

**DRAFT FOR CONSULTATION – NOVEMBER 2023**

**Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)**

**Prudential Standard CBA-03**

**Risk management requirements for co-operative financial institutions and co-operative banks**

***Objective and Key Requirements of this Prudential Standard***

*This Standard is made in terms of sections 105 and 108 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) (Financial Sector Regulation Act) read with section 46 of the Co-operative Banks Act, 2007 (Act No. 40 of 2007) (Co-operative Banks Act).*

*This Standard sets out the principles and requirements for risk management for co-operative financial institutions (CFIs) and co-operative banks registered in terms of the Co-operatives Banks Act.*

*This Standard covers matters concerning principles for risk management, risk management strategy, risk management framework, board approved policies, risk management procedures and tools, IT and cybersecurity risk, IT and cybersecurity strategy, internal controls, governance requirements for control functions, risk management function, compliance function, audit committee and regulatory reporting.*

**Table of Contents**

1	Commencement .....	3
2	Legislative authority .....	3
3	Definitions and interpretation .....	3
4	Application .....	4
5	Roles and responsibilities .....	4
6	Principles .....	4
7	Risk management strategy .....	5
8	Risk management framework .....	5
9	Board approved policies .....	7
10	Risk management procedures and tools .....	8
11	IT and cybersecurity risk .....	9
12	IT and cybersecurity strategy .....	9
13	Internal controls .....	11
14	Governance – general requirements for control functions .....	11
15	The risk management function .....	12
16	The compliance function .....	12

17	Audit committee .....	13
18	Regulatory reporting .....	15
19	Short title .....	15
	Attachment 1: Policies for managing financial and non-financial risks .....	16
	Attachment 2: Summary of requirements across tiers .....	21

## 1 Commencement

- 1.1 This Standard commences on 1 July 2024 (proposed).

Version Number	Commencement Date
1	1 July 2024 (proposed)

## 2 Legislative authority

- 2.1 This Standard is made in terms of sections 105 and 108 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) read with section 46 of the Co-operative Banks Act, 2007 (Act No. 40 of 2007).

## 3 Definitions and interpretation

- 3.1 In this Standard, “the Act” means the Co-operative Banks Act and any word or expression to which a meaning has been assigned in the Act or the Financial Sector Regulation Act bears the meaning so assigned to it, unless the context indicates otherwise.

- 3.2 For purposes of this Standard –

‘**audit committee**’ means the audit committee for a CFI<sup>1</sup> and a co-operative bank;  
‘**auditor**’ means a registered auditor as defined in the Auditing Profession Act, 2005 (Act No. 26 of 2005);

‘**Authority**’ means the Prudential Authority established in terms of section 32 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017);

‘**board**’ means the board of directors of the CFI or co-operative bank as appointed by the members in accordance with the constitution of the CFI or co-operative bank;

‘**CFI**’ means a co-operative financial institution as defined in the Act;

‘**co-operative bank**’ means a co-operative bank as defined in the Act;

‘**Co-operatives Act**’ means the Co-operatives Act, 2005 (Act No. 14 of 2005);

‘**control function**’ means each of the following:

- (a) the risk management function
- (b) the compliance function; and
- (c) the internal audit function, when required by the Authority;

‘**cyber event**’ means any observable occurrence in an IT system. Cyber events sometimes provide an indication that a cyber incident is occurring;

‘**cyber incident**’ means a cyber event that –

- (a) jeopardises the cybersecurity of an IT system or the information processed, stored or transmitted by the system; or
- (b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not;

‘**financial information**’ information relating to the finances of the CFI or co-operative bank;

‘**IT**’ means information technology;

‘**management**’ means the managing director and executive officers of the CFI or co-operative bank;

‘**material risk**’ means any risk that can have a material impact, both financial or non-financial, on the CFI, co-operative bank or on the interests of its financial customers; and

---

<sup>1</sup> In some instances, CFIs refer to the audit committee as the supervisory committee. It is advised that this audit committee should not be confused with audit committees that are appointed for companies.

