Alternatively, the draft engagement letter may be used as the guide to confirm the discussion.

Monitoring – Procedures (Fieldwork)

9.12 Engagement Letter Review and Distribution

Upon completion of profiling and information gathering as well as stakeholder engagement, the scope inclusions and exclusions may be agreed. These should be updated on Archer and a draft engagement letter distributed to the Business Contacts for Action to review and sign off. The engagement letter may go through amendments and all these amended versions must be maintained on Archer together with all evidence to confirm interaction with stakeholders.

The letter must as a minimum include the sections of the Act to be reviewed, the themes linked to those and any other information deemed relevant for the performance of the engagement.

Once all stakeholders agree, the final engagement letter must state the period which is under review and be signed by the head of the applicable business unit. The final signed engagement letter must be maintained on Archer. This will move the engagement status from Planning to Fieldwork.

9.13 Monitoring Techniques

Type	Description
Interviews or enquiry	Interviews are conversations, usually face to face, where questions and answers are exchanged related to a specific topic. Interviews allow for the monitoring specialist to obtain the necessary information from the source to facilitate the review. Enquiry consists of questioning knowledgeable persons throughout the entity. The Monitoring team should perform procedures in addition to the use of enquiry to obtain appropriate monitoring evidence. Enquiry alone does not

Type	Description
	always provide sufficient monitoring evidence and is not sufficient to test the operating effectiveness of internal controls.
Observation	Observation consists of looking at a process or procedure being performed by others. Observation provides monitoring evidence about the performance of a process or procedure but is limited to the point in time at which the observation takes place and by the fact that the Act of being observed may affect how the process or procedure is performed.
Re-performance	Re-performance is the monitoring's independent execution of procedures or controls that were originally performed as part of the entity's internal control, either manually or through the use of CAAT's.
Vouching	**Vouching does** not include valuation. **Vouching** is defined as the "verification of entries in the books of account by examination of documentary evidence or vouchers, such as invoices, debit and credit notes, statements, receipts, etc. To assert or confirm as a result of one's own experience that something is true or accurately so described.
Verification	Verification and validation are independent procedures that are used together for checking that a product, service, or system meets requirements and specifications and that it fulfils its intended purpose
Walkthroughs	Step-by-step test of all aspects of an environment, plan, or process to verify it is ready for its intended purpose. The objective is to obtain an understanding of the process; to identify high inherent risks; and key controls for those risks.
Mystery Shopping	Mystery shopping is a method used externally by market research companies or watchdog organizations, or internally by companies themselves, to measure quality of service, or compliance with regulation, or to gather specific information about products and services
Self-assessment/ attestations/ questionnaires	Confirmation of the existence of processes, based on individual/personal evaluation.

Type	Description
Inspection of records or documents	Inspection consists of examining records and documents, whether manual or in electronic form. Inspection of records and documents provides varying degrees of reliability, depending on the nature or source and the effectiveness of control over their production. Care should be taken as certain documentation may provide monitoring evidence with respect to existence, but not ownership.
Confirmation	Confirmation is the process of obtaining a representation of information or of an existing condition directly from a third party.
Recalculation	Recalculation consists of checking the mathematical accuracy of documents or records.
CAAT'S & Analytical procedures	Analytical procedures consist of evaluations of the reasonableness of relationships and trends that exists between financial and non-financial data.

These may be used depending on what is being tested/reviewed.

9.14 Monitoring Procedures Definitions

To reduce ambiguities and to adopt uniform meanings in monitoring procedures, the following definitions should be utilised:

Term	Definition
Analyse	To break into significant component parts and determine the nature of something.
Check	To compare or recalculate, as necessary, to establish accuracy or reasonableness.
Confirm	To prove to be true or accurate, usually by written enquiry or by inspection.
Evaluate	To reach a conclusion as to worth, effectiveness, or usefulness.

Term	Definition
Examine	To look at or into closely and carefully for the purpose of arriving at accurate, proper, and appropriate opinions.
Inspect	To examine physically.
Investigate	To ascertain facts about suspected or alleged conditions.
Review	To study critically.
Scan	To look over rapidly for the purpose of testing general conformity to pattern, noting apparent irregularities, unusual items, or other circumstances appearing to require further study.
Substantiate	To prove conclusively.
Test	To examine representative items or samples for the purpose of arriving at a conclusion regarding the population.
Verify	To establish accuracy.

9.15 Performing of Monitoring Procedures

The following procedures may be used to perform monitoring:

9.15.1 Walkthroughs

The objective is to obtain an understanding of the process; to identify high inherent risks; and key controls for those risks.

- A comprehensive walkthrough based on the process in question should be performed, whereby one transaction should be followed through the documented processes and systems if applicable (end-to-end). Screenshots/evidence of the process walkthrough must be obtained.
- An interview should be performed with the process owner and the process owner should sign off that the process (key controls) has been accurately documented.
- The walk-through should be documented. To assist in this process all monitoring specialist may utilize the step recorder functionality for evidence.
- Walkthroughs should be compared with RMP's (on Nimbus/excel) to identify gaps.
- The inserted template is a "sample testing sheet" for utilization during an engagement. The example of "sample test sheet" must be customized to the

engagement with the relevant procedures/tests conducted for each theme under review

- Reference the "Annexure – 2.3.2 Example Sample Testing Sheet"

9.15.2 Self-assessments/attestations/questionnaires

Self-assessments/attestations/questionnaires may be used in instances where a view of business is needed without an in-depth review being performed. This will allow for business to provide their assessment of the existing control environment. This will provide a view from business in terms of their rating of the control environment. This however needs to be confirmed through testing by the monitoring specialist to confirm the assessment provided by business is complete and accurate.

9.15.3 CAAT's and Analytics

Data analytics is a key strategic pillar to the RCRM Monitoring team in order to achieve its Monitoring Plan in an efficient and effective manner.

The following are benefits in using data analytics during an engagement:

- **Relevance:** Data analytics can help scope the engagement with focus on areas that require attention (risk-based)
- **Efficiency:** Fieldwork could be performed quicker via data analytics
- **Confidence:** Certain populations could be covered100%, thus eliminating sampling resulting in more accurate findings.
- **Business Independence:** Routine analytics can be passed to business, reducing the need for audit involvement (continuous monitoring)

The **biggest challenges** to incorporating data analytics into a monitoring process are:

- **Identifying relevant data:** What data exists, and where can it be found?
- **Articulating data needs:** Not understanding the data environment, and not asking clearly for what you want can make accessing the correct data more difficult than it needs to be.
- **Obtaining access to data:** Data analyst needs to understand and address the concerns of IT professionals regarding access to data.

- **Unclear data:** Data might not be easy to read (field titles and data structures unclear)
- **Inconsistent data:** Data might come from new and legacy systems, which means different data may be collected and recorded differently. Data may also be located in various, differently structured locations.

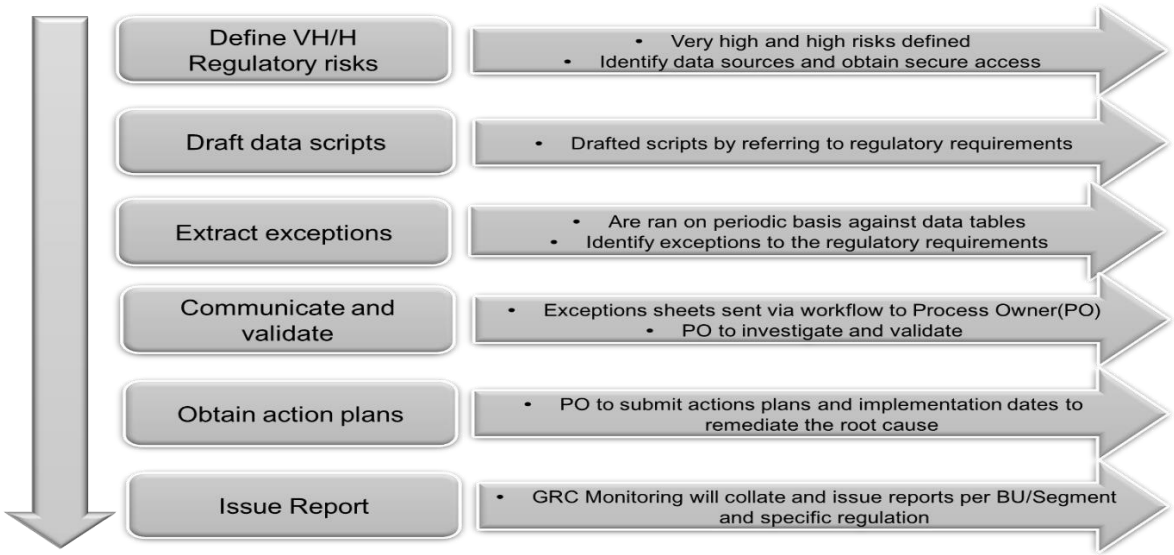
9.15.4 Ad hoc data analytics:

Where data analytics is required, the Monitoring Team will use the data request template/form to request for data extracts from the Data Analyst during each review.

The Monitoring specialist together with the Data analyst should build relationships with data owners and gain access to relevant data tables in the bank.

9.15.5 Real-time analytics:

"Real-time" monitoring is a strategic innovation that will be the differentiating factor between and other assurance providers, based on "real-time" identification, measurement and assessment of regulatory non-compliance.



9.15.6 Analytical Reviews

The ability to perform analytical review procedures will be dependent on the:

- Development of appropriate analytic objectives.
- Availability of appropriate data: What data the process captures? How is that data stored and for how long?

- Accessibility of data: Can we get access to the data and what protocols do we need to follow to obtain access?
- Integrity of data: The best analytical procedures are only as good as the quality of the data used.

The monitoring team should apply analytical procedures to assist in the following:

- In planning the nature, timing and extent of other monitoring procedures;
- Understanding the significant issues and risks;
- Understanding the business and its operations;
- As an overall review of financial information (if applicable).

Analytical procedures in the overall review of the internal monitoring

- Analytical procedures should be applied at or near the end of the monitoring when forming an overall conclusion to determine whether information is consistent with the monitoring's specialist overall knowledge of the business.

Extent of reliance on analytical procedures

The extent of reliance that the monitoring specialist places on the results of analytical procedures depends on the following:

- Significance of the items involved;
- Other monitoring procedures directed toward the same monitoring objective;
- Accuracy with which the expected results of analytical procedures can be predicted.

9.16 Management of Personal and Special Information

The Protection of Personal Information Act (POPIA) aims to protect an individual's right to privacy regarding their personal information which may have been collected by a third party during a normal commercial transaction or by their HR department prior to, or during, the course of their employment. It also seeks to bring South African law regarding ensuring and managing personal data in line with international data protection laws.

Note: In jurisdiction other than South Africa or with cross-border application, the procedures must be assessed against local laws and the procedures need to be shared with MCOE governance for approval.

Personal information (PI) refers to information relating to an identifiable, living natural person, and where applicable, an identifiable existing juristic person, and may include the following:

- Contact details: Email, telephone, address, etc.;
- Demographics: Age, sex, pregnancy, race, birth date, marital status, ethnicity, etc.;
- History: Employment, financial, educational, criminal, medical history, etc.;
- Opinions: Opinions of and about the person;
- Biometrics: Includes a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, and voice recognition, etc.; and
- Correspondence: Private correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.

Special Personal Information (SPI) is a higher degree of protection given to special personal information under POPIA given the highly sensitive nature of such information. Special personal information includes:

- Information concerning a child
- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political opinions
- Health (incl. physical or mental health, well-being, disability, etc)
- Sexual life
- Criminal behaviour

Note: It is not "personal information" if the information is already in the public domain or is not used, or intended to be used, in trade or commerce.

The purpose of POPIA is to regulate and formalise how companies collect, store, protect, access and distribute client information and to protect the ongoing integrity and sensitivity of that private information. The Act offers many safeguards regarding using an individuals' personal data, and primarily protects individuals from unsolicited emails and SMS's for services which they never applied for, as well as against any security

breaches that could result in identity theft, when personal information is stolen or offered too freely by a third party.

The Act regulates the manner in which personal information may be processed, by establishing conditions, in harmony with international standards that prescribe the minimum threshold requirements for the lawful processing of personal information.

9.16.1 Application and usage of information

MCOE as a second line of defence completes monitoring objectives to ensure compliance with the regulatory requirements, these measures must be monitored to determine, firstly, whether they are adequate and secondly, whether they are effective once business have developed, implemented, and embedded control measures. During a review MCOE mainly collects personal information as monitoring evidence in monitoring engagements (clients and bank employees) and key operational processes, e.g. Payroll data, AML transactions, etc. The information is stored on Archer, SharePoint, I Drive, Local Drives (i.e. Personal Drives), Paper Trail and emails. When personal information is shared in the "work papers" with business under review; the supporting documentation should be password protected and or anonymized Below are examples of PI collected during the monitoring process:

- Bank Customers – Personal information, banking transactions, activities, etc.
- LoD 1 and LoD 2 (Bank employees) – HR data, email addresses, employment, etc.
- Third Parties – Professional body membership information, employee ID numbers, etc.
- Employees (Bank employees) – Personal information, HR data including payroll records, CVs and performance reviews, etc. collected in HR-related engagements

Note. PI and SPI should not be retained in hard copy format during or after the monitoring engagement.

As monitoring officials we are mandated within an engagement to have unrestricted access and full authority to communicate with any staff member, examine any activity or entity of the Group, as well access to any records, files or data, including management information and minutes of all decision-making bodies, whenever relevant to the execution of its mandate. MCOE will respect the confidential nature of all information reviewed in the performance of its duties for Regulatory and Conduct Risk monitoring a requirement of Regulation 49 of the Banks Act and in line with FirstRand RCRM Framework and RCRM Manual is. The monitoring official will apply the care and skill expected of a reasonably prudent and competent monitor in handling Group information. In addition, the custody and retention of engagement records, regardless of the medium in which it is stored must be consistent with the Group's guidelines and any pertinent regulations.

Monitoring officials need to be fully aware of the data they are collecting, relevance to the engagement, and not collect/request data that is not necessary for the engagement, or data that could increase the risk of non-compliance to POPIA.

MCOE should follow the below steps during a monitoring engagement or operational activities to ensure adherence to POPIA execution before; during and/or at completion of the engagement:

Steps	Description
1.	MCOE's responsibility to protect PI and SPI obtained during an engagement should be reinforced in the engagement letter.
2.	Should any of the below information for MCOE employees be obtained, it must be securely stored on the systems (i.e. Archer, SharePoint, Paper Trail and I Drive): • Personal details, e.g. ID numbers • Training and certifications. • Continuing education requirements. • Qualifications. • Performance evaluations Incl. Personal Development Plans.
3.	PI and SPI gathered during an engagement either for information purposes or as engagement evidence must be stored on the systems (i.e. Archer engagement tool, SharePoint, Paper Trail I Drive, and Local Drive) which have restricted access. No PI and SPI must be kept in Hard Copy.
4.	PI and SPI can be recorded in work papers; however, no PI and SPI should be documented in engagement reports / finding sheets as part of engagement findings (details can be shared with management).
5.	Internal and External sharing of PI and SPI over emails must be password protected. The passwords must be shared separately and not within the same correspondence in which the data is sent. Data extracts (e.g. for CAATs) should only be transferred via secure channels.
6.	During monitoring finalization phase, all records pertaining to the monitoring engagement such as those stored on SharePoint, Paper Trail, I Drive, Local Drive, and emails must be transferred into the Archer engagement tool and other copies deleted.
7.	Complete Workpaper: Finalization overview procedure on the Archer file. Ensure that all monitoring evidence pertaining to the engagement such as those stored on SharePoint, Paper Trail, I Drive, Local Drive, and emails are fully migrated into the Archer monitoring tool.

