



FirstRand

COMPLIANCE MANUAL

25 June 2022

DOCUMENT CONTROL

Title	Compliance manual
Author	FirstRand Chief Compliance Officer
Document version	Version 6
Version date	25 June 2022
Committee Approval	FirstRand compliance risk committee
Date of next review	9 July 2023

Contents

1	INTRODUCTION	3
	Definitions:	4
	Compliance:	4
	Compliance risk	Error! Bookmark not defined.
	Conduct risk	4
2	STRATEGIC FRAMEWORK, RISK APPETITE AND RISK BASED APPROACH	5
2.1	Compliance Risk Appetite	5
2.2	Compliance Strategy	5
2.3	The Management of Compliance Risk	6
2.4	Group Compliance Structure and Engagement Model	7
2.5	Specialist Centres of Excellence (COEs)	9
2.6	Operating Business, Segment and Pillar Compliance Structure	12
3	GOVERNANCE AND OVERSIGHT	12
3.1	Introduction	12
3.2	Compliance Risk Committee (CRC)	13
3.3	Segment Compliance Governance Committees	14
3.4	Compliance Executive Committee (Compliance EXCO)	15
4	POLICIES, STANDARDS AND ADVISORY SERVICE	16
4.1	Introduction	16
4.2	Policy Implementation and Roles and responsibilities	16
4.3	Waiver with regard to set compliance policy requirements	17
4.4	Risk Based Decisions	18
4.5	BCBS 239 for Compliance Risk	18
5	ASSESSMENT, EVALUATION, MONITORING AND TESTING	19
6	REPORTING, DATA, MEASUREMENT, ESCALATION AND RESOLUTION	20
6.1.1	Compliance materiality reporting	20

COMPLIANCE MANUAL continued

6.1.2	Compliance themes	22
7	TRAINING, AWARENESS AND COMMUNICATION	24
7.1	Roles and Responsibilities	24
7.2	General awareness training	24
7.3	Compliance officers training	25
7.3.1	Compliance Essentials	25
7.3.2	Compliance Institute of Southern Africa (CISA)	25
8	REGULATOR/INDUSTRY (STAKEHOLDER) INTERACTION AND COORDINATION	26
9	FOSTERING AN ETHICAL/COMPLIANCE CULTURE	27
10	ANNEXURES & ABBREVIATIONS	28
11	ABBREVIATIONS:	29

1 INTRODUCTION

This compliance manual is to be read in conjunction with the FirstRand compliance risk management framework (**Annexure 1**). The compliance framework sets out the principles for the effective management of the group's compliance obligations and compliance risks. These principles specifically focus on what must be implemented, while the practical details around how it should be implemented are set out herein.

The need for a compliance manual arises primarily from the requirements of the Regulations relating to Banks¹, the relevant regulation which read as follows:

“(3) (p) shall compile and maintain a compliance manual that -

- (i) duly addresses all material risks to which the bank is exposed;
- (ii) duly addresses all material objectives and aspects of applicable legislation;
- (iii) refers to specific legislation, rules and regulations when appropriate;
- (iv) is readily available to all relevant staff;
- (v) is reviewed and updated at least once a year.”

In addition, the objectives of a compliance function are generally to²:

1. Assist executive and line management in discharging their responsibility to comply with applicable regulatory requirements, through the provision of compliance risk management services.
2. Enable FirstRand to demonstrate to its regulators that it is fit and proper to undertake its business.
3. Facilitate the management of compliance risk.
4. Minimise enforcement action by regulators.
5. Minimise the possibility of criminal and/or civil action against FirstRand.

The responsibilities of each of the group's compliance functions should be carried out under a compliance programme that sets out its strategy, structure (operating model), planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessments, compliance monitoring and testing, and educating employees on compliance matters. Within FirstRand in order to ensure a better understanding by all compliance employees, role players and stakeholders of what is practically required of them in terms of achieving these objectives, the compliance methodology and how they can achieve it, the compliance manual sets out how all the compliance responsibilities within the group should

¹ Regulation 49(4) q of the Regulations relating to Banks

For an up to date version of the Banks Act (Act no. 94 of 1990) and the Regulations relating to Banks (specifically the full text of sections and regulations that make reference to Compliance: Regulations 39, 47, 49 and 50; Section 60A and B, the South African Reserve Bank website can be accessed at <http://www.resbank.co.za/> under Publications and Notices. Other legislation may also refer to the requirement for a Compliance manual i.e., Prudential Standards under the Insurance Act.

² Taken from the Generally Accepted Compliance Practice (GACP) issued by the Compliance Institute of SA (CISA)

be carried out under a standardised compliance programme consisting of seven key elements. The seven key elements, which the overall compliance programme must address are:

COMPLIANCE PROGRAMME ELEMENT	ACTIVITY
Strategic framework, risk appetite and risk-based approach	Coordinate and definition of the compliance risk appetite and risk-based approach
Policies, standards and advisory	Produce minimum policies and operating standards and ensure review and communication of policies and standards. Ensure proper advice on new products and business lines.
Governance and oversight	Coordination of FirstRand compliance governance committees and analysis and challenge of any MI against legislative requirements, internal standards and policies
Assessment, evaluation, monitoring and testing	Assurance, evaluation and assessment of compliance risk management processes, frameworks, policies and activities
Training, awareness and communication	Compliance community learning and development aligned to defined competency framework and general staff awareness and training.
Stakeholder (regulatory/industry) interaction and coordination	Coordination and gateway for strategic regulatory correspondence and engagement with regulators (PA, SARB, FIC, NCR, FSCA, Information Regulator etc.)
Reporting, data, measurement, escalation and resolution	Assessment and reporting of material compliance risks as required by Regulation 49 and robust governance frameworks.

The principles of each element and high level “what must be done” under the compliance programme are explained in more detail in the body of the manual, with each section covering a key element and then supported by more detailed procedures contained in annexures (highlighted under section 9 below).

Definitions:

Compliance risk

Compliance risk refers to the risk of not adhering to compliance obligations. For this purpose, although not exhaustive, compliance obligations refer to all applicable compliance obligations, including FirstRand Limited (FirstRand or the group) adherence to applicable laws, regulations, regulatory requirements/expectations, directives, guidelines and other applicable specifications such as codes of conduct relevant to specific businesses.

Conduct risk

Conduct risk must be viewed in its widest sense and includes risks associated with delivery of fair customer outcomes and the integrity and efficiency of financial markets and touches every part of how juristic persons, inclusive of financial institutions, conduct their respective business affairs. From a compliance perspective, conduct risk also refers to the risk of

non-compliance with conduct standards and related requirements, as may be prescribed and/or expected from time to time, by regulatory and other related authorities.

2 STRATEGIC FRAMEWORK, RISK APPETITE AND RISK-BASED APPROACH

FirstRand fosters a compliance culture striving to observe both the purpose and the letter of the law as an integral part of its business activities. Deliberate or wilful acts of non-compliance will not be tolerated. The group seeks to achieve full compliance with applicable laws, regulations and supervisory requirements. In cases where there is legal uncertainty, a proper assessment of the facts, compliance obligations and related risks must be undertaken and where appropriate, external legal and/or regulatory opinions should be obtained.

The compliance strategy emphasizes using four main levers - process; people; analytics and technology to enable implementation of the seven key compliance programmatic elements.