**‘members’** means the members of the CFI or co-operative bank.

- 3.3 The ‘Objectives and key requirements of this Prudential Standard’ in the preamble of this Standard must not be used in the interpretation of any paragraph of this Standard.

## **4 Application**

- 4.1 This Standard applies to all CFIs and co-operative banks registered under the Act, irrespective of its categorisation under a specific tier, unless explicitly provided for in this Standard.
- 4.2 This Standard applies in addition to the requirements of the Co-operatives Act and the Principles of Good Governance for Co-operatives issued under the Co-operatives Act.

## **5 Roles and responsibilities**

- 5.1 The care, diligence and skill displayed by the board and management of a CFI or co-operative bank have a significant influence on the CFI or co-operative bank’s sustainability, safety and soundness as well as its ability to meet its business objectives.
- 5.2 The board of a CFI and co-operative bank is ultimately responsible for ensuring that the CFI or co-operative bank complies with the requirements and principles of sound risk management outlined in this Standard. This includes establishing the CFI or co-operative bank’s overall risk appetite and ensuring that the CFI or co-operative bank has implemented effective systems for risk management to address risks.
- 5.3 The board and the audit committee must inform the Authority in writing of any matter they become aware of in the performance of their functions that has or may contravene the principles and requirements of this Standard.
- 5.4 The audit committee of the CFI or co-operative bank is responsible for providing input and assurance to the members and the board about the operations, efficiency, and effectiveness of the components of the systems for risk management in the financial institution.
- 5.5 The Authority may request an auditor to provide assurance on the requirements of this Standard, if necessary.
- 5.6 CFIs and co-operative banks must, at all times, adhere to the provisions of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) which are applicable to the CFI or co-operative bank.

## **6 Principles**

- 6.1 A financial institution, such as a CFI or co-operative bank, is exposed to a number of risks that can adversely affect its ability to achieve its business objectives. These risks can cause a financial institution to lose earnings and capital and may negatively affect its reputation. CFIs or co-operative banks must accordingly implement a comprehensive, robust and disciplined risk management system that is commensurate with the nature, size, complexity and risk profile of the business.

- 6.2 The objective of risk management is not to eliminate risk, but to prudently manage risk. Risk management tools help to tolerate, treat, transfer or terminate risk. CFIs and co-operative banks typically try to manage some risks, such as credit risk, within defined risk or reward tolerances and other risks, such as operational risk, within expected threshold levels.

## **7 Risk management strategy**

### **7.1 Application of risk management strategy to Tier 1**

- 7.1.1 Tier 1 institutions will be required, as they become established, to work towards developing a risk management strategy. The Authority will monitor the developments of Tier 1 CFIs or co-operative banks in this regard and may specify to the relevant Tier 1 CFI or co-operative bank related requirements or conditions as deemed necessary.

### **7.2 Application of risk management strategy to Tier 2 and Tier 3**

- 7.2.1 A Tier 2 and Tier 3 CFI or co-operative bank must develop and implement a board-approved risk management strategy that sets out the types of risks that the financial institution is subjected to and the way in which it will manage those risks.

### **7.3 The risk management strategy must:**

- 7.3.1 be proportionate to the nature, size, complexity and risk profile of the CFI or co-operative bank and holistically focus on all sources of risk emanating from the financial portfolio and business activities of the financial institution;
- 7.3.2 include both quantitative and qualitative risk appetite and tolerance statements for each identified risk that articulates the levels of risk that a CFI or co-operative bank is willing to assume;
- 7.3.3 include a clear plan on how to prudently manage material risks; and
- 7.3.4 be approved by the board and annually reviewed.