Steps	Description
	The monitoring evidence must only be retained on Archer thus, the monitoring evidence will be retained in line with the records management requirements for RCRM.

10. ADEQUACY ASSESSMENT AND TESTING OF KEY CONTROLS

Based on the key controls identified and documented in the RMP together with management responses obtained through interviews and potentially walkthroughs, the monitoring team must identify the key controls to be tested. The monitoring team should understand both the manual and automated controls in place Monitoring must evaluate whether each key control identified is designed adequately to address and mitigate the relevant risk. Document the approach and evaluation criteria followed in reaching the adequacy assessment.

A walk-through should be performed (by interviewing the client and by observing) and one (1) transaction/sample should be selected where screen prints of each screen/control/step taken in the process should be obtained.

Document the attributes of the key controls and action plans, and assess the design adequacy of the control by considering the following:

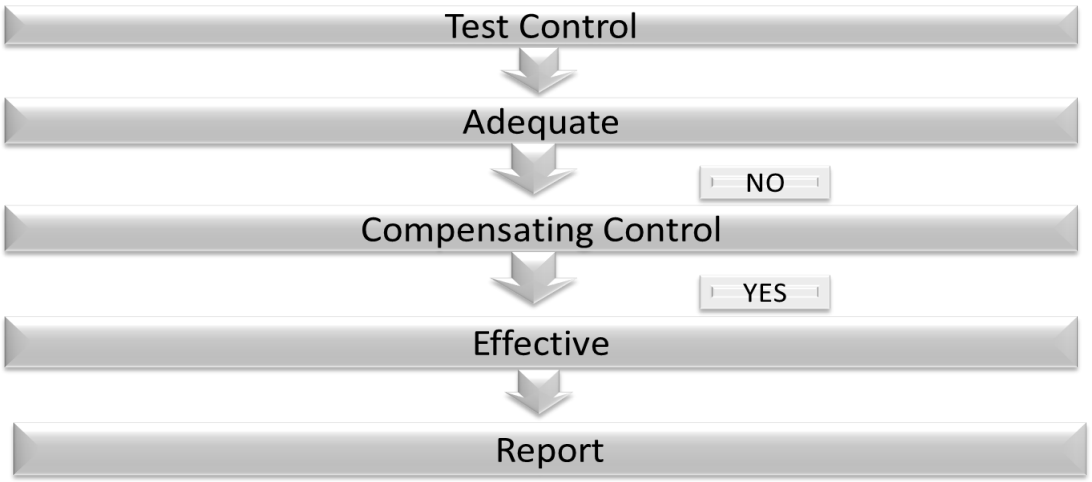
1. What is the objective of the control activity? (Completeness/Accuracy/Validity/Restricted access)
2. Who or what system performs the control activity?
    a. Do they understand the control objective?
    b. Are they competent to perform the control?
    c. When is the control activity performed? (Preventative/Detective/Corrective)
3. Is the control the most efficient control?
    a. Is the control very time consuming? (automated/manual/semi-automated)
    b. Is the control sustainable in the long term?
4. What is the frequency of the activity performed? (daily, weekly, monthly, bi-annually)

5. What mechanism is used to perform the activity? (Reports and systems)
6. Who is the "owner" of the activity? (Segregation of duties)
    a. Can the control be bypassed?
7. Does the control output match its objective?

Internal Controls are assessed as adequate if management has planned and designed them in a manner that provides reasonable assurance that the risk(s) for which the controls were intended will be mitigated to within a tolerable level in order to promote the achievement of the organization's objectives and goals in an efficient (accomplishes objectives and goals in an accurate and timely manner) and economical (accomplishes objectives and goals with minimum resources and effort) manner.

11. COMPENSATING CONTROLS

Adequacy reviews involve the review of the existing control using various methods to assess whether it reduces or mitigates the risk to a level of acceptance to management. The memo is suggesting where an existing control is inadequate a compensating control must be put in place to satisfy the objective or requirement for a control measure deemed to be inadequate using a compensating control template.



Compensating Control Template

Inadequate Control	Constraints	Document compensating Control

Name the Failed Control	List constraints preventing compliance with the requirement and identify any additional risk posed the failure of the inadequate control.	Document the compensating control and discuss how it may address the objectives of the failed control and mitigate the increased risk.

- Once the Compensating control template has been completed, effectiveness testing can be conducted.
- If the compensating control is adequate and effectiveness testing is successful, then it must be noted in the report that it is a compensating control and that the existing one control had failed.
- Depending on the outcome and the procedural changes which may still be affected by business in relation to the compensating control, a finding may be in the report in regard to the failed control.

12. CONTROL OPERATING EFFECTIVENESS TESTING

Controls should only be tested for effectiveness once they have been assessed for adequacy. If it is apparent that the internal control is inadequate, it should not be tested. If there are other controls which mitigate a particular risk, these should be considered.

For all key controls that were assessed as adequate, develop test/monitoring procedures to determine the operating effectiveness of the controls by considering the following:

- The test procedures performed will vary depending on whether an action plan or key control monitoring is being performed.
- The monitoring team should apply judgment in defining the nature and extent of monitoring procedures.
- The extent of testing will vary depending on whether it is a manual or an automated control.
- The number of items tested for automated controls can be minimal assuming that general computer controls are effective, and a detailed monitoring of the application system has been performed.
- Tests of manual controls are based on sampling, and the sample size is based on the frequency of the performance of the control.

12.1. Automated Control Testing

Monitoring is not responsible for testing IT controls; however, the team may test input and output (e.g. store and retrieve) controls to assess adherence to IT controls. The number of items tested for automated controls is one, as an automated control should follow the same logic irrespective of the number of times tested.

It is important to note that if you have already walked through an automated control during adequacy testing, you will have already in effect tested your sample of 1, therefore there is no need to test further.

12.2. Manual controls testing

Tests of manual controls are based on sampling, and the sample size is based on the frequency of the performance of the control.

12.3. Documentation of control testing

Control testing should show the objective of the control, who performed the control, the frequency of the control, the sample size and full details of the sample selected (including transaction population, volume, value and source) and conclusion drawn.

This can be documented on the Working paper template included, the RMP in the applicable column or directly onto Archer within the applicable Procedure in the Programme Library.

12.4 Programme Libraries

For each engagement only one Programme Library must be included. The Monitoring Specialist must first assess whether a Programme Library for a particular “Authoritative Source” exists prior to loading a new Programme Library. Where a Library exists but needs amendment, these changes must be forwarded to Archer Support (Archer CoE) for update to the Programme Library.

All sections of the Act (Authoritative Source) which is being reviewed must be included as Procedures within the Programme Library and these will be tested as part of the engagement. In the Programme Library and procedures, the Risk, Process, Control categorisations as well as Rationale for Business Process Rating and Business

Process Rating Level 1 will not be completed as only one programme library (AO) is completed per a legislation that is under review.

12.5. Working Papers (WPs)

The monitoring team should execute the test/monitoring procedures and document the results thereof in enough detail to support the conclusions reached within the working papers.

- An overall adequacy and/or effectiveness rating (Acceptable/Improvement required/Significant/Unacceptable) and a conclusion sentence should be documented in the WP
- Controls testing should include Adequacy and Effectiveness
  - Adequacy – Is the control defined, documented, evident, and measurable. (Identified during Walk-through)
  - Effectiveness – Is the control working as intended. (Identified during sample testing)

If the testing indicates that the control did not operate as intended, the following are steps to follow in dealing with control issues:

1) Understand the nature of the control issue. Consider the following in this regard:

- **Observation** – what is the current situation?
- **Standard** – what action should have been taken?
- **Cause** – what caused the observation to occur?
- **Effect** – what is the risk or impact as a result of the current situation?
- **Isolated/recurring incident** - is the incident isolated or is it the type of incident which will recur on a regular basis?

2) Extended testing: Typically, the control sample should not be extended, other than to verify the explanation provided when following up the failures with the client and and/or for significant findings where necessary. There may also be value in extending the control sample to determine the impact of the failure.

However, for controls occurring multiple times daily, if 1 in 25 fails, the sample may be extended by a further 25. If they fail rate of this 25 is 1 or above, the control is deemed to fail.

Should one control not be operating effectively, consider how the complete set of controls in aggregate mitigates the risk.

Frequency of Control	Control Type	Sample Size
Annual	Manual/IT dependent	1
Quarterly	Manual/IT dependent	2
Monthly	Manual/IT dependent	2 to 5. Select 3 if you require a mid-range.
Weekly	Manual/IT dependent	5 to 15. Select 10 if you require a mid-range.
Daily	Manual/IT dependent	20 to 40. Select 30 if you require a mid-range.
Multiple times per day	Manual/IT dependent	25 to 60. Select 30 or 45 if you require a mid-range.
As necessary	Manual/IT dependent	25 % of the occurrences limited to a minimum of 10 items but capped at 30 items.
IT General Controls	Manual/IT dependent	As per the guidance above.
IT Application Controls	Automated	One item per type of application control provided that the General Controls testing results were satisfactory.

3) Consider any compensating controls that may address the risk concerned: If a control is determined as not operating effectively, revisit compensating controls that may exist to contain the risk. It is important to note that the assurance we provide is in terms of whether controls over significant risks are effective. Should one control not be operating effectively, but there are adequate and effective compensating controls, we can still provide assurance that control over the risk is effective.

13. RISK RATING METRIC

Once testing of all key controls has been completed, the monitoring team must assign an opinion to each of the specific risk identified and tested as per the scope of the monitoring assignment. This risk opinion is an overall assessment of how well the risk is being mitigated based on the adequacy and effectiveness conclusions reached during fieldwork testing of the applicable key controls.

The definitions of these risk opinions are detailed for the monitoring report ratings in the following tables used for process and control ratings:

Compliance Monitoring Report/Process Rating	Description
High Assurance	The existing control environment provides a high level of assurance that material risks are identified and well managed, to ensure that business objectives will be achieved. No significant improvements are required .
Reasonable Assurance	The existing control environment provides reasonable assurance that material risks, which may threaten the achievement of business objectives, are identified and managed effectively. The compliance monitoring engagement has identified some scope for improvement in the environment. Appropriate action and time-lines have been agreed with management, in order to facilitate the achievement of business objectives.
Limited Assurance	The existing control environment provides limited assurance that material risks are identified and managed effectively. The achievement of business objectives is therefore threatened. Actions and time-lines to improve the adequacy and effectiveness of the environment have been agreed with management, in order to facilitate the achievement of business objectives.
No Assurance	The existing control environment provides no assurance that material risks are identified and managed effectively. There is therefore substantial risk that objectives will not be achieved. Immediate action is required to improve the environment.

Compliance Finding / Control Rating	Description
Acceptable	Key controls are adequate and operating effectively. Action is advisable. An isolated error, minor control deficiency or condition was identified during control assessments. The issue identified is managed effectively.
Improvement Required	Action is required. An error, control deficiency or condition was identified during a control assessment that can, and should be, corrected by management. These are non-adherence/non-compliance to controls, policies or regulations and the implementation of the recommendations can improve efficiency, effectiveness and service delivery.

Compliance Finding / Control Rating	Description
Significant Improvement Required	Immediate action is necessary to manage the potential effect/s as mitigating controls are partially adequate or partially effective. An error, control deficiency or condition which is a serious non-adherence/non-compliance to controls, policies or regulations.
Unacceptable	Urgent action is required to manage the potential effect/s, as no mitigating controls are in place. Critical findings were identified that could have a material negative impact on the risk control environment. Intervention strategies must be developed, executed and reported at appropriate governance levels.

Working Paper reviews:

- Working papers should be marked as prepared once they have been comprehensively completed and reviewed by the Engagement Reviewer.
- The Reviewer to confirm all issues identified during fieldwork by reflection on working papers were raised in the Finding sheet/Monitoring Report.
- The Reviewer should review the sample sizes; alignment of finding sheet to the working paper; testing strategy; and ratings of working papers.
- The Reviewer should ensure that all planning (Draft and Signed Scope letter), fieldwork (working papers and evidence) and reporting documents (Draft and Signed Monitoring Report) are saved on to Archer as well as in line with the Records Management approach for the Segment.
- For samples selected - Upload at least evidence of five (5) samples (but for example if one (1) was sampled, then upload evidence of the one (1) sample) for other assurance providers to re-perform and confirm results of the test.
- For findings raised – Upload evidence which supports the finding.

Monitoring – Reporting

14. RCRM ISSUES/FINDINGS

If a key control or management action plan does not adequately or effectively address or mitigate the relevant risk, a monitoring issue should be raised. Likewise, if one or more key controls do not adequately address or mitigate the relevant risk, consider the overall

implication of the combined key controls to that relevant risk. If the combined key controls do not adequately address or mitigate the relevant risk a monitoring issue should be raised.

All findings must be discussed and agreed with business prior to be loaded onto Archer, to ensure that all evidence in relation to a particular control has been provided for the review. In some instance, additional evidence may be provided by business which confirms that they control is actually adequate/effective as applicable.

Where findings have not been discussed and agreed with business the finding should not be loaded onto Archer, then additional evidence must be sought to close out the finding. These findings will not be removed/deleted from Archer, but rather further investigation/control testing must be facilitated to obtain the outcome confirmed by business.

All findings loaded on Archer must include:

- Accurate reflection of the root cause, clearly articulating the cause of the failure. For example, this should not read simply process error; rather, error cause through lack of application of four (4) eye principle process.
- Potential Impact providing a description of the Quantitative impact, e.g. error rates, potential/actual losses etc.
- “Recommendations” should include the requirement of the Act focusing on the letter and the spirit of the law.
- the classification must be completed in full.
- Estimated implementation date as well as a realistic plan of action to be agreed upon prior to the monitoring report being signed and distributed to stakeholders
- LOD 1 Implementer and owner as well as LOD 2 Compliance Officer
- Observer/SME – this should not be used as a catch all for information purposes as it creates bottlenecks/delays in the finalization and closure on a finding. This field is restricted to the inclusion of individuals who are SME’s and will provide the relevant information relating to the finding, i.e. rating, commentary on remediation action, status feedback, etc.
- Reference the “Annexure – MCOE LOD 1 Implementer and Owner Guide

Once an issue has been comprehensively completed, it must be marked as prepared by the creator. This must then be reviewed by the engagement manager within a reasonable time. Issues can be sent to client once an engagement is in Reporting. It is important that the monitoring specialist comprehensively completes the finalisation tab before clicking Yes to submit overall management response; refer to the section 19 Finalisation detailed below.

Where an Issue is raised which was not part of the scope of the engagement, these must be highlighted by the monitoring specialist as a matter for noting in the monitoring report and management must provide a plan of action to resolve the same. These may eventually after consultation with business be raised as findings within the engagement.

Where no findings are being raised through the engagement, it is imperative that the “For noting” is included to provide the reader of the report with context related to the scope, work performed and the results of such performance.

Matters for noting are housekeeping issues which are not key controls or failures, but rather issues that need to be highlighted to the business to create and strengthen the control environment and must be included under the Overall Conclusion section of the report.

Where a finding or issue is not a regulatory requirement, the issue should be raised as a matter for noting in the monitoring report and will not be loaded on archer for tracking purposes.

Once all findings have been agreed and reviewed the Draft Report may be exported from Archer. This Report may be edited to include additional information that the monitoring specialist deems necessary.