2.1 Compliance risk appetite

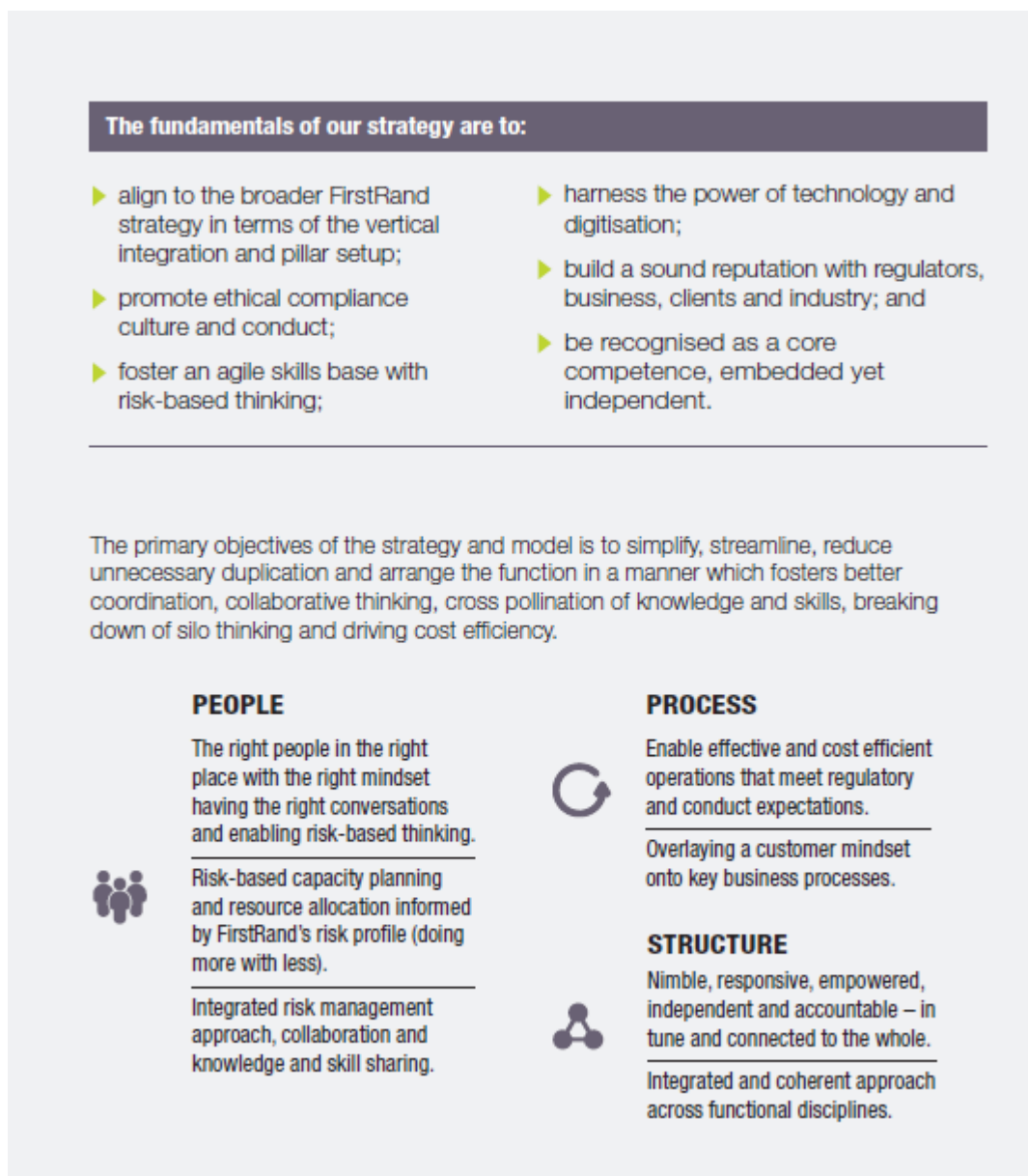
The group compliance risk appetite espouses that the group seeks to prevent its platforms from being abused for the purposes of financial crime, will not accept wilful and deliberate non-compliance, and seeks to achieve full compliance with the letter and purpose of applicable legislation and regulation. There may, however, be instances of unintended failures which result in non-compliance remedial action to be taken on a prioritised basis to address those instances which fall outside the defined tolerances as approved by appropriate governance structures of the group.³ Reference should be made to section 3 of the FirstRand compliance framework for a full description of the FirstRand board compliance risk appetite statement.

2.2 Compliance strategy

The FirstRand compliance function adopts a strategic vision of being recognised for leading compliance capability in order to enable business value, promote a sustainable compliance environment and culture, whilst achieving regulatory and stakeholder expectations. The fundamentals of this strategy are to align to the broader FirstRand strategy in terms of the vertical integration and pillar setup; promote ethical compliance culture and conduct; foster an agile skills base with risk based thinking; harness the power of technology and digitisation; build a sound reputation with regulators, business, clients and industry; and be recognised as a core competence, embedded yet independent.

The primary objectives of the strategy and model is to simplify, streamline, reduce unnecessary duplication and arrange the function in a manner which fosters better coordination, collaborative thinking, cross pollination of knowledge and skills, breaking down of silo thinking and driving cost efficiency.

³ The risk appetite statement does not advocate condonation for instances of identified non-compliance but rather espouses a risk-based approach that remediates all instances of non-compliance identified but on a prioritised basis aligned to defined tolerance levels.



2.3 The management of compliance risk

The management of compliance risk refers to all processes that are established to ensure, that in particular, all material compliance risks and associated risk concentrations are identified, measured, prevented/limited, controlled, mitigated and reported on a timely and comprehensive basis. A culture of ethics and integrity is core and is founded on a values led approach with compliance as an outcome.

The compliance community exists, therefore, to:

- Be the custodians of and influence sound compliance practices and culture
- Deliver compliance business solutions that meet regulatory requirements
- Anticipate and enable the understanding and activities of compliance
- Build a sound reputation with regulators, business, clients, industry
- Be recognised as a core competence, embedded yet independent

COMPLIANCE MANUAL continued

- Understand the regulatory universe; minimise regulatory sanction
- Operate consistently as a co-responsible community of compliance professionals
- Organise, operate, and deliver relevant compliance business solutions
- Optimise the effectiveness, efficiency and demonstrable application of compliance activities
- Deliver reliable assurance to key stakeholders regarding compliance within defined risk appetite

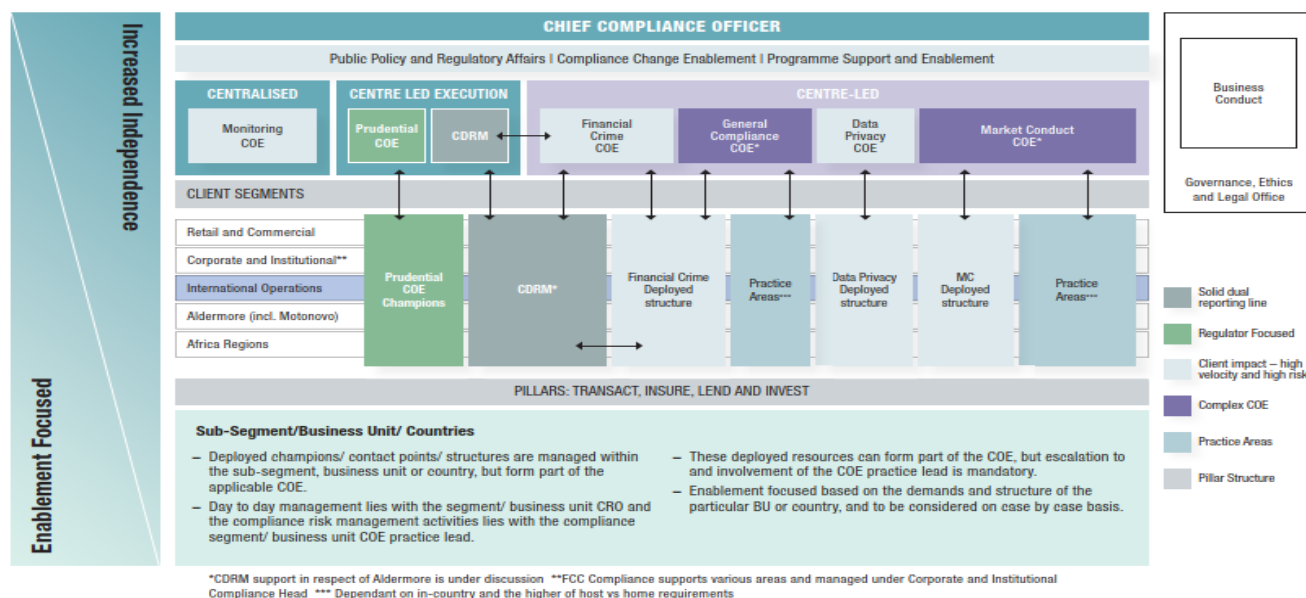
In order to promote independent management of compliance risk, the FirstRand Chief Compliance Officer has senior executive status within FirstRand, does not have direct business line responsibilities and reports directly to the FirstRand COO; board of directors; risk, capital management and compliance (RCCC) and audit committees; the compliance risk committee (CRC) (subcommittee of FirstRand RCC committee). The centralised compliance (Group Compliance) function provides specialist support and oversight of the compliance functions across all operating businesses, segments and pillars.

The segment heads of compliance and pillar heads of compliance have dual reporting lines and report both to their segment (or pillar where applicable) chief risk officers or segment CEO and to the FirstRand Chief Compliance Officer on matters of compliance risk⁴. Operating business compliance functions operate within this segment and/or pillar construct.

2.4 Group Compliance structure and engagement model

FirstRand's compliance structure is vast and collectively comprises of several teams across the group. This hybrid compliance structure consists of a centralised independent compliance function headed by the FirstRand Chief Compliance Officer, together with deployed compliance functions, led by heads of compliance within each of the operating businesses and segments and supported by compliance coverage in each of the pillars (currently transact, lend, insure and invest).

FirstRand Compliance – Operating Model



The compliance target operating model is based on the following design and architectural principles:

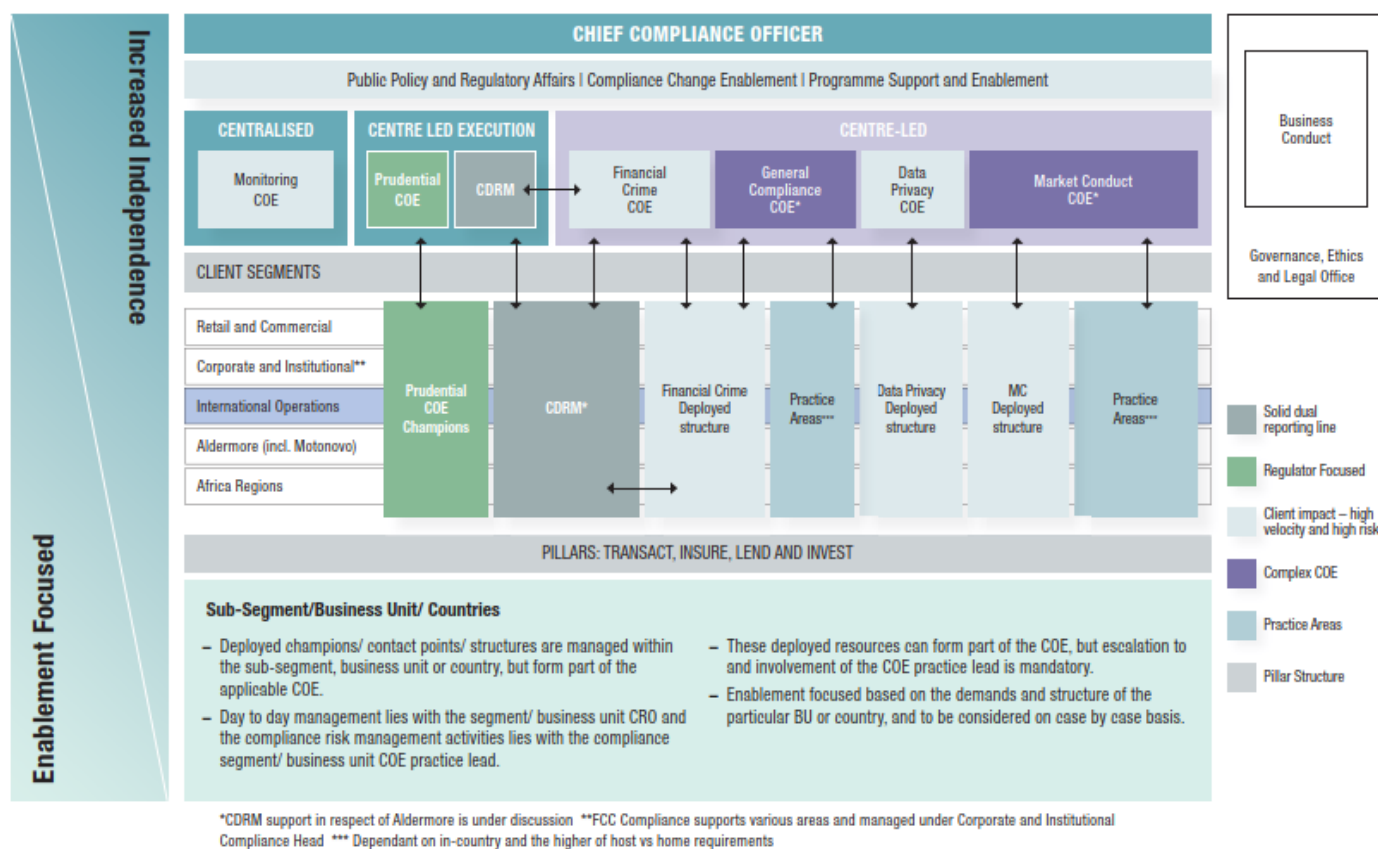


The function is led by the Chief Compliance Officer, who has overall accountability and responsibility of the independent group-wide function. The benefits of the operating model are the following:

- Future proofed strategy alignment, scalable model, covering all compliance risk types
- Closer collaboration and alignment of compliance structures across the function
- Easier access to subject matter experts
- Consistent and advice and guidance across the group
- Reduction of knowledge and skills gaps in compliance
- Strengthened alignment to other functional policies and operating models
- Vertical alignment in FirstRand, down to business units
- Accountabilities and responsibilities clarified across the function
- Built on a firm compliance foundation, the operating model enhances and structures the function into COEs, engagements and formalised ways of work

The group compliance team is located within FCC and predominantly houses the five main centres of excellence (COE), i.e.: Financial Crime, Market Conduct, Data Privacy and Protection, Prudential and General Compliance. These COEs are customer focused on managing high risk impacting pieces of legislation which directs the controls that need to be adhered to in relation to the group's customers, with the exception of the Prudential COE, which is regulator focused. The primary purpose of a COE is to manage the applicable regulatory risk type across the segments and business (scope for ROAI and Aldermore defined as appropriate) and provide contextual advisory solutions. Important to note is the difference between COEs and practice areas within a COE.

FirstRand Compliance – Operating Model



It is the responsibility of each segment to ensure that their compliance programmes are documented, kept up to date and made available to compliance staff and affected stakeholders. If an operating business unit, segment or pillar has reason to deviate from the compliance risk management framework such exception must be documented and submitted to the specific segment risk and audit committee as well as the compliance risk committee (CRC) for approval and noting in terms of the waiver process documented in section 3.3 below.

2.5 Specialist centres of excellence (COEs)

The purpose of the centres of excellence is to provide oversight over compliance sub-risk types and to assist the group in managing the compliance risk in order enable operating business and segment value, promote a sustainable compliance risk environment and culture, whilst achieving regulatory and stakeholder expectations through the nine service value streams.

A centre of excellence is a *pooling of resources* (virtually or physically, depending on the need) who have deep technical capabilities and experience to provide specialist services and support across the group. COEs have a group-wide span of control and mandate, is led by a head, and is comprised of a pool of deep technical capabilities and experience who provide specialist advisory services and support to business. Resourcing requirements are determined by the different activities that

are driven by the COE. These resources are located in group, segments, sub-segments and business units and operate as a deployed structure and the use of these resources will be determined by the work priorities that are managed within the COE.

Practice areas are defined as risk areas, e.g.: ABC, modern slavery, sanctions, etc. which form a sub-area of a broader COE and can leverage off the COE structures and members. These practice areas usually embed the required controls on existing rails and processes of the COE. The span of control can also be limited to a specific area.

The monitoring COE also forms part of the group mandated COEs, however, it operates through a centralised model by owning and managing the monitoring procedures and resources. Within the group compliance structure there are also enablement functions, i.e.: Programme Support and Enablement, Public Policy and Regulatory Affairs and the Compliance Change Enablement function. These functions perform activities that are supportive in nature to the compliance function in terms of projects, training, governance, automation, data analytics, and alignment to platform initiatives. The Public Policy and Regulatory Affairs function manages regulatory relationships and engagements across the group.

The client segment teams, which includes the Retail and Commercial (R&C), Corporate and Institutional (C&I), Pillar and Rest of Africa (RoFA) teams jointly form part of the compliance function that focuses on oversight and enablement to the business. The Client Desirability Risk Management (CDRM) COE function, which is an operational function, reports operationally to FirstRand's Chief Risk Officer, who has strategic and operational responsibility for customer and transaction monitoring, reporting and screening systems. The CDRM function must, however, continue to execute its mandate in accordance with the provisions of FirstRand's compliance risk management and compliance programme under FICA and will, accordingly, be subject to functional oversight by the FirstRand's Group's Chief Compliance Officer in relation to AML/CFT related functions being performed by the CDRM function.

In terms of the FirstRand compliance execution model, there are types of models:

1. The centralised execution model is defined as an operating model whereby processes are centrally designed, run and managed, e.g.: the standard operating procedures to executive the monitoring procedures. It is based on centralised deployment (where the deployed resources report into the COE structure). Execution of the procedures/ processes are performed end to end in terms of the central team.
2. In relation to the centre-led execution model, the processes are executed solely by the centre-led COE function that resides in a function, such as group. There is little to no dependence on other functions to execute the processes and only support is required from the COE champions in instances where coordination or facilitation is required.
3. In terms of the centre-led operating model, this operating model is operationalised through segment deployed execution. The COE is formed and mandated as a group-wide COE and the membership is made up of group, segment and RoFA practice leads/specialists (as appropriate). Deployed COE members are empowered and mandated to own and run the respective compliance programmes and the COE, as a collective, supports and collaborates as and when matters arise. This model enables collaborative thinking and problem solving and removes the siloes from group to segment to business unit.

The core generic responsibilities and mandate of the COEs are the following:

- Frameworks, policies, standard setting, compliance programme management, specialist advisory and risk appetite setting:
 - ✓ Provide thought leadership, define strategic direction and compliance programme plan
 - ✓ Set frameworks, policy, standards and risk and appetite statements and key metrics
 - ✓ Draft policies and minimum standards
 - ✓ Draft related generic training content, in conjunction with business
 - ✓ Assist, as necessary, in the review of transactions, deals, strategic initiatives, and other relationships to ensure conformity with related laws and regulations and the group's global policies
 - ✓ Identify material and strategic key risk focus area, including common thematic breakdowns
 - ✓ Set and oversee compliance programme tasks and deliverables
 - ✓ Provide specialist advice on complex matters
 - ✓ Approve, oversee and manage new license applications (as applicable)
 - ✓ Review new policy related papers, provide SME/COE view and substantive written responses including coordination of internal feedback
 - ✓ Host knowledge sharing workshops and growth plans for upskilling all the COE participants
 - ✓ Conduct impact analysis and guide on operational implementation plan
 - ✓ Coordinate group/entity-wide risks assessments
- Regulatory liaison:
 - ✓ Respond to regulatory inquiries (including complaints)
 - ✓ Draft regulations, directives and guidance notes, etc.
 - ✓ Participate in industry and regulatory meetings
- Governance committees and reporting:
 - ✓ Receive comprehensive reports from pillar/segments with matters for escalation and noting
 - ✓ Ensure reporting integrity, clear articulation of trends and insights
 - ✓ Facilitate appropriate escalation and aggregation of issues
 - ✓ Ensure reporting governance: ensure that the appropriate governance standards and protocols have been adhered to prior to COE escalation
 - ✓ Coordinate, collate, provide quality assurance and prepare documents and responses to information requests and onsite inspections
 - ✓ Coordinate and hold sub-committee meetings, as applicable to COE

The generic COE value streams and activities are set out in a “COE blue print” together with the specific COE engagement manuals are available under annexure 6.