15. ENGAGEMENT REVIEW and DRAFT REPORT

Upon completion of fieldwork, the reviewer must evaluate whether enough monitoring work has been performed and documented to support the conclusions reached and the risk and overall opinions assessed. All fieldwork must be completed and appropriately reviewed. All review notes must be appropriately addressed and closed on Archer. Evidence of the reviews performed must be documented and retained on file. All reviews and signoffs of fieldwork performed must be performed prior to the issuance of the final report.

The Engagement Reviewer must then review the entire engagement and the overall engagement as reviewed. Thereafter, the final report may be sent to the client.

A close-out meeting may be conducted, and open items addressed should this be required. Thereafter engagement is deemed to have concluded and a draft report may be issued. The draft report must be issued within five (5) days of end of fieldwork. Once Draft Report is issued, Management has five (5) working days in which to respond to the Monitoring Team. If no response is received within 5 working days relevant escalations must be done by the Monitoring team.

16. QUALITY ASSURANCE

The Quality Assurance (QA) process is applicable only to MCOE Engagements to be executed after fieldwork, once all procedures have been completed and potential findings have been drafted on the Working Paper. The QA process must be facilitated prior to discussion with business of potential findings. The QA process will be conducted on a sample basis per an engagement in the Franchise/Segment Monitoring Plan.

The Analyst/Specialist must trigger QA on Archer/send email to QA Manager pending update to Archer for workflow.

The QA Manager will be responsible to:

a) Review the agreed scope against the procedures
b) Assessment of all the procedures and a sample for retesting of Procedures. QA Manager will include coaching notes to the Analyst/Specialist

c) QA Manager will provide feedback to the Analyst/Specialist in the form of Coaching notes for implementation. The Reviewer for the engagement will ensure that the Analyst/Specialist applies the changes per the coaching note. Thereafter the potential findings may be discussed with business.

d) Once business has agreed on the findings, the draft report containing the findings, including ratings and remediation action, will be provided to the QA Manager to trigger the final QA process

e) QA Manager will trigger the QA Forum which will consist of:
   - QA Manager
   - Segment Head of Monitoring
   - Monitoring Engagement Manager
   - Line manager (Monitoring Engagement Manager)
   - Reviewer
   - Segment/Franchise SME
   - Group SME (as applicable)

f) QA Manager to distribute report via email (or trigger QA Process of Archer – once enhancement completed). Consolidates all feedback received from QA Forum, which is obtained either via email, Skype /VC/Meeting discussion/meeting. QA Forum to exercise judgement in respect to the Finding in relation to the procedures and risks identified, as well as interrogate the remediation action confirmed by business to confirm that the action does in fact remediate the risk. In addition, the ratings assigned to the findings must be assessed to ensure that there is agreement on the rating of the identified risk. The turnaround time for the QA forum to be completed is three (3) days, if commentary is not received from a specific member of the forum within the three (3) days, the report will be issued to the analyst/specialist with the commentary received to be actioned.

g) Only after consensus and sign off (email approval acceptable) may the report be issued to the client/business. Once the report is issued to the specialist/analyst the review notes must be actioned by the specialist/analyst. If the specialist/analyst has any queries or requires clarity of the review notes, the specialist/analyst can approach the respective member from the QA forum to resolve the review notes. The engagement reviewer must ensure review notes are addressed.

17. MEMO STYLED REPORT

Where no testing was performed for example, there is not a population available to sample from, or the themes of the relevant act do not impact on the BU, then a Monitoring Team must issue a Memo (report) to management.

18. FINAL REPORT

Before the final monitoring report is issued, all amendments to the report based on the close-out meeting and comments received by management since the issuance of the draft report must be appropriately reflected in both the working papers and the monitoring report.

All findings must at this point be loaded onto Archer with all the necessary information included. The final report can then be exported from Archer and edited to include any additional information the monitoring specialist deems necessary.

The final report must be issued within five (5) working days from the issuance of the final draft report with agreed action plans.

This must be signed off by business and provided to the Monitoring Specialist, who must then upload this as the final report on Archer.

19. FINALISATION

Once the engagement has been concluded and the Final Report which was issued to business and signed off has been loaded onto Archer, the monitoring specialist must update the Finalization tab by populating the overall opinion, overall management response, risk impact on business and franchise, as detailed in the signed monitoring report. The rating of the Process categories in the Finalization tab will not be completed as only one program library (AO) per a legislation is completed.

The monitoring manager must then click on the Yes checkbox next to the "Submit Overall Management Response" field, then SAVE AND CLOSE. The Reviewer is then able to close off the engagement.

20. ISSUE VERIFICATION ("Verified by Compliance" STATUS)

MCOE and Segments will check/review the progress of the implementation status of agreed management action plans; and provide verification of the adequacy and effectiveness (appropriateness) of management's implementation of agreed action plans in the proceeding financial year.

All issues must be verified timeously, i.e. once LOD1 (Implementer and Owner) has confirmed that it has been implemented and approved, the issue must be verified as soon as is reasonably possible to allow for closure.

This will include testing that the remediation action implemented, mitigates the root cause and the risk which was identified, through an adequacy review and if applicable an effectiveness test.

The field within Archer that supports the reviews are illustrated (and highlighted) in table below:

Actual Implementation Date	LoD 2 - Issue Date Verified	Number of Times Date Revised (1)(1)	Count If Past Due > 90	Count If Past Due > 365	Overall Issue Status	1st LoD Issue Status - Implementer	1st LoD Issue Status - Owner	2nd LoD Issue Status - Risk Manager	2nd LoD Issue Status - Compliance Manager	3rd LoD Issue Status – Audit Manager
11/11/2019		3	No	No	Approved - Not Verified	Implemented	Approved	Not Verified	Not Verified	Not Verified

Issue Verification Assessment

The purpose is to ensure that a walkthrough is initiated and a fresh sample of the enhanced controls is independently tested for adequacy and effectiveness, respectively, and assurance provided that the risk has been mitigated.

To initiate Findings/Issue Verification, the LOD2 Compliance Officer may inform Business of the verification by email correspondence and no formal engagement letter is required. Reference may be made to the engagement already concluded and confirmation that this is on verification on a specific finding/issue which is to be completed.

20.1 Verification Procedure – Adequacy Testing

Verification requires the listed LOD2 Compliance Officer to perform Adequacy testing by:

- Obtaining evidence of the action plan that was followed by management and concur that the actions remediated the root cause. Application of Procedure 12.5:
    - enquiry by interview/walkthrough supported by minutes;
    - enquiry by control self-assessment questionnaires;
    - analytical review and/or data analytical analyses (where applicable); and
    - observation or inspection/walkthrough.
- Validation one (1) transaction/one (1) action etc.
- Keeping the evidence on Archer.
- Adding a comment in the “Implementation Tracking” section on Archer detailing the outcomes of adequacy test (i.e. evidence obtained and acceptable/not acceptable) .Use descriptive headings and include dates and names when capturing comments in the “Status update” field to confirm impacted business unit, process, control, etc. as it applies. See status update field below.

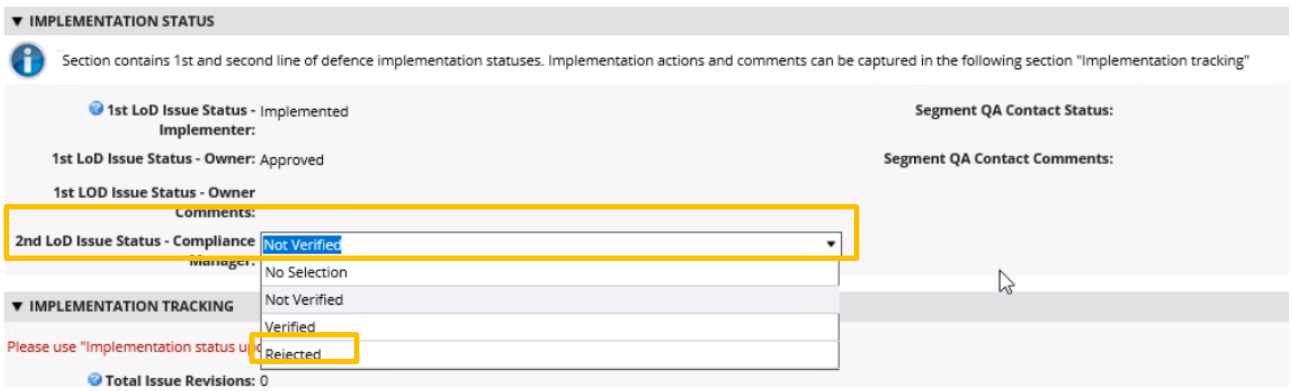
  This step requires that as part of adequacy testing, the remediated control is assessed and verified to have been implemented and that the design of the control is adequate to mitigate the identified risk. So a walkthrough of the remediate control should be completed to ensure that the documented status updates are in place.

Where the BU process owner does not have access to Archer and is not the LOD1 Implementer, he/she must request the listed LOD1 Implementer to log, populate and update the action plans on Archer on their behalf. Where the LOD1 Owner has challenges accessing the issue, it should be verified that the LOD1 Implementer has completed their Implementation and updated their status accordingly. This will initiate the workflow on Archer from the LOD1 Implementer to the LOD1 Owner.

Adequacy test results:

For both adequate and inadequate testing results evidence must be attached. Once testing has been completed, the results must be documented in the Implementation Tracking field on the issues on Archer.

- Should the action plans be found to be inadequate, a comment of such should be added to the Archer finding under “Status Update” and the finding should be marked “Rejected”. Archer will notify the implementer of the finding.



- Should the action plans be found to be adequate, a comment of such should be added to the Archer finding under “Status Update” and the finding should then be tested for effectiveness.

No formal report is required. However, the use of the Implementation Tracking section on Archer within the issue should be used to document outcomes of the Assurance testing.

20.2 Verification Procedure – Effectiveness Testing

To complete effectiveness testing a fresh sample of the enhanced controls is independently tested for effectiveness and assurance provided that the risk has been mitigated. Effectiveness testing requires us to confirm that the control is consistently applied across the selected sample.

Once adequacy has been successfully completed, Effectiveness testing must be performed by application of Procedure 12.5:

- Randomly selecting a new sample representative of the remediated base (if ring-fenced /remediated retrospective) or population (if new controls implemented prospective). Sample methodology table under Procedure 12.5 Working Papers to be applied.
- Performing effectiveness testing to ensure that the controls for the sample selected are functioning as intended and are consistently applied.
- Completing sample working paper. Template included in Annexure.
- Maintenance of the evidence on Archer.

Effective test results:

- If effective, update the Implementation Tracking section on the issue on Archer, as per the adequacy assessment above. The issue can then be marked as verified by compliance.
- If ineffective, the issue must be rejected for LOD1 Implementer and Owner to review and enhance the control.

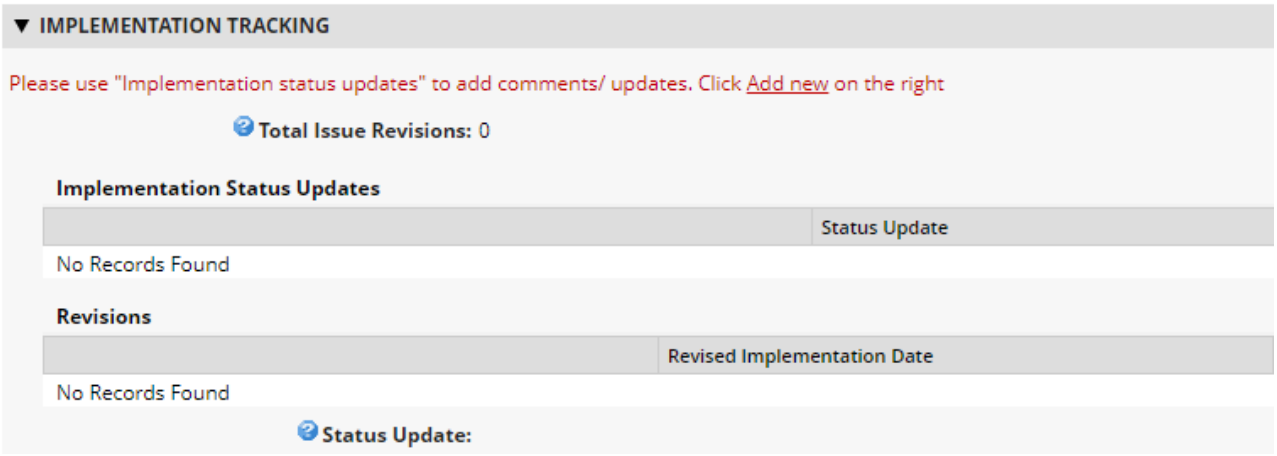
In order to efficiently manage verification, teams should apply the following approach:

- Finding/Issue verification must be performed in a timely manner as stated above and can also be completed in accordance with the themes of the monitoring activities as planned in a particular period/quarter (Thus incorporate into scheduled engagements rather than ad hoc engagements).

- When initiating a scheduled engagement, a report must be extracted from Archer of all "Verified" Archer findings and these should be included in scope to perform effectiveness testing and reporting within the engagement.

Once adequacy and effectiveness testing has been completed and the Archer Implementation Tracking section has been updated on the issue, as illustrated below, the issue can be marked "Verified by Compliance".

.



- If "Verified" is selected, the Overall Issue status of the finding will change to "Approved – Verified by Compliance".
- Use descriptive headings and include dates and names when capturing comments in the "Status update" field to confirm impacted business unit, process, control, etc. as it applies. See status update field above.

20.3 Level of work to be performed

The individual executing findings/issues verification should seek to obtain the same level of monitoring evidence and execution of fieldwork (i.e. walkthrough for adequacy assessments and sampling for effectiveness testing) for Issues Assurance as they would during the engagement.

As part of verification procedure, consideration should be given to the following which are reported to various governance committees at particular intervals:

- The timeliness of implementation in comparison to original deadline dates. (estimated versus actual implementation dates and assessment of aging of issue).
- The confirmation of adequacy and effectiveness of implementation of the action(s), revised action(s) or both. If alternative actions were designed and implemented, obtain the reason for change and assess the adequacy of the alternative action to mitigate the risk identified during the review.

21. RELIANCE/OTHER ASSURANCE PROVIDERS

It must be noted that where the Coverage Plan requires an engagement to be facilitated on an authoritative source that will be reviewed by another assurance provider, Compliance Officers may not place blind reliance on the work performed by such assurance provider. This includes simply obtaining the report issued by the other assurance provider and loading this onto the engagement on Archer as the final report. Other assurance providers include Internal and External Audit, Operational Risk, and/or Business Assurance.

The below process must be followed before reliance may be placed on the work performed by other assurance providers.

- Where an engagement is underway or has been completed by another assurance provider, the compliance officer must obtain the scope for such engagement
- This scope must be reviewed against the scope for Compliance, i.e. the completed risk management plan (RMP)
- The provisions included in the scope for review must be assessed in line with the scope of the RMP.
- control tests to be performed must be assessed to confirm consistency of testing.
- Where provisions or controls differ, the Compliance Officer must include these differing provisions in the testing to be performed by the Compliance Officer
- Assurance may then be obtained where there is consistency in terms of the applicable provisions and the control tests to be performed.
- For the balance, the Compliance Officer must then continue to engage with the applicable business area to continue the review

- In terms of the planning/scoping the Compliance Officer must then specify that part of the engagement will include taking assurance from the other assurance provider and all necessary documentary evidence relating thereto must be included. This will include but not be limited to:
  - The scoping documents
  - Working Papers
  - Evidence linked to working papers
  - Findings and Reports

22. COMBINED ASSURANCE

In order to place reliance on the work performed by either Internal or External Audit, the Combined Assurance Framework and Methodology to be finalised between all assurance providers, will govern the manner in which this process is executed. As such, the Operating Procedures must be read in conjunction with the Combined Assurance Charter, Framework and Methodology as applies.