2.6 Operating business, segment and pillar compliance structure

The responsibilities of the each of the group's compliance functions should be carried out under a compliance programme addressing the critical elements listed above and should set out (at a minimum) the operating businesses', segments' and pillars':

- strategy (specifically areas of focus in line with the overall group compliance strategy);
- structure (operating model);
- planned activities e.g., implementation and review of specific policies and procedures;
- compliance risk assessments;
- compliance monitoring and testing; and
- policy for educating staff on compliance matters.

The compliance programme should be risk-based and is subject to oversight by the FirstRand Chief Compliance Officer via monitoring and internal audit assessments to ensure appropriate coverage and coordination across all operating businesses, segments and pillars

It is the responsibility of each segment to ensure that their compliance programmes are documented kept up to date and made available to compliance staff and affected stakeholders. If an operating business, segment and pillar has reason to deviate from the compliance risk management framework such exception must be documented and submitted to the specific segment risk and audit committee as well as the compliance risk committee (CRC) for approval and noting.

3 GOVERNANCE AND OVERSIGHT

The group risk management framework (GRMF) highlights the key principles and guidelines applied with respect to the effective management of risk across FirstRand in the execution of business strategy.

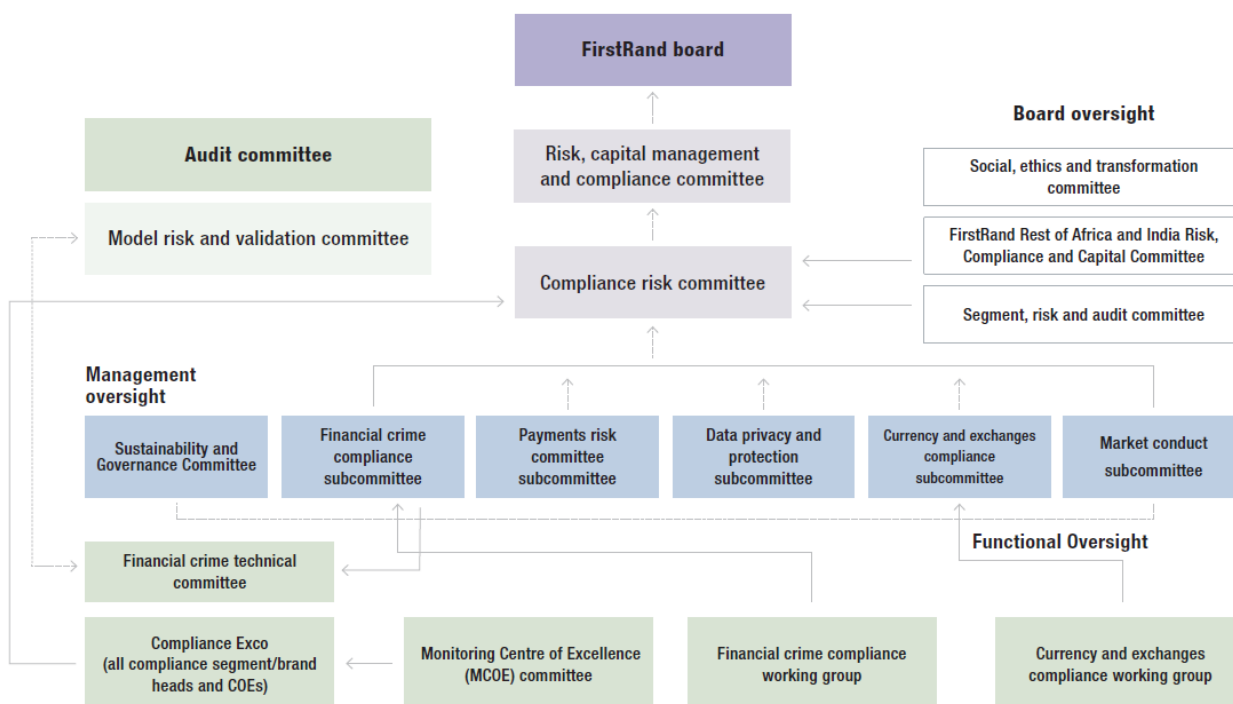
The GRMF is the overarching risk management policy of the FirstRand board. The policy is ancillary to the board's corporate governance framework and gives effect to the requirements of the Banks Act 94 of 1990 (Banks Act) and Regulations, Insurance Act 18 of 2017 and the Prudential Standards prescribed under the Act, Companies Act, 71 of 2008, the principles of the King Code on Corporate Governance 2016 (King IV), and similar acts and regulations in the jurisdictions where the group has its operations. The compliance risk management framework is established in terms of the GRMF and is a management tool to ensure effective compliance and business success. The frameworks set out the high-level principles for the effective management and governance of the group's compliance obligations and compliance risks.

3.1 Introduction

The governance of compliance risk is covered across the operating businesses and segments by various governance platforms that provide functional, management and board oversight of compliance. Functional oversight is provided by amongst others the compliance Exco (see 2.4 below), the monitoring centre of excellence committee and other COE working groups which assist the group structures contained below with management and oversight of compliance risk. Similarly, within the operating business and segments, management oversight is provided by segment specific compliance committees

and quality circles which ensure the flow of information to the group structures are considered and the necessary oversight provided. These are, in turn supplemented with the segment specific governance structures illustrated below in section 2.3. For specific detail on the operating business/segment charters (or terms of reference) the segment compliance heads should be contacted.

Overview of group compliance governance and oversight



3.2 Compliance risk committee (CRC)

The CRC is constituted pursuant to the group risk management framework (GRMF) as approved by the board of directors of FirstRand Limited (the board) and the risk, compliance and capital committee (RCCC), respectively. The CRC is a subcommittee of the RCCC (a FirstRand board risk committee) and meets quarterly.

The primary objective of the CRC is to assist the RCCC in discharging its responsibilities relative to the effective management of the group's compliance risk including, AML/CTR risks as determined, *inter alia*, by:

- Section 60A of the Banks Act, 1990 (Act No. 94 of 1990)
- Section 64A of the Banks Act, 1990 (Act No. 94 of 1990)
- Regulation 39 of the Banks Act, 1990 (Act No. 94 of 1990): Process of corporate governance
- Regulation 49 of the Banks Act, 1990 (Act No. 94 of 1990): Compliance function
- Principles of compliance function in Banks issued by the Basel Committee on Banking Supervision
- Financial Sector Regulation Act (FSR Act 9 of 2017)

- The Financial Intelligence Centre Act 2001, (Act 38 of 2001); International sanctions, related regulations and board resolutions
- GOI 3 of the Prudential Standards to the Insurance (Act 18 of 2017)
- Risk data aggregation and risk reporting (BCBS239)
- Relevant in-country legislation

The CRC is mandated to constitute any sub-committees deemed necessary in order to ensure that the diverse range of compliance risks that the group is faced with are properly managed and monitored within the formalised risk control management and monitoring structures. The CRC shall be responsible for the review of and approval of the charters and composition of the sub-committees of the CRC. The current sub-committees which provide for management oversight of specialised compliance risks cover:

- financial crime regulatory compliance sub-committee
- financial crime technical committee
- data privacy and protection sub-committee
- currencies and exchange sub-committee
- market conduct sub-committee
- payment risk sub-committee

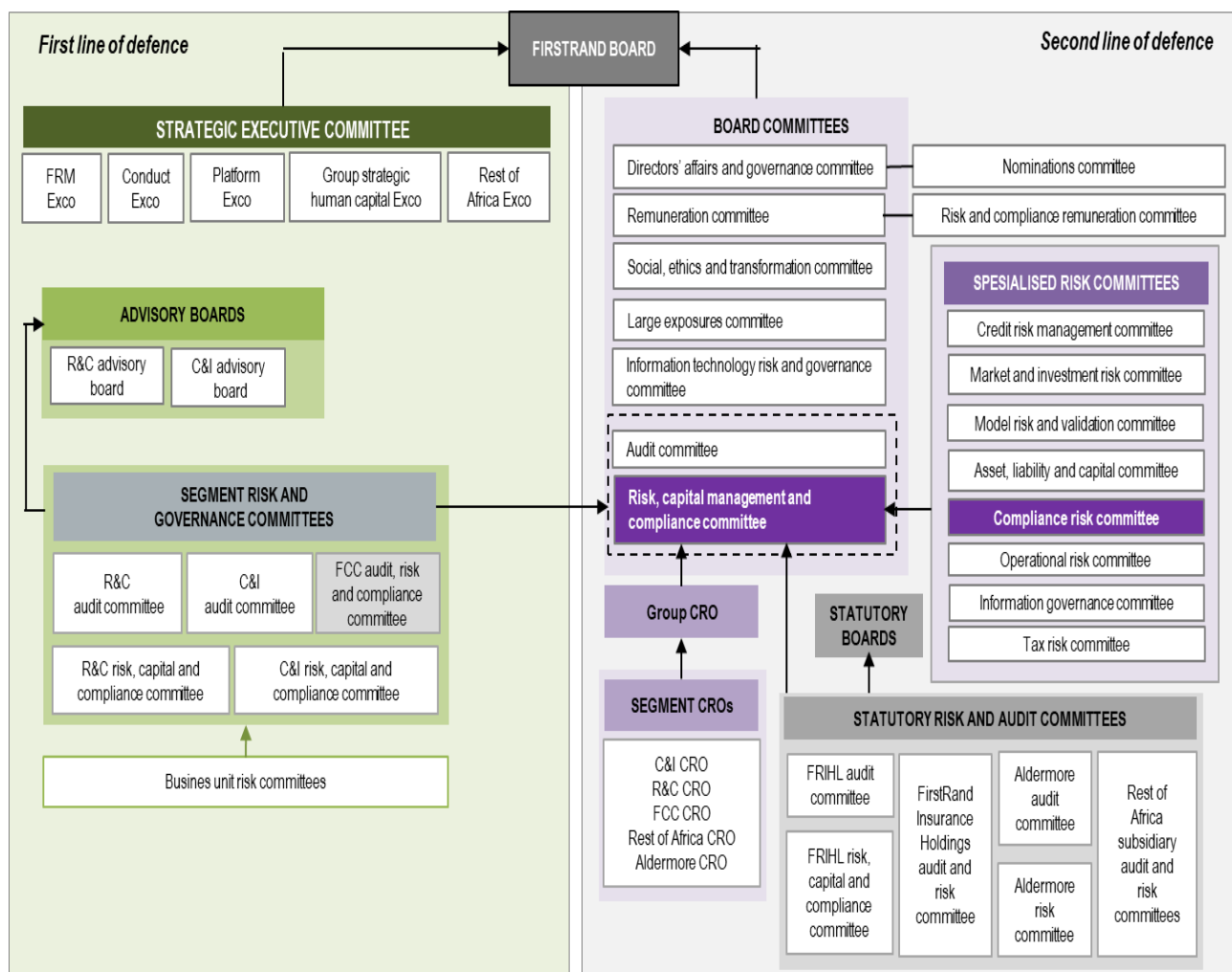
The mandates for each of these sub-committees are covered in the CRC charter under annexure 2.

3.3 Segment compliance governance committees

Compliance is reported on a quarterly basis at the following internal segment governance committees, generally, before being escalated to the CRC (refer to the segment compliance teams directly for more detailed information).

Segments governance committees reporting lines⁵

⁵ Reflects revised FirstRand governance reporting structures for 2022 and are held by FirstRand Company Secretary.



3.4 Compliance executive committee (Compliance Exco)

The FirstRand compliance Exco is constituted as a management committee for the compliance function of FirstRand Limited. Membership includes all the heads of compliance segments and pillars, the heads of the Insure, Lend and Invest Pillars and is chaired by the FirstRand Chief Compliance Officer. The scope includes but is not limited to (**FirstRand compliance Exco terms of reference – annexure 3**):

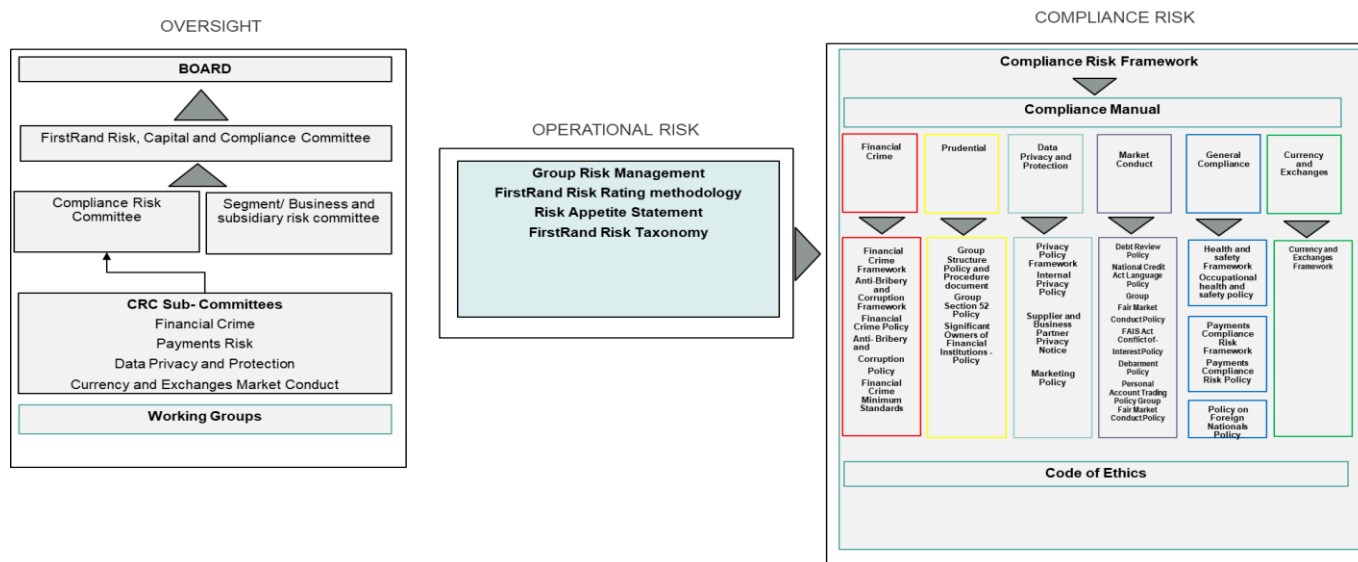
- Spanning across the compliance portfolio across FirstRand's business footprint, inclusive of national and international operations and both banking and non-banking operations.
- Approving any group minimum standards, group operating standards and any other governance documents prior to approval thereof at the CRC where these are of generic applicability and are not approved at one of the established sub-committees of the CRC.
- Providing advisory, decision making and monitoring of the structural architecture of the compliance function, its people, frameworks; policies and enabling platforms.

4 POLICIES, STANDARDS AND ADVISORY SERVICE

Compliance frameworks, policies, procedures and guidelines are designed to inform your everyday responsibilities, to set minimum standards, and to address and mitigate potential risk areas. The compliance framework and policies are aligned and complimentary to the GRMF and other enterprise risk management (ERM) policies as set out below.

4.1 Introduction

Compliance frameworks, policies, procedures and guidelines are designed to inform all staff responsibilities, set minimum standards and address and mitigate potential risk areas. They are part of the broader group-wide risk framework and policy repository. This is illustrated below:



4.2 Policy implementation and roles and responsibilities

- Operating businesses, segments and pillars are responsible for the implementation of, and compliance with all FirstRand compliance frameworks, policies, procedures and guidelines.
- FirstRand employees must comply with the compliance frameworks, policies, procedures and guidelines and accordingly have an obligation to familiarise themselves with those that are applicable to their areas of responsibility.
- Compliance must ensure that employees are appropriately informed in this regard, monitor and report on employees' compliance with this requirement.
- Where any deviation from applicable compliance frameworks, policies, procedures and guidelines occurs, the policy waiver process should be followed as per section 3.3. below.
- FirstRand Group Compliance will maintain oversight of all compliance frameworks, policies, procedures and guidelines published on the SharePoint intranet site - compliance policy repository. **[Click here to access the compliance policy repository.](#)**
 - Group Compliance must ensure that the process followed for the development or revision of compliance frameworks, policies, procedures and guidelines is transparent and inclusive. Input from relevant stakeholders will be obtained and incorporated.

Depending on legal/other requirements, compliance will on an annual/biennial basis review all compliance frameworks, policies, procedures and guidelines in accordance with the CRC charter's annual work plan. A copy of the CRC charter can be accessed at ***FirstRand CRC Charter (annexure 2)***.

4.3 Waiver with regard to set compliance policy requirements

There may be instances where the business is required to adopt a position which will result in non-compliance with certain policy requirements. A waiver is a long-term exemption from a policy requirement or requirements. Waivers may only be granted by exception, e.g., where there are legal prohibitions to compliance or where there is legal or business justification for non-compliance with a policy or standard requirement which justification falls within the applicable segment's approved risk tolerance threshold.

Waivers are generally only possible under very limited circumstances, and for as long as the challenge, constraint, prohibition or justification exists. Despite the compulsory nature of the framework, policies and standards, it is accepted that exceptional circumstances could exist that would necessitate the business to deviate from applicable policy requirements in relation to applicable legislation. This section is not applicable to instances where FirstRand policies are not applicable to certain subsidiaries/entities by way of the fact that the legislation to which the policy pertains, has no force or application to the entity/subsidiary. An example of this is the Financial Advisory and Intermediary Services Act (FAIS) which has effect within SA but not in other countries. In this regard, the FAIS policy, even though a group policy, will, therefore, not apply to FirstRand's offshore subsidiaries and will similarly not require any waiver processes to be followed. Similarly, if a subsidiary/entity is not a licenced insurer or a manager of a collective investment scheme, the Insurance Act, 2017, CISCA and relative policies will not apply. It should, however, be noted that the application of South African legislation to FirstRand's offshore subsidiaries must be carefully considered, on a case-by-case basis, to confirm whether or not such legislation and regulatory instruments issued in terms of such legislation, applies to FirstRand's offshore subsidiaries. An example is the South African Banks Act, 1990 and the Regulations relating to Banks, which applies, directly or indirectly, within the context prescribed, to FirstRand's offshore subsidiaries. The FirstRand compliance manual, therefore, provides for the granting of waivers with regard to applicable compliance policy requirements. The FirstRand compliance manual also provides for the management of instances where business is informed or discovers on their own accord that minimum compliance policy requirements have not been met and that a breach has therefore occurred.