23. FINDINGS/ISSUES EXTENSIONS MANAGEMENT PROCEDURE

These procedures are for the approval for extensions and are categorised in line with the significance of the identified risk.

Unacceptable and Significant Improvement findings

These must be signed off by business and must be presented to the relevant governance/executive committee for approval. It is to be noted that a compliance officer may not approve these extension requests. The extension application must include a rationale for request together with interim mitigating controls. An amended remediation date and if applicable remediation action must be provided with confirmation of the LOD1 Implementers and Owners.

Improvement Required Findings

These findings may be approved by Compliance for the first request only. Thereafter, where a further extension is required these must be presented to the relevant governance/executive committee for approval. The extension application must include a rationale for request together with interim mitigating controls. An amended remediation date and if applicable remediation action must be provided with confirmation of the LOD1 Implementers and Owners.

The inserted template needs to be completed for each finding/issue requiring and extension. The details required are listed below.

Finding Reference	
Business unit/Segment/Country	
Finding name	
Finding rating	
Potential Impact/Exposure	
Root Cause	
Initial Agreed Management action plan	
LOD 1 Implementer/Owner	
Initial Implementation Date	
Committee for Approval	
Status update, progress update *(including mitigating controls already implemented, still outstanding).*	
Rationale for extension	
Revised/Proposed Implementation Date	

24. ESCALATION PROCESS

RCRM MCOE supports all Segments with ensuring the Annual coverage plan and all high and very high legal requirements are reviewed. To this end, an Escalation Process is necessary to provide documented and approved timelines to ensure timely finalisation of all monitoring reports.

Escalation timelines will support the following:

- First Line of Business responsibilities where management action is required to support the monitoring intervention as well as proactively address any findings. This includes sign-off of the scope, provision of evidence through fieldwork, findings validation and remediation action plans, as an example

- Achievement of the Annual Monitoring Plan on a timely basis within the applicable governance cycle;

- Monitoring reports will remain relevant and support Second Line with the necessary Board escalations; and

- Alleviation of long outstanding reporting phases (Report remain in draft for extensive periods).

Stakeholder definitions	1st Line	2nd Line
Segment (SA)	Business Contact for Action	Head of Compliance (HoC)
		Compliance Manager (CM)
		Chief Risk Officer (CRO)
	Line Manager	Monitoring Champions (where applicable)
ROAI		Head of Compliance (HoC)
		Compliance Manager (CM)
		Chief Risk Officer (CRO)
In-Country	Process Owner (PO)	Head of Compliance (HoC)
	Chief Executive Officer (CEO)	Compliance Officer (CO)
		Compliance Manager (CM)
		Chief Risk Officer (CRO)

Escalation process elements

Scope sign off

- Monitoring Teams will provide Management/Business with the proposed scope electronically and follow up with a meeting to discuss.

- At the meeting all concerns and recommendations/suggestions for amendment to scope must be agreed.

Provision of Evidence (Fieldwork)

- When requested to do so, and within a reasonable period, Management/Business must provide the necessary evidence to support walkthroughs and the completion of the fieldwork for a review.
- In order for the Monitoring team to assess the control environment, this evidence needs to be provided to perform testing which confirms the controls which were detailed in the walkthroughs.

Validation of findings

- The Regulatory Risk Monitoring teams will provide management with draft findings and supporting evidence for management to validate.
- Validation should be completed before the Monitoring Report is finalised.
- Management acknowledges that any further supporting evidence will not be considered once the Monitoring Report is finalised (unless under exceptional circumstances for example when the correct process owner was not approached). All supporting evidence will be shared within 48hrs of request and no follow ups will be done.
- Any time period referred to in this process may be extended by agreement between the CEO and the Head of RCRM/Monitoring manager.

Escalation Timelines

Activity	Timeline	Description
Scope	2 days (48 hours)	The Monitoring team will provide the scope electronically prior to the meeting. Management must within 48 hours accept/reject the scope Monitoring team to confirm with Management timelines and escalation on Day 3

Activity	Timeline	Description
Evidence/Fieldwork	2-3 days	After walkthroughs have been performed the team will facilitate testing on the discussed procedures. There is a requirement for management/business to provide the teams with the necessary information for performance of the testing Should this not be provided within the required period it creates delays in the execution of testing and finalisation of the review. Monitoring team to confirm with Management timelines and escalation on Day 3
Report	Day 1 – 10 (Working days)	The first draft of the Monitoring Report (*findings validation by management already completed*) must be issued to the First Line of Business (process owner) by RCRM. Management has 10 working days to respond with: • Action plans/management comments; • Implementation dates; and • Physical sign off. A reminder e-mail will be sent every three (3) days by the Compliance Officer/Compliance Manager to the Process Owner.
	Day 11 – 15 (Working days)	RCRM to escalate to the impacted stakeholders, i.e. Executive responsible for Business or segment/country CRO (by written correspondence and including the draft report and trail of correspondence) when: • The ten (10) working days has lapsed, and the action plans/management comments and implementation dates have not been provided. • If finding discussions with the Process Owner and RCRM is at a "deadlock"

Activity	Timeline	Description
		(Disagreeing parties remain supportive of their viewpoints) or discussions result in conflicting views due to interpretation of the act/regulatory requirement then the finding requires immediate escalation. • All parties should agree that they are at a "deadlock" point. • If the dispute relates to interpretational differences, the matter should be escalated to a Subject Matter Expert (SME) to provide a view. • The Executive/CRO and RCRM have another five (5) working days (Day 11-15) to address possible conflicting views and strengthen the client relationship to ensure consensus is reached; action plans and implementation dates are prioritised; and sign-off is obtained.
	Day 16 - 17 (Working days)	Escalate to the high level stakeholder e.g. CEO/Head of Division/Segment when: • No resolution could be obtained during day 11 – 15. The client and RCRM have another two (2) working days (Day 16-17**)** to escalate the matter to the relevant CEO for resolution.
	Day 18 (Working day)	The Segment HOC or HOM: • Escalates the lack of management comments /action plans/implementation dates to the CRO and CEO in the same communication. • Informs the CEO and CRO in writing that the Monitoring report will be finalised; circulated; and reported to Governance Committees without reflecting the client's action plans/management comments; implementation dates; and sign off if not received within 17 working days from the date of first escalation.

Activity	Timeline	Description
		• A further note will be made in the report that no sign-off was obtained after a formal Escalation process was followed.
Other	Immediate escalation	The Segment RCRM teams will immediately escalate to the HOC to immediately engage with the CRO when: • First Line of Business pushes back on the Monitoring team entering for a review • Sampled documentation is not provided by First Line of Business within the prescribed period after written request to First Line of Business (i.e. 2-3 working days, unless extenuating circumstances are communicated by either RCRM or Management/Business) – (Monitoring team to provide what time period they usually give the client) • Finding discussions with the client is at a "deadlock" or discussions result in conflicting views due to interpretation issues relating to an act/regulatory requirement. • Any other issues where management assistance is required.

25. GUEST MONITOR PROGRAMME

The programme is designed to enable the MCOE to insource specialised skills, additional resourcing and just-in-time flexibility. The Guest Monitor Programme brings individuals with in-depth understanding of business and monitoring knowledge to enable the delivery of greater value to the MCOE stakeholders. In doing so, cross pollination of business and regulatory risk and controls monitoring knowledge occurs between the Monitoring Team members and business.

Any permanent employee of the FirstRand Group and/or any of its subsidiaries with sufficient, useful and relevant experience may participate in the RCRM MCOE Guest monitor programme provided that they have provided written approval from their line manager for the time allocated for Monitoring activities.

The Monitoring analyst/specialist, LoD1 and/or LoD2 staff member/s cannot be part of a Monitoring engagement if:

- Staff allocated have significant threats to their independence or lack the level of competence required to perform the proposed work.
- It relates to work the impacted staff has been involved in and which has already been, or will be, reported to management or those charged with governance by their function.
- The work relates to the functional review and assessment of LoD2.

The programme will be run two-fold with the following versions:

- A guest monitor that has in-depth business knowledge insourced to transfer business knowledge to the monitoring team.
- A guest monitor insourced from one MCoE monitoring team to another (including across country

Guest Monitors will interact with MCOE staff to collaboratively identify mutually beneficial engagements. MCOE Segment Head of Monitoring and the Guest Monitor will be responsible to for the listed process activities, roles and responsibility criteria as listed below:

MCOE Activity	Guest Monitor Activity
Requirements to be addressed prior to engaging the Monitoring Analyst/Specialist, LoD1 and/or LoD2 staff to provide direct assistance in the capacity of a Guest Monitor.	The Guest Monitor to attain the following: • Obtain written agreement from an authorized representative of the function that the staff member will be allowed to follow the MCOE's instructions, and there will be no interference from the area they currently work in; and • Obtain written agreement from the Guest Monitor that they will keep confidential specific matters as instructed by MCOE management and inform MCOE of any threat to their objectivity that may arise during the engagement.
Provide Training for the Guest Monitor on the Monitoring Standards and Operating Procedures, and where appropriate, provide Archer Training.	Examine and raise insight against the preparatory materials before the start of the monitoring engagement, such as information about business context, inherent risks (as defined in line with risk

MCOE Activity	Guest Monitor Activity
	assessments and Risk Management Plans), regulatory requirements and interpretation and understanding, and other relevant information applicable.
Solicit feedback from the Guest Monitor and the assigned MCOE team members during and after the engagement and evaluate performance and satisfaction with the Guest Monitor programme.	This information should be shared with the allocated Manager, Segment Head of MCOE, and the FirstRand Head of Monitoring & Assessment. Thus, eliciting on-going feedback on the value of the programme to ensure continuous improvement.

MCOE Segment HOM would determine the nature and extent of work that may be assigned to a Guest Monitor considering timing, extent of direction, supervision and review that is appropriate in the circumstances.
• The amount of judgment involved in:
  • Obtain written agreement from an authorized representative of the function that the staff member will be allowed to follow the MCOE's instructions, and there will be no interference from the area they currently work in.
  • The inherent risk of the legislative provisions, processes, business and regulatory requirement complexity and risk profile of the business.
  • The Guest Monitor's evaluation of the existence and significance of threats to the objectivity and level of competence of the LoD1 and/or LoD2 staff who will be providing such assistance.	

MCOE Segment HOM will direct, supervise and review the work performed by the Guest Monitor on the engagement in line with the normal engagement review processes and the MCOE Monitoring Standard.	A learning plan will be developed and agreed with the respective line manager. This will ensure that the Guest monitor's tenure in the MCOE is beneficial to the individual and enables the MCOE to assess performance against agreed key performance indicators. The learning plan

MCOE Activity	Guest Monitor Activity
	may be documented in email format and agreed with the guest monitor.
The respective line manager within MCOE will provide regular, at a minimum monthly, feedback to the Guest Monitor on performance. • Where performance within the assigned engagement is deemed to be unfavourable to the efficiency and effectiveness of MCOE, the Guest Monitor's tenure and approval to continue participating in the programme may be revoked.	The respective line manager to whom the Guest Monitor reports will be provided with regular feedback, at a minimum monthly, on the Guest Monitor performance. • The Guest monitor and the respective business line manager will be notified via email and any assets allocated to the Guest Monitor will need to be returned within 48 hours

ANNEXURES:

Name
MCOE Staffing Module Archer Appointment (Section 9.3)
Annexure - Staffing Module Archer Appoi
Self-Disclosed Issues – Factual Correctness (Section 9.9)
FSR RCRM SDI Template April 2020.c
2.3.2 Example Sample Testing Sheet (Section 9.15.1)
2.3.2 Example Sample Testing Sheet
MCOE LOD 1 Implementer and Owner Guide (Section 14)
Annexure - LOD 1 implementer and Owı

FNB
First National Bank
como podemos ajudar?

Memorandum

To:	FNBM EXCO
From:	FNBM Credit & Finance
Date:	29 January 2021
Subject:	Write off Process

PURPOSE

The purpose of this document is to outline the write-off process – relating to:

- Mandatory / regulatory (i.e. Aviso 16) write offs
- Dormant account write-offs (negative balances)
- Debt relief/settlement agreement write offs

WRITE OFFS – REGULATORY & DORMANT ACCOUNTS (NEGATIVE BALANCE)

Nº	WRITTEN OFF PROCESS	BUSINESS OWNER
1	Identify monthly accounts to be written off as per Central Bank Directive 16	CREDIT
2	Ensure 100% provision	
3	Obtain SCRC & DRC (DRC if required) approval	
4	Submit list of accounts to IT for processing closure	
5	Settle / repay the due instalments	IT
6	Settle full capital amount	
7	Cancel all seal tax and penalty fees	
8	Credit loan account to nil using provisions GL(If the account balance is on Local or foreign currency use the Respective GL with the correspondent currency to use the provisions)	
9	Open CCO/residual account showing both capital and interest	
10	Recoveries to manage the residual accounts as per the current recoveries process	CREDIT
11	Send the list of residual accounts to Credit in order to recon/validate that all accounts were closed	IT
12	Credit to verify the confirmation of closure to both the IT and Finance teams	CREDIT
13	Reverse any interest accrual/charges from the residual accounts	FINANCE
14	Reconcile the Provision and other GL accounts	

- Mandatory (Regulatory) write offs will follow the directive from the Central Bank as per the Aviso 16 credit policy. These accounts require write off once they have reached a maximum NPL ageing. These write offs will occur monthly and will be managed/coordinated by the Credit team. IT and Finance play a supporting role in the process.
- Dormant accounts with negative balances are included in this process as they will age in NPL until required to be written off as per the directive.
- The write off process was recently revised to include all product types and to also cater for US$ currency facilities.
- The process is being managed as part of the credit optimization project and will go live in February (next month).