It is the responsibility of each segment to ensure that their compliance programmes are documented kept up to date and made available to compliance staff and affected stakeholders. ***The details of the standards and process that must be followed for approval of waivers is contained in annexure 5.***

Similarly, there may be instances where the business is required to adopt a position which will result in non-compliance with certain policy requirements. Where the domestic legislative and/or regulatory requirements of the host country sets lower standards than those contained in FirstRand compliance policies or standard, a waiver must be obtained to exempt the business from the relevant FirstRand policy requirement(s). A waiver is the action/decision to exclude an operating business,

segment and/or pillar, or a section of employees, from the requirements of FirstRand compliance policy requirements which are otherwise mandatory.

From the above it is clear that a comparison between host country legislation and FirstRand compliance policy requirements must be drawn. It is the responsibility of the management of the particular international operation in the host country to ensure compliance with the laws of the host country and to determine where these obligations differ from that which is stated in FirstRand policy.

4.4 Risk-based decisions

The compliance risk appetite statement acknowledges that there may be instances of unintended failures which result in non-compliance and that remedial action will be taken on a prioritised basis to address those instances which fall outside the defined tolerances it, however, does not advocate condonation for instances of identified non-compliance but rather espouses a risk-based approach that remediates all instances of non-compliance identified, but on a prioritised basis aligned to defined tolerance levels.

In instances where a conclusion (arrived at after careful consideration) is reached that it is impossible to either prevent and/or fully mitigate the matter (could be either identified instances of non-compliance or anticipated instances of non-compliance) i.e., it is not possible to take further preventative action, management shall report this inability to comply to the appropriate governance committee together with the reasons for such failure or inability to comply. These risk-based decisions (dealing with the identified instances of inability to comply) and the reasons therefore must be fully contextualised in line with the board approved compliance risk appetite policy statement and must be subject to the appropriate governance process as detailed in the exemption standard (annexure 5 of the compliance manual). ***The details of the standards and process that must be followed for risk based decisions is contained in annexure 5.***

Engagement with relevant regulators or similar authorities, where appropriate and / or required, will be conducted in consultation with the relevant COE head, subject matter experts (SME) and the affected operating business, segment and/or pillar.

4.5 BCBS 239 for compliance risk

Compliance seeks to implement and ensure the on-going compliance with the principles and requirements set out in the risk data aggregation and risk reporting (RDARR) framework. The compliance standards, procedures and guidelines in respect of this framework has been out in the BCBS 239 Standard for Compliance Risk (***annexure 7***)

5 ASSESSMENT, EVALUATION, MONITORING AND TESTING

As stated in the FirstRand compliance governance framework, the compliance process consists of four distinct phases, which are dealt with in more detail in operating procedures:

- Phase I compliance risk identification;
- Phase II compliance risk assessment/measurement;
- Phase III compliance risk monitoring/mitigation; and
- Phase IV compliance risk reporting/management.

The compliance process is an iterative process and should be followed annually based on the compliance risks identified, measured, monitored, reported and the mitigating corrective actions taken by business. Phase I and II (identification and measurement) covers the ability of the compliance function and business to gain an in depth understanding of the compliance risk profile of the business based on the nature of the business (taking into account customers, services and/or products) and the identified impacting legislation/regulatory instruments/compliance themes that have a bearing on that business. There are over 200 primary pieces of legislation and their subordinate regulatory provisions that affect the group in some way. A risk-based approach to prioritising the compliance management and monitoring of these outputs is followed which in turn is supported by compliance risk rating methodology (***annexure 8 – FirstRand compliance risk rating methodology***⁶). These processes are operationalised within the regulatory universe (RU) and risk management plan (RMP) processes. ***Detailed operating procedures detailing this process is contained in annexures 9 and 10.***

Phase III (compliance 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. Compliance monitoring is a requirement of Regulation 49 of the Banks Act, amongst others, which requires continuous compliance-related monitoring to be performed and ***detailed monitoring standards and operating procedures are contained in annexures 13 and 14.***

Phase IV (compliance risk reporting) is contained under section 5 below.

It is the responsibility of all compliance managers to ensure that senior management is involved in every phase of the process. This is in line with the compliance governance framework that confirms management's (line 1) accountability for compliance risk and mitigating controls.

⁶ Aligned and supplementary to the FirstRand risk rating methodology framework

6 REPORTING, DATA, MEASUREMENT, ESCALATION AND RESOLUTION

Every group employee is responsible for reporting incidents of non-compliance with legislation that he/she is aware of. This should be reported via the relevant BU/segment compliance manager.

It is the responsibility of all compliance employees to promptly report any incident of non-compliance identified, by way of monitoring or a disclosure, directly to the senior management of the business unit as well as to segment compliance and compliance.

Regulation 49 of the Banks Act 94 of 1990: specifies that a bank's compliance officer must:

- report non-compliance with laws and regulations or supervisory requirements to the chief executive officer, the Board of directors and the audit committee of the bank in a timely manner;
- submit a report on the level of compliance with laws and regulations or supervisory requirements at every meeting of the board or the audit committee of the bank and submit a copy of such a report to the Registrar of Banks; establish prompt mechanisms for reporting and resolving non-compliance with laws and regulations or supervisory requirements.

The Prudential Standards to the Insurance Act 18 of 2017, provides that the FirstRand Insurance Holding's compliance function must have access to and report to the board of directors or a committee of the board identified by the board of directors on:

- the strategy of the compliance function;
- the compliance monitoring plan, including specific annual or other short-term goals being pursued and the performance against such goals; and
- information on its resources, including an analysis on the appropriateness of those resources.

The compliance function is responsible for:

- facilitating prompt reporting and resolution of non-compliance with laws, regulations and/or supervisory requirements;
- reporting on progress with the independent monitoring plan and non-compliance with laws, regulations or supervisory requirements to the FirstRand CEO, the Board of directors, and CRC in a timely manner;
- submitting reports on the results of the annual compliance risk monitoring plan and the level of compliance with laws, regulations and/or supervisory requirements by the group at every quarterly RCCC and audit committee meetings and the board of directors, and provide the SA Reserve Bank, Banking Supervision Department with copies of these reports. FirstRand Insurance Holding's compliance function is responsible to submit such report to the Financial Services Board.

6.1.1 Compliance materiality reporting

In terms of Regulation 49(3) (d) & (e) of the Regulations relating to Banks (Banks Act Regulations) and prudential standards under the Insurance Act, all material incidents of non-compliance must be reported to the board of directors of FirstRand or where applicable, board of directors of the insurer. ***The reporting operating procedure details and supports compliance officers with what to report and the principles for reporting (annexure 15).***

In order to ensure that reporting to board governance committees is streamlined it is important for reports to flow promptly to the board of directors or a committee of the board of any material compliance failures (e.g., failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation). Compliance reporting should consider the following factors on terms of materiality for reporting up to board and board sub-committees:

- Any matter that constitutes a 'material malfunction' as defined by the board of directors of FirstRand Limited in terms of Regulation 40(4)(a)(v) of the Banks Act. Only the following should be considered for reporting to board and board sub-committees:
 - material matters affecting compliance with regulatory and/or supervisory requirements and expectations;
 - material risks;
 - material incidents of non-compliance;
 - material deviations from the compliance governance framework;
 - serious systemic&/control weaknesses as they relate to regulatory and/or supervisory requirements and expectations;
 - repetitive non-material incidents of non-compliance, which collectively, may be material; and
 - wilful, and/or grossly negligent incidents of non-compliance;

With reference to Regulation 36(8)(a) of the Banks Act:

- Any correspondence between the group, including the offshore regulated entities (mainly offshore banking operations/groups) and any supervisory authority (including those in offshore jurisdictions) which relates to matters that may or are likely to have a material impact on the Group and/or the supervisory duties of the Registrar of Banks. (These should, once identified, be considered on a case-by-case basis).
- Any material information which may or is likely to negatively affect the group, including the offshore regulated entities (mainly offshore banking operations/groups).
- Any other information or documentation at our disposal that relates to matters that may or are likely to have a material impact on the group and/or the offshore regulated entities (mainly offshore banking operations/groups).
- Any material information which may or is likely to negatively affect the suitability of a major shareholder.

For the purposes of defining materiality in this context, the following non-exhaustive list applies:

- Any matters that are rated as severe or major residual impact in terms of the FirstRand compliance risk rating methodology.
- Any matter which could potentially lead to the:
 - loss of the banking and/or other regulatory licence,
 - imposition of restrictive conditions on the continued operation of the existing licences,
 - imposition of a potential fine of R5 million and higher,
 - imposition of a potential redress to customers exceeding R10 million.
- Any matter which may have a serious impact on our relationships with Regulators.

- Any matter which may impact on the organisation's brand and image with its clients.
- Any compliance related matter which seriously impacts on the ability of the group to achieve business objectives e.g., launch products.
- Any matter that may lead to the imprisonment of any executive officer or an employee of the group.