DEBT RELIEF/SETTLEMENT AGREEMENTS WRITE OFFS

This occurs under the following scenarios:

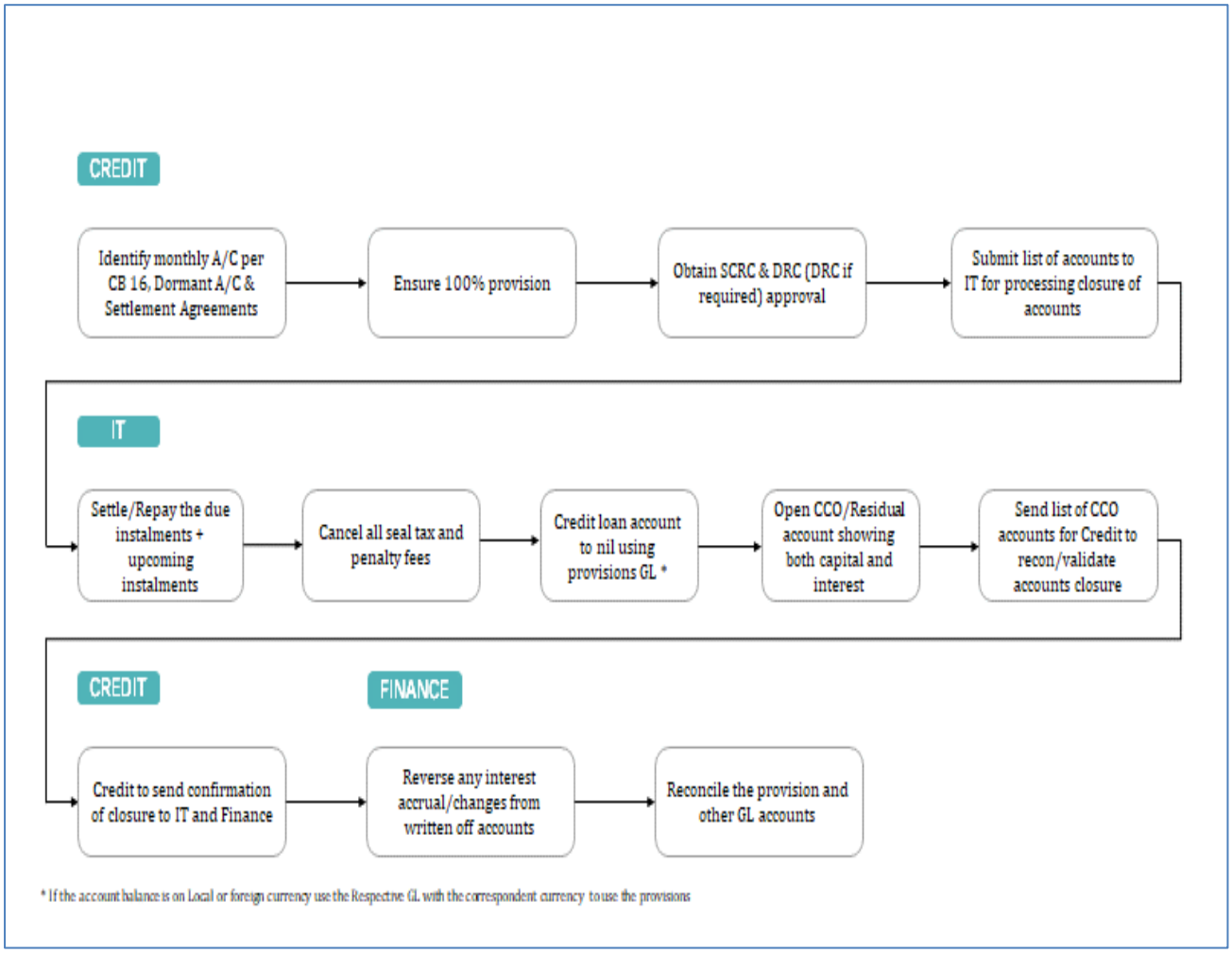
- When the bank has reached an agreement with the client to waive/discount either capital, interest or both as part of the settlement. This normally applies to delinquent or NPL classified accounts whereby the objective is to salvage exposure and minimize the credit risk.
- If the bank has recovered less than the total exposure through the sale of assets via Court auction. The balance of exposure is written off is unrecoverable.
- When clients settle debt prior to maturity and request for the waiving of the early settlement penalties.

The following information is required as part of the recommendation for debt relief/settlement agreement. The memo is then presented to the SCRC/DRCC for approval

- Brief client background
- Account classification and NPL ageing (if in NPL)
- Status of litigation & recommendation from Attorney firm
- Security value (with updated valuation)
- Provision held. Credit will ensure that capital provision is held, Finance to ensure that ISP (interest in suspense) provision is held

---

PROCESS MAP FOR WRITE OFFS



APPROVAL FORUM

The FNBM Senior Credit Risk Committee (SCRC) and FSR Debt Restructure Credit Committee (DRCC) are the mandated bodies that approve all write offs. This mandate can be delegated to sub-committees.

FNB
First National Bank
como podemos ajudar?

Memorandum

To:	FNBM EXCO
From:	FNBM Credit & Finance
Date:	29 January 2021
Subject:	Process for the management of Properties in Possession (PIP)

PURCHASING AND SELLING A PROPERTY/PIP:

- Approval panel consists of – HoC, CEO and CFO. Consensus is required to reach a decision.
- The proposal/recommendation to purchase or sell the PIP will be prepared by Credit Recoveries in conjunction with Finance.
- The recommendation should include a detailed background of the case and all actions taken to recover from the client. Total exposure including provision held to be shown (if the account remains on balance sheet) or total written-off exposure against the client. The exposure to be broken down into capital and interest.
- **For a purchase** – detailed status of the litigation process and outcome of the auction process (i.e. if the property had advanced to an auction at that stage) is required.
- **For a sale** – detailed explanation of all initiatives taken to sell the property to date (e.g.: marketing and advertisements done, informing our customer base or other interested 3rd parties) and including the evidence of all/any offers received for the sale.
- Critically an updated valuation together with a strong motivation for the purchase/sale must accompany the proposal. The valuation should not be older than 6 months and sourced from the Bank approved valuator only.
- All ancillary property costs incurred to date (once held as a PIP) or to be incurred with a proposed acquisition. Property or holding costs relate to property rates, taxes, utilities, insurance, security and maintenance.
- Also include the expected timeframe to dispose/sell the asset should the proposal be recommending an acquisition as a PIP.
- The CEO is mandated on behalf of the FNBM Board to sign the Deed of purchase and sale.
- Any change to this mandate should result from a resolution of the Board and documented in the minutes accordingly.

ACCOUNTING TREATMENT FOR A PURCHASE/SALE – TBC (Await confirmation from Group Finance):

- **On balance sheet**
- **Off balance sheet**

The expectation and indicative guidelines thus far recommend that the property/asset is held off-balance sheet. For this reason, the loan is to be fully provided at the time of acquisition into PIP. It is important to ensure that the property is bought inn at an appropriate and conservative price relative to the market.

MAINTENANCE OF PIP:

- As soon as ownership of the property is registered in favor of the Bank or the Bank is appointed trustee by the Court, Credit Recoveries shall notify the Finance and Infrastructure Departments to take the necessary actions to secure and ensure the necessary maintenance of the property.
- Following the purchase, for safeguarding reasons the locks and keys to the property must be replaced. The Finance department will become responsible for the overall management and maintenance of the property. Credit Recoveries will remain available to provide any required support.
- Once in possession, all maintenance charges will be incurred by the Bank.
- It is critical to ensure that the property is insured and is well secured (eg: 24-hour security, armed response) as the property is now under Bank ownership.
- Finance is responsible for maintaining an up-to-date record of all costs incurred for maintenance, accordingly these costs shall be considered in determining the appropriate sale price at the time of a sale.
- Monthly visits/inspections to be undertaken to ensure that properties are being maintained in good condition.
- LARC is to manage the revaluation of the property on an annual basis or upon ad-hoc request by the approval panel.

DISCUSSION POINTS: To be discussed at ExCo

- Accounting treatment – currently the Group Finance team are working on a PIP policy that governs the accounting treatment and overall management of PIPs. We have been told that the policy is WIP and expected to be concluded early next year. From our discussions with the SA team, we believe the policy should align to the abovementioned processes.
- Whether employees or their families are eligible to purchase PIPs or not.

Our recommendation is to adopt the proposed process with immediate effect until the final FSR Group PIP policy is concluded. We shall review the Group policy once obtained for adoption.

FNB MOÇAMBIQUE, SA PRIVACY POLICY

CCTV NOTICE

DOCUMENT CONTROL

POLICY LEVEL:	FNBM
EFFECTIVE DATE:	31th April 2021
NUMBER OF PAGES:	3
DATE	15th February 2021
APPROVED BY:	EXCO
Document Owner	Name: Sérgio Gomes Designation: Chief Operation Officer Physical Address: 420, 25 de Setembro, JATI, 1st Floor Tel: +258 21 35 5905 e-mail: Sergio.gomes@fnb.co.mz
VERSION NUMBER:	1.0
SIGNATURE	Peter Blenkinsop (Chairman)

Proposed CCTV Notice – Branch/ Cash Centre / ATM

“These premises are monitored by CCTV. By entering these premises, you agree to the processing of your image and personal information for the detection, prevention and prosecution of crime, as the law requires and to protect your, our and others lawful interests. For more on the Bank’s privacy notice, visit our website.”

Proposed Privacy Notice – Head office (CCTV notice to be built in)

“These premises are monitored by CCTV. By entering these premises, I agree to FNB using my personal information (PI), such as my image, name and contact details, to manage my entry into the building to protect my, our and others lawful interests and for the detection, prevention and prosecution of crime as the law requires. FNB shall delete my PI once this purpose has been concluded. For more on FNB’s privacy notice, visit our website.”

Proposta de Aviso de CCTV – Balcão/ Tesouraria Central / ATM

Estas Instalações dispõem de sistema de vídeovigilância CCTV. Ao aceder, concede a captação da sua imagem e dados pessoais e respectiva utilização em casos de prevenção, investigação de crimes e protecção de interesses legítimos conforme previsto no artigo 41º da Constituição da República de Moçambique.

Proposta de Aviso de CCTV – Sede – Serviços Centrais (Aviso de instalação de CCTV)

Estas Instalações dispõem de sistema de vídeovigilância CCTV. Ao aceder, concede a captação da sua imagem e dados pessoais e respectiva utilização em casos de prevenção, investigação de crimes e protecção de interesses legítimos conforme previsto no artigo 41º da Constituição da República de Moçambique.

POLÍTICA DE PRIVACIDADE DE DADOS DO FNB MOÇAMBIQUE, SA.

POLÍTICA DE PRIVACIDADE DO CLIENTE

POLÍTICA DE PRIVACIDADE DO FNB

DOCUMENTO DE CONTROLO

NÍVEL DA POLÍTICA:	FNBM
DATA EFECTIVA:	30th April 2021
NÚMERO DE PÁGINAS:	13
DATA	15th February 2021
APROVADO POR:	EXCO
Titular do Documento	Nome: Sergio Gomes Designação: COO Endereço Físico: 420, 25 de Setembro, JATI, 1st Floor Tel: +258 21 35 5905 e-mail:
VERSÃO NÚMERO:	1.0
ASSINATURA	Peter Blenkinsop (Presidente)

POLÍTICA DE PRIVACIDADE DO FNB

IMPORTANTE

O presente importante documento explica como o FNB Moçambique irá processar a sua informação pessoal.

Quando nos referimos a "processar", significa como recolhemos, utilizamos, armazenamos, disponibilizamos, destruímos, actualizamos, divulgamos, ou tratamos de outra forma a sua informação pessoal. Como regra geral, só iremos processar a sua informação pessoal se tal for necessário para prestar ou oferecer um serviço, fornecer um produto ou realizar uma transacção com o cliente. Respeitamos a sua privacidade e iremos tratar a sua informação pessoal de forma confidencial.

Podemos combinar a sua informação pessoal e utilizar a informação pessoal combinada para qualquer dos fins declarados na presente Política de Privacidade.

No presente documento qualquer referência a "nós" ou "nosso" é interpretada como FNB Moçambique SA.

MUITO IMPORTANTE: Se fizer uso dos nossos serviços, bens, produtos e canais de serviço, concorda que podemos processar a sua informação pessoal conforme explicado na presente Política de Privacidade. Por vezes, poderá dar-nos o seu consentimento para processarmos a sua informação pessoal. Leia-a cuidadosamente considerando que pode limitar os seus direitos.

NOTA: Considerando que o FNB Moçambique, SA é uma subsidiária do FirstRand Limited, que é uma organização global, esta Política de Privacidade aplicar-se-á ao processamento de informação pessoal por qualquer membro do FirstRand Limited a nível global. Se o FNB Moçambique, SA. processar informação pessoal para outra parte ao abrigo de um contrato ou mandato, a política de privacidade da outra parte aplicar-se-á ao processamento.

O FNB Moçambique, SA. pode alterar regularmente esta Política de Privacidade se a lei ou as suas práticas comerciais assim o exigirem.

A versão da Política de Privacidade apresentada no nosso website aplicar-se-á a todas as interacções que o cliente tiver com o FNBM. Para consultar a versão mais recente desta Política de Privacidade visite o seguinte website < http://www.fnb.co.mz/>.

Conteúdo

1. O QUE É INFORMAÇÃO PESSOAL?

As informações pessoais referem-se à qualquer informação que o identifique ou que se relacione especificamente com o cliente.

As informações pessoais incluem, entre outras, as seguintes informações respeitantes ao cliente:

- Estado civil (casado, solteiro, divorciado);
- nacionalidade;
- idade;
- língua; data de nascimento; educação;
- o seu histórico financeiro (como o seu rendimento ou a sua compra, investimento e comportamento bancário com base, entre outros, em transacções de conta);
- o seu número de identificação (como um número de conta, número de identidade ou número de passaporte);
- o seu endereço de e-mail; endereço físico (como endereço residencial, do trabalho ou a sua localização física); número de telefone;
- os seus identificadores online; perfis nas redes sociais;
- suas informações biométricas (como impressões digitais, sua assinatura ou voz);
- sua raça; género; sexo; gravidez; origem étnica; origem social; cor; orientação sexual;
- a sua saúde física; saúde mental; bem-estar; deficiência; religião; crença; consciência; cultura;
- seu histórico médico (como o seu estado de HIV/SIDA); histórico criminal; histórico de emprego;
- as suas opiniões, preferências e opiniões pessoais;
- sua correspondência confidencial; e / ou
- os pontos de vista ou opiniões de outras pessoas sobre o cliente e seu nome constituem igualmente suas informações pessoais.

As informações pessoais incluem informações pessoais especiais, conforme explicado abaixo.

2. QUANDO PROCESSAREMOS A SUA INFORMAÇÃO PESSOAL?

Só processaremos as suas informações pessoais para fins legais relacionados com o nosso negócio se o seguinte se aplicar:

- se o cliente tiver consentido;
- se uma pessoa legalmente autorizada por si, pela lei ou por um tribunal, tiver consentido;
- se for necessário concluir ou executar sob um contrato que celebramos com o cliente;
- se a lei o exigir ou permitir;
- se for necessário para proteger ou defender o seu interesse legítimo, o nosso ou o de terceiros; e / ou
- se se tratar de um menor, através do consentimento de uma pessoa competente (como um pai ou responsável.

3. O QUE É INFORMAÇÃO PESSOAL ESPECIAL?

Informações pessoais especiais são informações pessoais sobre:

- suas crenças religiosas;
- suas crenças filosóficas (por exemplo, onde o cliente participa de um concurso e é solicitado a expressar sua visão filosófica);
- sua raça (onde o cliente solicita um produto ou serviço em que as informações estatísticas devem ser registadas);
- sua origem étnica;
- sua filiação em sindicatos;
- suas convicções políticas;
- sua saúde (onde solicita uma apólice de seguro);
- sua vida sexual (onde solicita uma apólice de seguro);
- suas informações biométricas (como verificar sua identidade); e / ou
- o seu comportamento criminoso e a alegada prática de uma infracção (por exemplo, para prevenir o branqueamento de capitais conforme exigido por lei ou quando se candidata a um emprego ou estabelece uma relação com o FNBM).

4. QUANDO IREMOS PROCESSAR A SUA INFORMAÇÃO PESSOAL ESPECIAL?

Podemos processar as suas informações pessoais especiais nas seguintes circunstâncias:

- se tiver consentido o seu processamento;
- se o processamento for necessário para criar, usar ou proteger um direito ou obrigação legal;
- se o processamento for para fins estatísticos ou de pesquisa e todas as condições legais forem satisfeitas;
- se as informações pessoais especiais foram tornadas públicas pelo cliente;
- se o processamento for exigido por lei;
- se a informação racial for processada, e o processamento for necessário para identificá-lo; e / ou
- se as informações de saúde são processadas, e o processamento for para determinar o seu risco de seguro ou para cumprir uma apólice de seguro ou para impor um direito ou obrigação de seguro.

5. QUANDO E COMO IREMOS PROCESSAR INFORMAÇÃO PESSOAL DE MENORES

Um menor é uma pessoa que é definida como menor pela legislação de um país e que não foi reconhecida como um adulto pelos tribunais de um país.

Processamos as informações pessoais de menores, se a lei permitir.

Só processaremos as informações pessoais de menores se uma ou mais das seguintes opções se aplicar:

- uma pessoa que pode concordar legalmente consentiu o processamento, sendo um pai ou responsável;
- o processamento é necessário para criar, utilizar ou proteger um direito ou obrigação legal, como quando o menor é herdeiro num testamento, beneficiário de um consórcio, beneficiário de uma apólice de seguro ou segurada em termos de uma apólice de seguro;
- as informações pessoais da criança foram tornadas públicas pelo menor, com o consentimento de uma pessoa que pode concordar legalmente;
- o processamento seja para fins estatísticos ou de pesquisa e todas as condições legais são satisfeitas;
- em que o menor é herdeiro num testamento, se necessário para dar efeito ao testamento;
- quando o menor é beneficiário de um fundo fiduciário, se necessário para dar efeito à escritura fiduciária;
- onde o menor beneficia de uma conta bancária como uma conta de investimento ou poupança; e / ou
- se o menor for uma pessoa segurada ou beneficiária de uma apólice de seguro, se necessário para dar efeito à apólice.
- onde o menor tem idade legal suficiente para abrir uma conta bancária sem a assistência dos pais ou do tutor;
- se o menor for uma pessoa segurada ou beneficiária de uma apólice de seguro, se necessário para dar efeito à apólice.

6. QUANDO E ONDE OBTEMOS INFORMAÇÃO PESSOAL RESPEITANTES AO CLIENTE?

- Recolhemos informações pessoais directamente do cliente.
- Recolhemos informações sobre o cliente com base no uso dos nossos produtos, serviços ou canais de serviço (como websites, ATMs)
- Recolhemos informações sobre o cliente com base em como se envolve ou interage com o FNBM, como em redes sociais, e-mails, cartas, telefonemas, pesquisas.
- Recolhemos informações sobre o cliente de fontes públicas (como jornais) e de terceiros com os quais interagimos com a finalidade de conduzir os nossos negócios (como parceiros, fornecedores de listas ou nossos fornecedores de serviços).

Se a lei assim o exigir, solicitaremos o seu consentimento antes de recolher informações pessoais sobre o cliente junto de terceiros.

Os terceiros junto dos quais podemos recolher as suas informações pessoais incluem, mas não se limitam, ao seguinte:

- FNBM, quaisquer empresas ligadas ao FNBM, empresas subsidiárias, seus associados, cessionários, delegados, designados, afiliados ou sucessores em título e/ou terceiros nomeados (como seus agentes autorizados, parceiros, empreiteiros e fornecedores) para qualquer um dos propósitos identificados nesta Política de Privacidade;
- membros do FirstRand Limited (que incluem o First National Bank, WesBank (incluindo a Direct

Axis SA (Pty) Ltd.), Rand Merchant Bank) e FirstRand Investment Management Holdings Limited (Ashburton Investments), FirstRand Life Assurance Limited, FirstRand Limited, quaisquer empresas ligadas, subsidiárias, seus associados, cessionários, delegados, consignatários, afiliados ou sucessores em título e/ou terceiros nomeados (como os seus agentes autorizados, parceiros, subcontratados e fornecedores) para qualquer dos fins identificados na presente Política de Privacidade;

- cônjuge, dependentes, parceiros, empregador, requerente conjunto ou titular da conta e outras fontes semelhantes;
- pessoas que devidamente autorizadas pelo cliente a compartilhar as suas informações pessoais, como uma pessoa que faz uma reserva de viagem em seu nome ou um médico para fins de seguro;
- advogados, agentes de rastreamento, cobradores de dívidas e outras pessoas que auxiliam na execução de acordos;
- prestadores de serviços de processamento de pagamentos, comerciantes, bancos e outras pessoas que auxiliam no processamento das suas instruções de pagamento, como fornecedores de pagamentos com cartões (VISA ou MasterCard);
- seguradoras, correctores, outras instituições financeiras ou outras organizações que prestam auxílio no processo de subscrição de seguros e seguros vida, fornecimento de apólices e produtos de seguro e seguro vida, avaliação de sinistros de seguros e seguros vida e outros fins relacionados;
- autoridades policiais e de prevenção de fraude e outras pessoas encarregadas da prevenção e repressão de crime;
- autoridades reguladoras, mediador da indústria, departamentos governamentais, autoridades fiscais locais e internacionais;
- agências de crédito;
- fiduciários, executores ou curadores nomeados por um tribunal de justiça;
- prestadores de serviços de verificação de cheques;
- nossos provedores de serviços, agentes e subcontratados, como correios e outras pessoas que usamos para oferecer e fornecer produtos e serviços ao cliente;
- tribunais ou órgãos judiciais;
- Fornecedores de listas de marketing.

7. RAZÕES PELAS QUAIS É NECESSÁRIO PROCESSAR A INFORMAÇÃO PESSOAL DO CLIENTE

As suas informações pessoais serão processadas pelas seguintes razões e de acordo com a legislação do país:

- para lhe fornecer produtos, bens e serviços;
- comercializar os nossos produtos, bens e serviços;
- responder às suas questões e reclamações;
- cumprir os requisitos legislativos, regulamentares, de risco e de compliance (incluindo

orientações, sanções e regras), códigos de conduta voluntários e involuntários e acordos do sector ou para satisfazer os requisitos de informação e pedidos de informação;
- detectar, prevenir e denunciar acções de roubo, fraude, branqueamento de capitais e outros crimes. Isso pode incluir o processamento de informações pessoais especiais, como alegado comportamento criminoso ou o fornecimento de informações falsas, enganosas ou desonestas ao abrir uma conta com o FNBM ou evitar a responsabilidade por negligência;
- para fazer cumprir e cobrar qualquer acordo quando estiver em situação de incumprimento ou violação dos termos e condições do acordo, como rastrear o cliente ou instituir procedimentos legais contra o cliente;
- realizar pesquisas de mercado e comportamentais, incluindo pontuação e análise para determinar se o cliente se qualifica para produtos e serviços ou para determinar o seu risco de crédito ou seguro;
- desenvolver, testar e melhorar produtos e serviços para o cliente;
- para fins históricos, estatísticos e de pesquisa, como segmentação de mercado;
- para processar instrumentos de pagamento (como um cheque) e instruções de pagamento (como uma ordem de débito);
- para criar, fabricar e imprimir instrumentos de pagamento (como um cheque) e dispositivos de pagamento (como um cartão de débito);
- realizar avaliações de acessibilidade, avaliações de crédito e pontuação de crédito;
- para desenvolver modelos de crédito e ferramentas de crédito;
- para abrir, gerir e manter as suas contas ou relacionamento com o FNBM;
- divulgar e obter informações pessoais de agências de crédito relacionadas ao seu histórico de crédito;
- para permitir que possamos efectuar a entrega de bens, documentos ou avisos ao cliente;
- segurança, verificação de identidade e para verificar a precisão das suas informações pessoais;
- para comunicar com o cliente e executar as instruções e pedidos dos clientes;
- para pesquisas de satisfação de clientes, promoções e outros eventos;
- subscrição e administração de seguros e seguros vida;
- processar, considerar ou avaliar indemnizações a receber resultantes de sinistros;
- fornecer apólices de seguros e produtos e serviços relacionados;
- permitir que o cliente participe e utilize produtos e serviços de valor agregado;
- avaliar os nossos riscos de crédito e seguros; e / ou
- para quaisquer outros fins relacionados.

8. COMO USAMOS A INFORMAÇÃO PESSOAL DO CLIENTE PARA FINS DE MARKETING

- Usaremos as informações pessoais do cliente para comercializar produtos financeiros, seguros, investimentos e outros serviços bancários relacionados com o cliente.
- Também podemos comercializar produtos, bens ou serviços não-bancários ou não-financeiros para o cliente.
- Faremos isso pessoalmente, por correio, telefone ou canais electrónicos, como SMS e e-

mail.

- Se não for nosso cliente, ou em qualquer outro caso em que a lei o exija, só iremos realizar as nossas actividades de marketing através de comunicações electrónicas com o seu consentimento.
- Em todos os casos o cliente pode solicitar o cancelamento do envio de comunicações de marketing a qualquer momento.

9. QUANDO IREMOS UTILIZAR A SUA INFORMAÇÃO PESSOAL PARA TOMAR DECISÕES AUTOMÁTICAS A SEU RESPEITO?

Uma decisão automatizada é tomada quando a informação pessoal do cliente é analisada para tomar uma decisão sem intervenção humana nesse processo de decisão.

Podemos fazer uso das informações pessoais do cliente para tomar uma decisão automatizada, conforme permitido por lei. Um exemplo de tomada de decisão automatizada é a aprovação ou recusa de um pedido de crédito quando o cliente solicita um descoberto ou cartão de crédito ou a aprovação ou recusa de um pedido de seguro. O cliente tem o direito de consultar quaisquer decisões tomadas e nós forneceremos as razões para as decisões, na medida do razoavelmente possível.

10. QUANDO, COMO E COM QUEM PARTILHAMOS A INFORMAÇÃO PESSOAL DO CLIENTE?

Em geral, só partilharemos informações pessoais do cliente se uma ou mais das seguintes opções se aplicar:

- se tiver o consentimento do cliente;
- se for necessário concluir ou executar sob um contrato que temos com o cliente;
- se a lei assim o exigir; e / ou
- se for necessário proteger ou defender os seus interesses legítimos, nossos ou de terceiros.

Sempre que necessário, o FNBM pode partilhar as suas informações pessoais com as seguintes pessoas. Estas pessoas têm a obrigação de manter as suas informações pessoais seguras e confidenciais:

- FirstRand Bank Limited para qualquer uma das finalidades identificadas nesta Política de Privacidade;
- os nossos Colaboradores, conforme exigido pela natureza das suas funções;
- advogados, agentes de rastreamento, técnicos de cobranças e outras pessoas que auxiliam na execução de contratos;
- fornecedores de serviços de processamento de pagamentos, comerciantes, bancos e outras pessoas que suportam o processamento das suas instruções de pagamento, como fornecedores de pagamentos com cartões (como VISA ou MasterCard);
- seguradoras, correctoras, outras instituições financeiras ou outras organizações que

auxiliam na subscrição de seguros e seguros vida, no fornecimento de seguros e seguros vida, na avaliação de sinistros de seguros e seguros vida e outros fins relacionados;
- agências policiais e de prevenção de fraude e outras pessoas encarregadas da prevenção e repressão de crimes;
- autoridades reguladoras, mediador da indústria, departamentos governamentais, autoridades fiscalism locais e internacionais e outras pessoas que a lei exige a partilha das suas informações pessoais;
- agências de crédito;
- nossos provedores de serviços, agentes e subcontratados, como correios e outras pessoas que usamos para oferecer e fornecer produtos e serviços ao cliente;
- pessoas a quem cedemos os nossos direitos ou delegamos as suas obrigações ao abrigo de acordos, como por exemplo, onde um negócio é vendido;
- tribunais que exigem informações pessoais para julgar referências, acções ou pedidos;
- o público em geral onde o cliente envia conteúdo para as nossas redes sociais, como a nossa página no Facebook;
- fiduciários, executores ou curadores nomeados por um tribunal de justiça;
- prestadores de serviços de verificação de cheques;
- os nosso empreendimento conjunto e outros parceiros com os quais celebramos contratos comerciais.

11. QUANDO E COMO COMPARTILHAMOS A SUA INFORMAÇÃO PESSOAL COM AS AGÊNCIAS DE CRÉDITO

Podemos obter informações pessoais do cliente em agências de crédito por qualquer um ou mais dos seguintes motivos, de acordo com os requisitos da legislação do país:

- caso tenha sido solicitado ou expressamente consentido;
- verificar (comprovar e confirmar) a identidade do cliente;
- obter ou verificar os dados de emprego do cliente;
- obter e verificar o estado civil do cliente;
- obter, verificar ou actualizar o contacto ou detalhes de endereço do cliente;
- obter um relatório de crédito respeitante ao cliente (que inclui o seu histórico de crédito e pontuação de crédito) quando o cliente solicita um contrato de crédito (como um descoberto) para evitar empréstimos imprudentes ou sobreendividamento;
- determinar o risco de crédito do cliente;
- cobrança de créditos;
- rastrear a localização do cliente;
- actualizar os detalhes respeitantes aos contactos do cliente;
- realizar pesquisas, análises estatísticas ou testes de sistemas;
- determinar a fonte de rendimento do cliente;
- criar cartões de pontuação de crédito que são usados para avaliar aplicações de crédito; e / ou
- determinar que produtos e serviços que devem ser promovidos ou oferecidos ao cliente.

Compartilharemos informações pessoais do cliente com as agências de crédito por (entre outros) qualquer um ou mais dos seguintes motivos:

- reportar o pedido de um contrato de crédito;
- reportar a celebração de um contrato de crédito;
- reportar a rescisão de um contrato de crédito;
- reportar o comportamento do pagamento num contrato de crédito; e / ou
- reportar o incumprimento de um contrato de crédito, como o não pagamento integral ou pontual.

Por favor, consulte o seu contrato de crédito específico com o FNBM para o esclarecimento de informações adicionais.

12. EM QUE CIRCUNSTÂNCIAS IREMOS TRANSFERIR A INFORMAÇÃO PESSOAL DO CLIENTE PARA OUTROS PAÍSES?

Partilharemos apenas informações pessoais do clienye a terceiros em outro país apenas em uma ou mais das seguintes circunstâncias:

- se as suas informações pessoais serão adequadamente protegidas ao abrigo das leis do outro país ou por um contrato com o terceiro destinatário;
- se a transferência é necessária para celebrar ou executar sob um contrato com o cliente ou um contrato com um terceiro que seja do interesse do cliente;
- se o cliente tiver concedido a transferência; e / ou
- se não for razoavelmente prático obter o consentimento do cliente, a transferência será do seu interesse.

A transferência será feita de acordo com os requisitos e salvaguardas da lei.

Sempre que possível, a parte que processar informações pessoais do cliente no outro país concordará em aplicar o mesmo nível de protecção disponível por lei em Moçambique ou se as leis do outro país proporcionarem uma melhor protecção, as leis do outro país serão acordadas e aplicadas.

Um exemplo de transferência de informações pessoais do cliente para outro país ocorre quando são efectuados pagamentos respeitantes a aquisição de bens ou serviços num país estrangeiro.

NOTA: Considerando que o FNBM faz parte de uma organização global (FirstRand) as informações pessoais do cliente podem ser compartilhadas ao nível das entidades do FirstRand Limited em outros países e processadas nesses países.

13. DEVERES E DIREITOS SOBRE A INFORMAÇÃO PESSOAL QUE TEMOS SOBRE O CLIENTE

O cliente deve fornecer prova de identidade ao exercer os direitos abaixo.

O cliente deve informar ao FNBM sempre que ocorrer qualquer alteração respeitante as suas informações pessoais.

O cliente tem o direito de solicitar o acesso às informações pessoais detidas pelo FNBM, entrando em contacto com o FNBM. Isto inclui solicitar:

- confirmação que o FNBM detém informações pessoais do cliente;
- uma cópia ou descrição do registo que contém informações pessoais do cliente; e
- a identidade ou categorias de terceiros que tiveram acesso às suas informações pessoais.

Iremos satisfazer a pedidos de acesso a informações pessoais dentro de um prazo razoável. O cliente pode ser obrigado a pagar uma taxa razoável para receber cópias ou descrições de registos, ou informações sobre terceiros. Informaremos ao cliente sobre a taxa antes de satisfazer ao seu pedido.

Por favor note que a lei pode limitar o seu direito de acesso à informação.