6.1.2 Compliance themes

A theme-based approach to compliance risk monitoring and reporting has been developed to:

- close the gap between compliance and business;
- alleviate the monitoring burden on compliance officers by catering for coverage of multiple legislation under thematic reviews;
- identify and eliminate regulatory overlap and thereby eliminate over-reporting;
- align the compliance process to business processes (process risk control identification & assessment – PRCI&A) and ensure relevant compliance information on risks and controls are communicated to combined assurance providers for inclusion in PRCI&A implementation;
- ensure alignment of compliance risk management process to market conduct standards (where applicable); and
- meet regulatory and board assurance requirements.

The compliance risk themes are described below.

	Theme	Description
1	Fit and proper	Focus on requirements of directors and employees to conduct and present themselves in a required and appropriate (professional/ethical) manner, both internally and externally, e.g., FAIS Fit and Proper, code of ethics, Companies Act requirements for directors, Prudential Standards GOI 4 Fit and Proper requirements for Insurers, compliance culture etc.
2	Licences, approvals and policies	Focus on requirements and conditions that need to be adhered to in order to commence and/or continue conducting business (e.g., FAIS licence, FIC registration, banking licence, registration with the NCR, registered/licensed insurer, JSE, investment, portfolio and platform management). Includes policy and standard development. Includes policies required in terms of legislation for example, the language policy as required in terms of the NCA. Any actions related to licences or approvals with the applicable regulator such as obtaining and displaying of certificates, registration and compliance with regulatory conditions also included herein.
3	Transaction monitoring	Focus on manual and automated transactional surveillance.
4	Issuing products (includes new and existing products and pricing)	Focus on requirements relating to the issuing of products and services includes new product approval process and pricing considerations, ensuring products are included in AML surveillance feeds. Includes any product requirements ensuring that NCA requirements are complied with such as applying the eligibility criteria to determine NCA impacted consumers, categories of credit agreements and agreements complying with any regulatory requirements.

	Theme	Description
5	Workplace, human capital and training	Focus on requirements relating to the relationship between the employer, employee, training, learning and development and workplace safety includes both voluntary and compulsory legislated training requirements
6	Marketing and disclosures	Focus on regulatory requirements relating to all actions to market, promote and advertise products and services on an external and/or internal basis, e.g., reference to licences, above and below the line marketing, direct marketing or factual information intermediary services (e.g., NCA, FAIS, Insurance Legislation and CPA). Focus on disclosures required to be made in terms of regulatory requirements. Marketing not limited to disclosures, but any regulatory requirement linked to marketing either directly or indirectly.
7	Customer onboarding enhanced due diligence and customer screening	This theme includes regulatory requirements that need to be adhered to prior to entering into a business relationship with a prospective client. These requirements may relate to customer consents, screening of customers and payments, identification and verification of customers, and processes relating to cross-border services or activities. The requirements may further relate to affordability assessments, internal assessment mechanisms and procedures in order to ensure credit is not recklessly extended as well as any regulatory consumer rights are afforded and complied with. Any platform where a customer is onboarded such as an auction is also included as well as the related regulatory compliance requirements in respect of those platforms.
8	Advice	Focus on advice provided by the group, e.g. NCA pre-assessment information and FAIS financial needs analysis.
9	Claims and complaints	Focus on the complaints process and claims from customers (e.g. FAIS complaints process requirements, NCA debt recovery requirements, insurance claims, FSB Complaints Management Discussion Document and post sales FICA complaints). Includes any claims or complaints lodged by the consumer with an external regulatory body or ombud.
10	Record keeping	Focus on the retention, safeguarding and retrieval of information stored (client, institutional and transactional).
11	Post-sales services	Focus on ongoing advice, post sales service levels, warranties, ongoing platform and investment administration. Includes any enforcement action or notices required prior to any enforcement action commencing. Further includes any related rights consumers may have such as applying for debt review, administration or declare themselves insolvent. Therefore, any action which the consumer undertakes after the agreement with the group has been concluded and impacts the agreement are included as a post-sales service. Includes but not limited to promotional competitions or loyalty programmes.
12	Outsourcing and third party management	Focus on third party SLAs, outsourced FSPs, binder and other platform or administration agreements. Includes any service providers or suppliers that the group has engaged to provide any goods or services on behalf of the group.
13	Information management and data quality	Focus on regulatory requirements relating to the obtaining and disbursement of confidential information (both customer and employee). Also focus on regulators' expectations with regard to data quality e.g., data aggregation.
14	Regulator and statutory reporting/disclosure	Focus on regulatory requirements relating to statutory disclosures or reporting to regulators, e.g., the reporting of suspicious transactions, cash threshold reporting,

	Theme	Description
		annual compliance reports in terms of FAIS, LTIA and NCA. Includes any statutory reporting to industry bodies such as bureaus or the Department of Human Settlements Office of Disclosure.

7 TRAINING, AWARENESS AND COMMUNICATION

In as far as the ongoing training of compliance staff is concerned, Regulation 49 requires the bank to do the following:

(q) shall recruit sufficient staff of the correct quality in order to monitor and test continuously the bank's compliance with laws and regulations or supervisory requirements;

(r) shall ensure that compliance staff are trained on a continuous basis in order to ensure that they have adequate technical knowledge in order to understand the regulatory framework that applies to the bank, as well as the risks to which the bank is exposed.

FirstRand is also obliged to comply with the requirements of the Insurance Act in respect of the compliance function as follows:

12.5. must ensure that regular training is conducted on compliance obligations, particularly for employees in positions of trust or responsibility, or who are involved in activities that have significant legal or regulatory risk.

Compliance general awareness training is a formal programme that educates employees and third parties on the policies, procedures and actions required to prevent non-compliance with the law. These policies and procedures are often job or industry specific. However, in many cases they are mandatory and apply across industries that are licenced to perform certain services in terms of specific legislation. **(Compliance learning and development standard is contained in annexure 16)**

7.1 Roles and responsibilities

The objectives of compliance training cover two distinct areas:

- develop and prioritise key training and awareness initiatives (general awareness training) for FirstRand to meet regulatory requirements; and
- develop and implement customised training for compliance officers within the group that is focused on identified competencies including technical knowledge, soft skills and business acumen to enable implementation of the compliance programme and ensure compliance officers within the group have the necessary skills and support to fulfil their duties and fulfil the requirements of Regulation 49 of the Banks Act.

7.2 General awareness training

Compliance-related training is used as a key control for the implementation of an effective compliance programme and for the mitigation of compliance risk arising from regulatory and/or supervisory requirements. As such and due to the legislative imperatives for training of both compliance specific and general employees, compliance training must always be prioritised and should not compete with any non-legislative training requirements for resources.

The target audience for each training programme initiative must follow a risk-based approach which will be decided by FirstRand Group compliance (COEs) with input by L&D. The business compliance officers together with the COE will provide the necessary guidance on who needs to be included or excluded for the training and will carry the risk.

7.3 Compliance officers training

7.3.1 Compliance essentials

This programme includes content and focus areas on the compliance programme with the aim of covering wide ranging topics that affect the compliance community. The key components of the programme will be delivered via induction, e-learning and continuous professional development (CPDs) sessions.

7.3.1.1 Induction

The induction programme is a half-day session held every second month. It provides new joiners information on strategy, programmes, tools and where to get support. The programme topics will be supported by CPD sessions.

7.3.1.2 The e-learning component will cover

- The context of compliance management – the elements of compliance risk management.
- Understanding my role - what is the role a compliance officer plays in business?
- Corporate governance and compliance - corporate governance as the context for managing compliance risk in an organisation.
- Compliance risk profile/regulatory universe - setting the regulatory universe.
- Risk management - using risk management tool in compliance risk management.
- Reporting – relevant, accurate reporting
- Policies – the use and application of compliance policies, frameworks, and standards which policies should you be aware of.
- My Toolkit - tools to support every employee to deliver on their mandate.

7.3.1.3 Continuous professional development (CPD) sessions

L&D will support the hosting of monthly CPDs covering pre-determined topics determined by FirstRand Group compliance.. The annual CPD calendar will be planned, incorporated and approved via the annual same process as the compliance training needs analysis and plan. Attendees can claim CPD hours from Compliance Institute of South Africa (CISA).

7.3.2 Compliance Institute of Southern Africa (CISA)

The Compliance Institute Southern Africa is the recognised professional body for all compliance officers. All employees are encouraged to become members and apply for the professional designations. Since 2011, CISA has developed an occupational curriculum for compliance officers as well as registering two professional designations with the South African Qualifications Authority (SAQA):

- CPrac (CI(SA)) – Compliance Practitioner – currently available; and
- CProf (CI(SA)) – Compliance Professional – currently available.

For more information on CISA go to: <http://www.Compliance sa.com> or email info@Compliance sa.com

8 REGULATOR/INDUSTRY (STAKEHOLDER) INTERACTION AND COORDINATION

The management of the relationship with relevant regulators is a collective responsibility, with Group Compliance through the public policy and regulatory affairs function taking the lead role and with support provided by the relevant operating businesses, segments and pillars. Group Compliance acts as the gateway for all correspondence with regulators to ensure a single point of contact and effective management and tracking of correspondence and responses thereto. In the offshore subsidiaries, each head of compliance acts as the primary conduit for communication with their in-country regulators. FirstRand Group Compliance is engaged where issues need to be communicated to the SARB. Through the public policy and regulatory affairs function, Group Compliance also serves as the central point of coordination and engagement with the Banking Association South Africa (BASA) and other relevant industry bodies.