O cliente goza do direito de solicitar que sejam efectuadas correcções ou que as informações pessoais que temos sobre o cliente sejam excluídas se forem incorrectas, irrelevantes, excessivas, desactualizadas, incompletas, enganosas, obtidas ilegalmente ou se não tivermos autorização para mantê-las. O cliente deve apresentar uma solicitação por escrito. A alteração pode levar até 15 dias úteis para que seja reflectida nos nossos sistemas. O FNBM deve solicitar os documentos do cliente para verificar a alteração das informações pessoais.

Um contrato específico que o cliente tenha celebrado com o FNBM pode determinar como o cliente deve alterar as suas informações pessoais fornecidas no momento em que celebrou o contrato específico. Por favor, siga estes requisitos. Se a lei exigir que o FNBM mantenha as informações pessoais do cliente, estas não serão apagadas a seu pedido. A destruição de determinadas informações pessoais pode levar à cessação da relação comercial do cliente com o FNBM.

O cliente pode contestar, por motivos razoáveis, o processamento das suas informações pessoais.

Não poderemos dar efeito à objecção do cliente se o processamento das informações pessoais do cliente foi e é permitido por lei; o cliente deu o seu consentimento para o processamento e o nosso processamento é feito de acordo com o consentimento do cliente ou o processamento é necessário para concluir ou executar ao abrigo de um contrato com o cliente.

O cliente deve informar ao FNBM sobre qualquer objecção por escrito.

Caso tenha dado o seu consentimento para o processamento das suas informações pessoais, pode cancelar o seu consentimento. Se o cliente cancelar o seu consentimento, explicaremos as

consequências. Poderemos proceder ao processamento das suas informações pessoais mesmo que tenha cancelado o seu consentimento, se a lei o permitir ou exigir. Pode levar até 15 dias úteis para que a alteração reflicta nos nossos sistemas, durante este tempo podemos igualmente processar as informações pessoais do cliente.

O cliente goza do direito de apresentar uma reclamação junto do FNBM ou com qualquer órgão regulador competente sobre uma suposta violação de protecção das suas informações pessoais. A sua reclamação será resolvida na medida do possível.

14. COMO PROTEGEMOS A INFORMAÇÃO PESSOAL DO CLIENTE?

Tomaremos medidas técnicas e organizacionais apropriadas e razoáveis para proteger as informações pessoais do cliente de acordo com as melhores práticas da indústria. As nossas medidas de segurança (incluindo salvaguardas físicas, tecnológicas e processuais) serão apropriadas e razoáveis. Isto inclui o seguinte:

- manter os nossos sistemas seguros (como monitorar o acesso e o uso);
- armazenar os nossos registos com segurança;
- controlar o acesso aos nossos edifícios, sistemas e/ou registos; e
- destruir ou eliminar registos com segurança.

O cliente pode proteger igualmente as suas informações pessoais. Visite o *website* do negócio relevante com a qual o cliente estabeleceu um relacionamento comercial para obter informações adicionais.

15. POR QUANTO TEMPO ARQUIVAMOS A INFORMAÇÃO PESSOAL DO CLIENTE?

As informações pessoais do cliente serão mantidas pelo tempo que:

- a lei assim assim o exige;
- um contrato entre o cliente e o FNBM exige que o mesmo seja mantido pelo FNBM;
- o cliente tenha consentido o FNBM a manter;
- o FNBM é obrigado a manter para alcançar os propósitos listados nesta Política de Privacidade;
- exigimos para fins estatísticos ou de pesquisa;
- um código de conduta exige que seja mantido pelo FNBM; e / ou
- exigimos para nossos propósitos comerciais legais.

Nota: O FNBM irá manter as suas informações pessoais mesmo que não exista mais uma relação com o FNBM, durante 15 anos a contar da data em que a relação com o cliente finda.

16. NOSSA POLÍTICA DE *COOKIE*

Um *cookie* é um arquivo pequeno de dados enviado através dos nossos *websites* ou aplicativos para o disco rígido do seu computador ou dispositivo ou navegador de Internet onde é salvo. O *cookie* contém informações para personalizar sua experiência nos nossos websites ou aplicativos e pode melhorar a sua experiência nos *websites* ou aplicativos. O cookie identificará igualmente o seu dispositivo, como computadores ou smartphones.

Ao utilizar os nossos *websites* ou aplicativos, o cliente concorda que os *cookies* podem ser encaminhados do *website* ou aplicativo relevante para o seu computador ou dispositivo. O *cookie* permitirá saber que o cliente já visitou o *website* ou aplicativo antes e fará igualmente a identificação. Podemos utilizar o *cookie* para evitar situações de fraude.

17. COMO IREMOS PROCESSAR INFORMAÇÕES SOBRE PESSOAS RELACIONADAS A UMA PESSOA JURÍDICA, OU SEJA, PESSOAS RELACIONADAS?

Se o cliente é uma pessoa jurídica (como uma empresa ou sociedade limitada), podemos recolher e usar informações pessoais respeitantes aos directores, administradores, empregados, beneficiários efectivos, sócios, accionistas, membros, signatários autorizados, representantes, agentes, ordenante, beneficiário, clientes avalistas, cônjuges dos avalistas, fiadores, cônjuges de fiadores, outros provedores de garantia e outras pessoas relacionadas com a pessoa jurídica. Estas são pessoas relacionadas.

Se o cliente fornecer informações pessoais de uma pessoa relacionada, o cliente garante que a pessoa relacionada esteja ciente que o cliente está a compartilhar as suas informações pessoais com o FNB e que a pessoa relacionada consentiu.

Processaremos as informações pessoais de pessoas relacionadas, conforme estabelecido nesta Política de Privacidade, portanto, as referências a "o cliente" ou "seu" nesta Política de Privacidade incluirão pessoas relacionadas com as emendas necessárias.

18. INFORMAÇÕES QUE PODEMOS PARTILHAR COM OUTROS BANCOS OU PEDIDOS DE OUTROS BANCOS

- Qualquer outro banco pode solicitar ao FNBM (a pedido do cliente desse banco ou do próprio banco) informações factuais sobre a posição financeira do cliente. Isso é feito emitindo o que é conhecido como código de um banqueiro.
- Essas referências e códigos bancários são normalmente solicitados quando se deseja estabelecer uma relação com o outro banco ou quando se está a solicitar uma conta comercial com um cliente de outro banco.

- São informações factuais sobre a posição financeira do cliente baseadas na forma como o cliente geriu a sua conta transaccional com o FNBM. As informações factuais são fornecidas na forma de referência e código de um banqueiro.
- As referências e códigos do banqueiro só serão fornecidos com o consentimento expresso, implícito ou tácito do cliente.

FNB EMPLOYEE PRIVACY NOTICE

DOCUMENT CONTROL

POLICY LEVEL:	FNBM
EFFECTIVE DATE:	31st March 2021
NUMBER OF PAGES:	9
DATE	15th February 2021
APPROVED BY:	Head of Department and noted at EXCO
Document Owner	Name: Melba Jorge Designation: Head of Human Resources Physical Address: 420, 25 de Setembro, JATI, 1st Floor Tel: +258 21 35 5905 e-mail: Melba.jorge@fnb.co.mz
VERSION NUMBER:	1.0

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE

Protecting the privacy of personal information of its employees is very important to FNB Moçambique S.A. (FNB). To do so, FNB follows general principles in accordance with applicable privacy laws and, particularly, the African Union Convention for Data Privacy and Cybersecurity (Convention).

FNB has developed the following FNB employee privacy notice (notice) to help employees understand how FNB collects, uses and safeguards their personal information.

FNB's notice includes general information regarding FNB's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FNB's notice incorporates by reference FNB's acceptable use of information resources policy.

2. SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employee (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by the FNB.

3. DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION.

FNB will process personal information collected from employees.

3.1 Responsible party

FNB MOÇAMBIQUE, S.A. (FNB), a joint stock company, with headquarter at September 25 Avenue, no. 420, JAT Building I, 1st floor, Room 8, in Maputo City, registered at legal Entities Register under the number 12,540, sheets 162, of Book C-30, holder of the Tax Identification Number 400076391, This company is the responsible party.

3.2 Definition of employees' personal information

For the purpose of this notice, and other documents referred to in this notice, personal information means information about an identifiable, living, natural person.

By way of example, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

Personal information does not include aggregated or anonymised information where FNB is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee, which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only. For instance, "20% of FNB's employees own or use a laptop computer" is not personal information.

Personal information, processed by FNB, regarding FNB employees (**personal information**) includes the following types of information:

- personal details, including but not limited to, name, address, location information, online identifier, emergency contact details, birth certificate number, employee number or identity number, educational and other qualifications, and curriculum vitae;
- job-related details, e.g. start date, place of work, salary, benefits, absence records;
- financial information, e.g. bank account number;
- performance/evaluation information, e.g. whether an employee performs their job duties in accordance with the relevant requirements.

An employee undertakes to communicate his/her personal information to FNB when specifically requested by FNB to do so.

3.3 Definition of employees' special personal information

There are special categories of an employee's personal information, which FNB will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (**special personal information**).

FNB processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with FNB's obligations under the applicable laws and regulations.

FNB will not retain or process special personal information unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric personal information may be requested by FNB.

3.4 Purposes for the processing of personal information

Personal information will be processed by FNB in the normal course of business of managing employees for various purposes:

- For required banking information in order to process an employee's remuneration.
- To suggest the opening of a bank account on behalf of the employee, in order to secure staff rates.

- To admit the employee to the Social Insurance.
- To comply with the FNB's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, or prospective employee. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.
- To comply with all applicable laws authorising or requiring such processing.
- To carry out the specific obligations and duties of FNB in the field of employment legislation.
- To realise objectives laid down by, or by virtue of, tax or other applicable legislation.
- To properly assess performance under an employment contract.
- To undertake management activities, such as succession planning, talent management, training, work planning, task management, assessment of employee performance, and to control security and access to facilities.
- To market products, goods and services to the employee, the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of employee-specific product offerings; and/or otherwise securing and facilitating the employee's employment with the FNB, including rendering to the employee value added services (such as employee wellbeing initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.
- To share spouse/children personal information for business purposes, e.g. for business travel purposes, events, etc.
- To share children details, e.g. beneficiary of pension on the death of a parent.
- To share close relatives' details – next of kin/emergency contact persons.
- To compile statistics and results from research studies and related programs.
- To process in order to send work-related communications to the employee's mobile device via any of the group's platforms including the RMB, FNB and WesBank apps.
- The purposes above are mandatory for employees to provide their personal information to enable the processing of:
- the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract, or
- compliance with legal obligations to which FNB is subject, or
- the protection of a legitimate interest of the employee; or
- the legitimate interests pursued by FNB, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- for a prospective employee: to FNB being unable to enter into an employment contract with that prospective employee, and

- for an employee: to FNB being unable to provide services and/or privileges to the employee and his dependents, not fulfil orders/instructions by his demand or interest or, in extreme cases, such refusal may lead to terminate the contract if the extent of such refusal become materially adverse the maintenance of the relationship.

There may be instances where FNB will lawfully process personal information for purposes not listed above.

Where the provision of personal information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5 Quality of personal information

FNB will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate and not misleading, and is updated where necessary.

The FNB's human capital functions have provided the self-service channels, through which employees are required to update personal information if it changes. The onus is on the employee to utilise this channel to update his/her personal information, when necessary.

For updates to personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6 Security and confidentiality of personal information

All personal information processed by FNB will be held confidentially.

FNB will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7 Retention of personal information

Personal information will not be kept by FNB for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNB reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FNB.

Other than in the instances, FNB may request the employee's consent for the further retention of personal information and will state the reasons for making such a request.

3.8 The transfer of personal information

Employees' personal information may be shared by FNB with third parties with whom FNB contracts to process such personal information and pursuant to the instruction of FNB, under specific terms or terms as set forth in this notice for the purposes mentioned above.

Provided that FNB ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FNB and in accordance with this notice, FNB may transfer personal information within the group, operators (see 0 below) or other third parties based outside Mozambique with whom FNB has a lawful justification, e.g. a signed a contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by FNB, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of personal information.

3.9 Use of operators

An operator is a person who processes personal information on behalf of FNB in terms of a contract or mandate, without coming under the direct authority of FNB.

FNB may assign the processing of FNB employee personal information to an operator which will process the personal information only with the knowledge or authorisation of FNB.

FNB will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by FNB.

3.10 Employees' privacy rights

3.10.1 Access to information

The employee has the right to access the personal information which relates to him/her. Where an employee wishes to request personal information, which they do not have a direct right to, but which information is needed to protect a right of the employees, a request must be addressed judicial courts.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to him/her. The employee can update, and correct certain types of personal information stored on the human capital platform using the self-service channel. For instructions on how to do so, the employee should contact the responsible person in their human capital department.

For updating other types of personal information, the employee should address a simple request to that effect to the responsible human capital department. Should FNB be unable to correct the personal information, FNB must explain its position in writing to the employee.

Should FNB refuse the correction, the employee is entitled to request that a statement be attached to the personal information, which indicates that a correction has been sought and not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information, which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
- legally prohibited from being recorded, communicated or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to the responsible human capital department.

FNB must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should FNB refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information, which indicates that a request for removal of personal information has been sought and not made.

3.10.4 Right to complain

Employees have the right to submit a complaint to the Data Privacy National Authority or other competent authority regarding an alleged breach of the conditions for lawful processing of personal information as set out in Convention and other applicable laws and regulation.

An employee can choose to submit complaints to FNB for resolution before submission to the Data Privacy National Authority. Any queries or complaints regarding the employee's personal information can be directed to the respective human capital manager within the FNB.

3.11 Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice and for access to information about his or her personal information processed within the context of this notice, (e.g. employee discloses his HIV status to his line manager, who then communicates this to the entire office) the employee may contact their data privacy officer, line manager or their human capital department.

FNB must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12 Reference to other FNB policies

- FNB acceptable use of information resources policy:

  The FNB acceptable use of information resources policy aims to ensure effective, efficient and secure use of FNB's information resources and informs employees of what is deemed acceptable and unacceptable practice. Subject to the terms of this notice, FNB will monitor the use of its information resources by employees. This notice also contains requirements and guidelines for dealing with the personal information of clients.
- FNB internal privacy policy.
- FNB privacy framework.

-END-

FNB MOÇAMBIQUE, SA SUPPLIER PRIVACY NOTICE

DOCUMENT CONTROL

POLICY LEVEL:	FNBM
EFFECTIVE DATE:	30th March 2021
NUMBER OF PAGES:	8
DATE	15th February 2021
APPROVED BY:	Head of Department and noted at EXCO
Document Owner	Name: Jacinto Delgado Designation: Chief Financial Officer Physical Address: 420, 25 de Setembro, JATI, 1st Floor Tel: +258 21 35 5905 e-mail: Jacinto.Delgado@fnb.co.mz
VERSION NUMBER:	1.0

FNBM SUPPLIER NOTICE

Contents

1. DEFINITION OF CERTAIN TERMS USED IN THIS NOTICE

Affiliate	Means (a) any subsidiary or a holding company or a subsidiary of the holding company of either party, or (b) any entity that controls, is controlled by, or is under common control with, either party. The terms "subsidiary" and "holding company" will have the meaning assigned thereto in Article 2 Law 15/99, of 1 November amended by Law 9/2004, of 21 July. The term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty percent) plus 1 (one) of the possible votes.
Associate	Means any entity or unincorporated joint venture in which FNBM has the right to receive at least 20% (twenty percent) of the profit share or similar benefit derived from such entity or unincorporated joint venture.
Automated	Means any equipment capable of operating automatically (without human intervention) in response to instructions given for the purpose of processing information.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
FirstRand or **the group**	Means FirstRand Limited and its South African subsidiaries (as defined in the Companies Act, 2018) including divisions, segments and business units, but specifically excluding subsidiaries, where such entity is a subsidiary as a result of an investment by any one of RMB's private equity businesses, (predominantly legally structured under FirstRand Investment Holdings (Pty) Ltd (FRIHL).
Operators	Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
Processing	Means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in

	any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Responsible party	Defined in the Electronic Transaction Law no 3/2017, of 9 January as a public or private body or other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

2. BACKGROUND AND PURPOSE OF THIS NOTICE

Protecting the personal information of the FNBM's suppliers is important to FNBM**.** To do so, FNBM follows general principles in accordance with applicable privacy laws and African Union Convention for Data Protection and Cyber Security in particular.

FNBM has developed a FNBM supplier privacy notice (**notice**) to enable its suppliers to understand how the FNBM collects, uses and safeguards their personal information.

3. RESPONSIBLE PARTY

FNBM with headquarter at September 25 Avenue, no. 420, JAT Building I, 1st floor, Room 8, in Maputo City, registered at legal Entities Register under the number 12,540, sheets 162, of Book C-30, holder of the Tax Identification Number 400076391. This company is the responsible party.

A supplier in the context of the notice means a natural or juristic person that provides a product or renders services to FNBM and is a data subject with relevant personal information relating to it.

4. PERSONAL INFORMATION PERTAINING TO SUPPLIERS

Personal information refers to any information relating to the supplier and which identifies the supplier (who can be a natural or a juristic person). If a supplier is a juristic person, the FNBM may collect and use personal information relating to the juristic person's directors, officers, employees, beneficial owners, partners, shareholders, members, authorised signatories, representatives, agents, payers, payees, customers, guarantors, spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person. These are related persons.

If the supplier provides the personal information of a related person to FNBM, the supplier warrants that the related person is aware that the supplier is sharing their personal information with FNBM and that the related person has consented thereto. FNBM will process the personal information of related persons as stated in this notice, thus references to "the supplier" in this notice will include related persons with the necessary amendments.

Examples of the supplier's personal information (natural or juristic person) could include, but is not limited to:

- the supplier's financial information, which includes banking account information and financial records including bank statements provided to the FNBM;
- invoices issued by the supplier to the FNBM;
- the contract/agreement with FNBM;
- other identifying information of the supplier, which includes company registration number, tax number and contact details;
- marital status and matrimonial property regime (e.g. married in community of property);
- national origin;
- age;
- language;
- education;
- financial history;
- identifying number (e.g. an account number, identity number or passport number);
- email address;
- physical address (e.g. residential address, work address or physical location);
- telephone number;
- online identifiers;
- social media profiles;
- biometric information (like fingerprints, signature or voice);
- race;
- gender;
- criminal history;
- personal views, preferences and opinions; and/or
- confidential correspondence.

Some of the personal information elements, are considered special personal information, specifically as explained below.

Special personal information is personal information about the following:

- criminal behaviour, to the extent that such information relates to the alleged commission of an offence (to prevent money laundering as required by law, or when entering into a business relationship with FNBM),

or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

5. THE PURPOSES IN REFERENCE TO PROCESSING OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS

Personal information will be processed by FNBM in the normal course of the management of suppliers for various purposes. Such purposes include, but are not limited to:

- To procure products, goods and services from the supplier.
- To respond to enquiries and complaints from the supplier.
- To maintain the supplier's data.
- To comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules), voluntary and involuntary codes of conduct and industry agreements or to fulfil reporting requirements and information requests.
- To detect, prevent and report theft, fraud, money laundering and other crimes. This will include conducting criminal, credit reference/bureaux, sanctions, anti-bribery and other related reference checks on the supplier to the extent provided by applicable laws and regulations. Such checks may be conducted on an ongoing basis throughout the period of engagement and may include lifestyle audits as well as reporting on the conduct of suppliers where required to do so by law to the relevant bodies after termination of the underlying agreement;
- To comply with all applicable laws authorising or requiring such processing;
- To process special personal information, like alleged criminal behaviour or the supply of false, misleading or dishonest information.
- To enforce and/or collect on any agreement when the supplier is in default or breach of the agreement terms and conditions, like tracing the supplier or to institute legal proceedings against the supplier.
- To conduct market and behavioural research, including scoring and analysis.
- For historical, statistical and research purposes, like market segmentation or performance management.
- For security, identity verification and to check the accuracy of the supplier's personal information.
- For performing vendor risk management processes;
- To communicate with the supplier and carry out the supplier's instructions and requests;
- To enable the supplier's participation in supplier development programmes, including training and evaluation to access resources like funding and banking.
- For any other related purposes.

The provision of personal information by suppliers is mandatory to enable:

- the performance of the contract to which the supplier is party or in order to take steps at the request of the prospective supplier prior to entering into the contract, such as the signing of a non-disclosure agreement whilst busy with negotiations;
- compliance with legal obligations to which the FNBM is subject;
- the protection of a legitimate interest of the supplier; or
- the legitimate interests pursued by the FNBM, or by the third party to whom the personal information is disclosed for one or more of the above purposes.

There may be instances where FNBM will lawfully process personal information for purposes not listed above. Where the provision of personal information is voluntary in such instances, a consent from the supplier (which consent may at any moment be withdrawn) will be sought where the law requires.

6. THE CONSEQUENCES RELATING TO SUPPLIERS WHO DO NOT PROVIDE THEIR PERSONAL INFORMATION TO FNBM

A supplier undertakes to provide their personal information to the FNBM when specifically requested to do so. If a supplier should not want to do so and the personal information is needed to enter into a contract or business relationship, then FNBM will be unable to enter into a contract or pursue any contractual relationship with the supplier.

7. THE QUALITY OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS

FNBM will take reasonable and practicable steps to ensure that the personal information of the FNBM's suppliers is complete, accurate and not misleading, and is updated where necessary.

Suppliers can update their personal information, once given, by forwarding such a request to the responsible supplier contact within the FNBM, or by directing such a request FNBM's procurement mailbox. The contact person will be the individual the supplier is working/dealing with the FNBM. The contact for the procurement mailbox (procurement@FNBM.co.mz).

8. SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS

All personal information of the supplier processed by FNBM will be held confidentially.

FNBM will take reasonable, appropriate technical and organisational measures to keep the supplier's personal information secure in accordance with the FNBM's policies and procedures on information security, and in accordance with any applicable legislation.

9. RETENTION OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS

Personal information will not be kept by FNBM for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNBM reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by the contract between the supplier and FNBM.

Other than in the aforementioned instances, FNBM may request the supplier's consent for the further retention of their personal information and will state the reasons for making such a request.

10. THE SHARING OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS

The supplier's personal information may be shared within the FirstRand group and with affiliates and third parties with whom FNBM contracts to process such personal information and pursuant to the instruction of FNBM, under specific terms or purposes as set forth in this notice. A simplified legal entity structure for the FirstRand group can be found at https://www.firstrand.co.za/the-group/ownership-and-legal-structure/. Moreover, certain affiliates and third parties could be based outside of Moçambique. In such instances, FNBM will comply with cross-border transfer conditions of personal information as set out in Convention.

FNBM will ensure that reasonable and adequate safeguards are in place when sharing the supplier's personal information as set out above.

11. THE USE OF OPERATORS TO PROCESS PERSONAL INFORMATION PERTAINING TO SUPPLIERS

FNBM may assign the processing of the supplier's personal information to an operator who will process such personal information on the basis of a contract entered into with FNBM. The terms of such a contract FNBM will ensure that the operator processes the supplier's personal information on a confidential basis and to apply reasonable and adequate security standards when processing the supplier's personal information.

12. PRIVACY RIGHTS OF SUPPLIERS

Privacy rights	Description and information to exercise such rights
The right to be informed	The notice has been developed to enable suppliers to understand how FNBM collects, uses and safeguards their personal information.
The right to access to information	The supplier has the right to access their personal information. The supplier may follow various avenues to access personal information. The supplier may make use of the following process via the FNBM's procurement mailbox (procurement@FNBM.co.mz) The supplier may also address a request in accordance with the procedure established for this purpose.
The right to the correction, destruction, deletion and objections to the processing of the Suppliers personal information	Such requests can be forwarded to the responsible relationship manager in FNBM. The responsible relationship manager will advise on the form and manner to submit and action such requests. The supplier could also update personal information through the supplier mailbox at (procurement@FNBM.co.mz)
The right to object to direct marketing	If the supplier's personal information has been used for direct marketing purposes, FNBM will afford the supplier (and the individuals or representatives or related parties of the supplier) an opportunity to opt out from receiving such direct marketing.
The right to submit a complaint to the FNBM and to the competent authority	Suppliers have the right to submit a complaint to the information regulator regarding an alleged breach of the conditions for lawful processing of personal information as set out in Convention. The supplier can choose to submit complaints to FNBM for resolution before submission to the competent authority. Any queries or complaints regarding the suppliers personal information can be directed to the responsible relationship manager within FNBM.

13. RESPONSIBILITIES OF SUPPLIERS UNDER CONVENTION

When a supplier processes personal information for responsible party in terms of a contract or mandate, the supplier will be required to adhere to the obligations set out in FNBM's data protection policy for suppliers. This policy sets out the rules of engagement in relation to how personal information is processed by suppliers on behalf of FNBM as well as the minimum legal requirements that FNBM requires the suppliers to adhere to, including compliance to Convention and the General Data Privacy Regulation where this regulation does not conflict to in-country laws and regulations, and other legislation where applicable, from time to time, in their capacity as service providers to FNBM. This policy is applicable to all suppliers that engage with FNBM and handle personal information as defined in applicable law.

14. DOCUMENT INFORMATION

Any changes and / or amendments to the notice will come into force and effect once the updated notice has been published on the relevant supplier electronic channels and a notice regarding the publication of the updated notice has been dispatched to the supplier or the supplier's authorised representative(s).

-END-

POLÍTICA DE PRIVACIDADE DO FNB MOÇAMBIQUE, SA.

AVISO DE COOKIE DO FNBM

AVISO DE COOKIE DO FNBM

DOCUMENTO DE CONTROLO

Título	Aviso de Cookie do FNBM		
Autor	Sansão Monjane		
Versão do Documento	1.0		
Data da Versão	Fevereiro de 2021		
Aprovação	Comité para Aprovação:	Data de Aprovação:	Versão para Aprovação:
	Comité de Privacidade e Protecção de Dados		
Data da próxima revisão			

CONTEÚDO:

AVISO DE COOKIE DO FNBM

1. O QUE É UM COOKIE?

Um cookie é uma pequena unidade de dados que é enviada de um website para o dispositivo do utilizador, tal como um computador, um tablet, etc. (geralmente sob a forma de um ficheiro de texto). O objectivo de um cookie é fornecer um mecanismo fiável para "lembrar" informações de estado (mantendo um registo das acções anteriores). Um exemplo seria recordar o conteúdo de um carrinho de compras online, e as acções que o utilizador realizou enquanto navegava sem se inscrever ou entrar na sua conta online.

Não sabemos necessariamente quem é o utilizador do dispositivo, mas sim o comportamento desempenhado a partir de um dispositivo. Vários utilizadores do mesmo dispositivo não seriam necessariamente distinguíveis uns dos outros. No entanto, os cookies poderiam ser utilizados para identificar o dispositivo e se o dispositivo estiver ligado a um utilizador específico, o utilizador também seria identificável.

2. QUE TIPO DE COOKIES PODE-SE ENCONTRAR NO WEBSITE DO FNBM?

Os cookies primários são utilizados no website do FNBM (FNB Moçambique). Os cookies são definidos pelo website do FNBM .

Os cookies primários são directamente armazenados no website do FNBM. Estes cookies permitem ao website do FNBM recolher análises, dados, memorizar configurações linguísticas, ou executar outras funções úteis que proporcionam uma boa experiência ao utilizador .

Durante a visita do cliente ao website do FNBM, podemos utilizar o seguinte cookie listado na tabela abaixo. A tabela ajuda a explicar as funções do cookie e o período em que o cookie pode permanecer activo .

Origem	Uso	O Serviço	Duração
Cookie Primário	Identificação do Navegador/Dispositivo	Isto permite ao website do FNBM identificar o dispositivo/navegador.	Persiste para além de uma única sessão.
	Autenticação	Ao entrar num servidor web, será restituído um cookie que identifica o utilizador que entrou no sistema com sucesso.	Válido apenas para uma sessão única.

Quando os cookies só são válidos para uma sessão única, o cookie será apagado quando o cliente fechar o seu navegador. Quando os cookies se mantiverem, o cookie será armazenado na página web do cliente até que seja apagado pelo cliente.

3. EM QUE MOMENTO DEVE-SE FAZER USO DOS COOKIES?

O FNBM só irá processar cookies que identifiquem o cliente para fins lícitos :

- Se o cliente tiver consentido;
- Se uma pessoa legalmente autorizada pelo cliente, pela lei ou por um tribunal, tiver consentido em seu nome;
- Se for necessário concluir ou executar sob contrato, que o FNBM mantém com o cliente;
- Se a lei assim o exigir ou permitir;
- Se for necessário para proteger ou defender o cliente, o interesse legítimo do FNBM ou de terceiros (de benefício para...por exemplo, prevenção em matéria de fraude); ou
- Se o cliente for menor e uma pessoa competente (como um dos pais ou tutor) tiver consentido em nome da criança .

Podemos utilizar cookies devido (incluindo, mas não se limitando a) às seguintes razões:

- Fraude, crime financeiro e outras formas de prevenção, detecção e denúncia de crimes;
- Gerir e melhorar a segurança (por exemplo para evitar a utilização fraudulenta dos dados de *login*) para o FNBM e o cliente ;
- Várias razões analíticas como a forma como os utilizadores utilizam o website do FNBM para que possamos introduzir melhorias;
- Marketing e publicidade, por exemplo para decidir que soluções (bens, produtos, serviços ou benefícios) lhe podem interessar e para personalizar o marketing em várias aplicações e websites; e / ou
- Reconhecimento dos utilizadores do website ou dispositivos do FNBM que regressam ao website do FNBM.

4. O QUE DEVERÁ ACONTECER SE O UTILIZADORNÃO QUISER FAZER USO DOS COOKIES?

Todos os navegadores permitem ao cliente recusar a aceitação de cookies e remover os cookies actuais. Os métodos a seguir variam de navegador para navegador, e de versão para versão. O cliente pode bloquear os cookies no website do FNBM, se desejar. O bloqueio de certos cookies pode ter um impacto negativo sobre a usabilidade do website do FNBM. Por exemplo, exigimos cookies para permitir que o cliente faça login e, ao remover os cookies originais, a sua experiência bancária pode ser afectada.

5. INFORMAÇÃO ADICIONAL SOBRE COOKIES

- O navegador do cliente memoriza o cookie e o website fica sem acesso a quaisquer dados no seu dispositivo.
- Uma vez que os cookies são armazenados em ficheiros de texto, não podem ser utilizados para distribuir vírus para o dispositivo.

AVISO DE COOKIE DO FNBM

- Num único dispositivo com vários utilizadores; a experiência do website do FNBM seria personalizada com base no comportamento de todos os utilizadores que utilizam o dispositivo e não apenas de um utilizador individual.
- Se o cliente desactivar os cookies, não irá apagar os cookies anteriormente recolhidos, mas irá interromper a criação de novos cookies, os cookies expirados serão removidos automaticamente.

-FIM-