The Public Policy and Regulatory Affairs office facilitates the process through which the board maintains an effective relationship with both local and international regulatory authorities for the group's regulated subsidiaries, offshore branches and representative offices. The office also provides the group with a central point of engagement, representation and coordination in respect of relevant regulatory and public policy-related matters at a strategic level. This function is differentiated from the existing and continuing engagement with regulators at an operational level, i.e., regulatory reporting, compliance and audit.

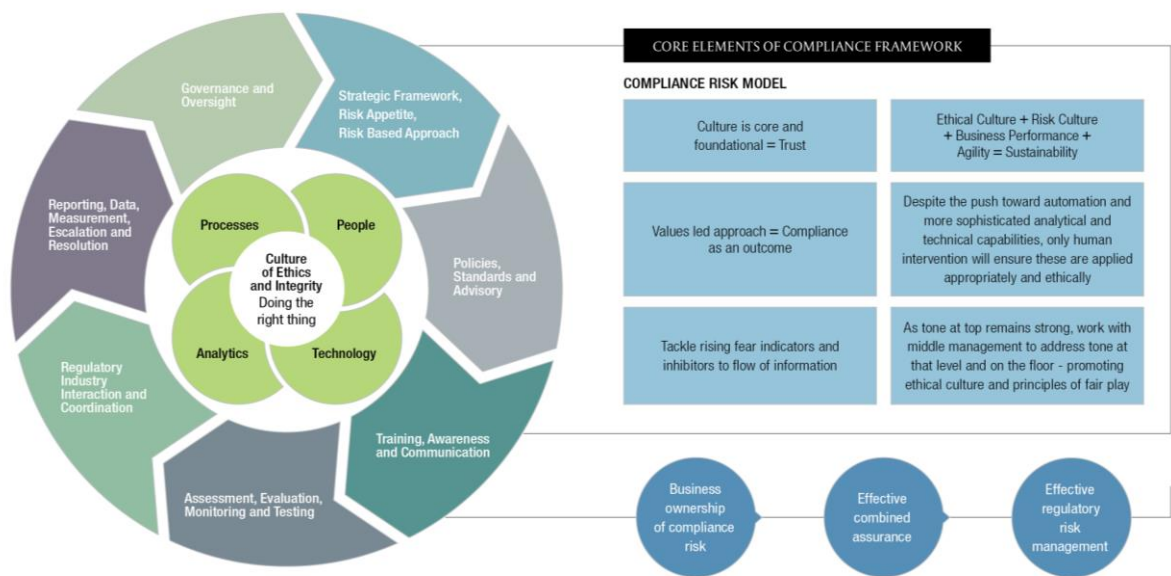
For purposes of the obligations of FirstRand Insurance Holdings, the head of the compliance control function is responsible for management of the relationship with the FSCA and PA (as the case may be) and is the point of contact with the regulatory authority in respect of insurance matters. Similarly, Ashburton Investments deals directly with relevant regulators, pension funds, CISA etc. The relevant FirstRand Compliance SME must be kept apprised of formal liaisons with these regulators.

Should segment compliance (or deployed compliance employees) have a requirement to interact formally with any regulator (formal contact being identified by virtue of the potential materiality of the risk or the outcome which the matter, if not adequately and appropriately addressed, could hold for the group's operations and/or reputation and/or regulatory relationships) on matters that do not qualify as day-to-day operational contact (constituting the exchange of day-to-day communications/daily interactions with regulators around usual operational activities in Group Compliance with regulatory requirements), they should do so in consultation with Group Compliance, Public Policy and Regulatory Affairs executive and the relevant specialist (SME) who should be kept informed of and copied on all such correspondence or interactions.

Effective management of information and clear communication between all compliance staff is essential to ensure the effective management of compliance risk. Effective management of information will enable compliance function to respond meaningfully, consistently and swiftly to the rapidly changing regulatory environment in order to mitigate risk.

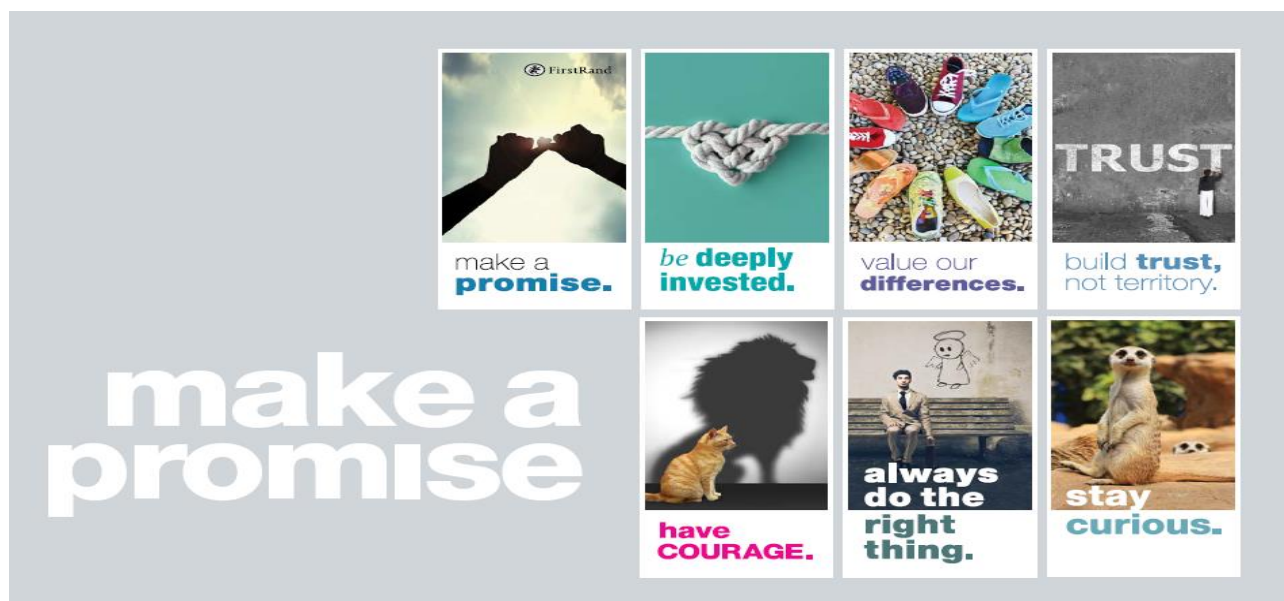
9 FOSTERING AN ETHICAL/COMPLIANCE CULTURE

FirstRand’s compliance governance framework will not be effective unless the board of directors promotes these values of honesty and integrity throughout the organisation. Compliance with applicable laws, rules and standards should be viewed as an essential means to this end. As is the case with other categories of risk, the board is responsible for ensuring that the compliance governance framework appropriately manages the group’s compliance risk. Culture is core and foundational to the compliance programme.



To this end the FirstRand code of ethics forms the constitution, or the base reference point, for the business practices of all businesses in the FirstRand fold. All FirstRand employees, executives and non-executives should read and ensure that they understand the FirstRand code of ethics.

FirstRand’s values include:[FirstRand Philosophy - Home \(sharepoint.com\)](#)



Importantly, FirstRand is committed to treat all suspected or confirmed contraventions of the FirstRand code of ethics individually, according to their merits and in their specific contexts, while paying due heed to applicable policy and law.

It is every employee's responsibility to know how the FirstRand code of ethics relates to them and their role within the workplace. Should they observe conduct that they believe to be contrary to FirstRand's values and guiding principles, they should report these incidences, again using the prescribed approaches. Should they require ethics advice, they should consult the code of ethics, because it lays down appropriate ways to obtain such guidance. **Click here download a copy of the FirstRand code of ethics**

10 ANNEXURES AND ABBREVIATIONS

Ann no	Name	Hyperlinks
1	Compliance governance framework	
2	CRC charter	
3	Compliance Exco terms of reference (TOR)	
4	Compliance policy repository	
5	Exemption standard – waivers and inability to comply	
6	COE engagement manuals	
7	BCBS239 for regulatory risk minimum standard	

COMPLIANCE MANUAL continued

8	Compliance risk rating methodology	
9	FirstRand regulatory universe (South Africa)	
10	FirstRand compliance - prioritised regulatory universe	
11	Regulatory universe (RU) operating procedure	
12	Risk management plan (RMP) operating procedure	
13	FirstRand compliance monitoring standards	
14	FirstRand compliance monitoring operating procedures	
15	Compliance reporting procedure (including materiality thresholds for reporting to governance committees)	
16	Compliance learning and development standard	
17	Compliance risk management maturity model	

11 ABBREVIATIONS:

COE	Centre of excellence
SME	Subject matter expert
NCA	National Credit Act
CPA	Consumer Protection Act
POPI	Protection of Personal information
FAIS	Financial Advisory and Intermediary Services Act
RMP	Risk management plan
PRCI&A	Process, risk, control identification and assessment
Co	Compliance officer