### **7.4 At a minimum, a CFIs or co-operative bank's documented risk management strategy must:**

- 7.4.1 identify the objectives of the strategy;
- 7.4.2 describe each material risk (including emerging risks) and the financial institution's approach to managing those risks;
- 7.4.3 list the policies and procedures for dealing with risk management;
- 7.4.4 summarise the roles and risk management responsibilities of the board, board committees and senior management;
- 7.4.5 include a documented process for board approval for any deviations from the risk management strategy or risk appetite; and
- 7.4.6 outline the CFI's or co-operative bank's approach to ensuring all stakeholders of the CFI or co-operative bank are aware of the risk management framework and for instilling an appropriate risk culture across the institution.

## **8 Risk management framework**

- 8.1 The board of a CFI or a co-operative bank must ensure that an effective system of internal controls is in place to provide reasonable assurance from a control perspective that the CFI or co-operative bank is being operated consistent with its strategies, policies and procedures, which are attaining their intended outcomes.

- 8.2 The details of risk management framework differ among CFIs and co-operative banks and depend on the nature, size, complexity and risk profiles of individual financial institutions.
- 8.3 Application of a risk management framework to a Tier 1 and Tier 2
- 8.3.1 Tier 1 and Tier 2 institutions will be required, as they become established, to work toward developing such a framework. The Authority will monitor the developments of Tier 1 and Tier 2 CFIs or co-operative banks in this regard and may specify to the relevant Tier 1 and Tier 2 CFI or co-operative bank related requirements or conditions as deemed necessary.
- 8.4 Application of risk management framework to Tier 3
- 8.4.1 A Tier 3 CFI or co-operative bank must develop and implement a risk management framework.
- 8.5 A CFI or a co-operative bank must establish, maintain and operate within a system of effective internal controls designed to ensure that the risk management framework is operating effectively and incorporates appropriate checks and balances to ensure that the financial institution operates effectively and efficiently.
- 8.6 The risk management framework must:
- 8.6.1 be approved and reviewed annually by the board;
- 8.6.2 incorporate and address at least the following:
- (a) the risk strategy and risk appetite of the CFI or co-operative bank;
  - (b) policies and related procedures and tools for assessing, monitoring, reporting and mitigating risks that may affect the operations of the CFI or co-operative bank and the ability of the CFI or co-operative bank to meet its obligations to financial customers;
  - (c) appropriate resources and systems for the purposes of aggregating risks; and
  - (d) functionality of information and reporting of material risks to the board, board committees and members of the CFI or co-operative bank.
- 8.6.3 be integrated with its organization structure, decision-making processes, business operations and risk culture; and
- 8.6.4 measure the risk exposure of the CFI or co-operative bank against the risk appetite limits on an ongoing basis in order to identify potential concerns as early as possible.
- 8.7 Other factors that affect the risk management framework are the control environment, experience and qualifications of management and persons in control functions as well as the delegation of authority.
- 8.8 The risk management framework should correlate with the:
- 8.8.1 financial institution's business strategy and plans;
  - 8.8.2 need to generate an appropriate level of sustainable earnings;
  - 8.8.3 interrelationships among risk, reward, capital and liquidity;
  - 8.8.4 nature, size, and complexity of risks that accompany specific decisions; and
  - 8.8.5 regulatory requirements.

- 8.9 The board of the CFI or co-operative bank that is categorised as a Tier 3 CFI or co-operative bank must establish and adequately resource risk management, compliance and internal audit functions to enable:
- 8.9.1 proper identification and addressing of risks that impact on the CFI or the co-operative bank;
  - 8.9.2 the undertaking of adequate monitoring of the implementation of the CFI's and co-operative bank's policies and procedures;
  - 8.9.3 timely and accurate information flows within the CFI or co-operative bank;
  - 8.9.4 effective communication of the CFI's and co-operative bank's objectives, strategies and policies to members of the CFI or co-operative bank; and
  - 8.9.5 promote a CFI or co-operative bank risk and compliance culture.

## **9 Board approved policies**

- 9.1 In respect of Tier 1, Tier 2 and Tier 3, the following board-approved policies and any other policy that is specified to a particular CFI or co-operative bank by the Authority depending on the nature, size complexity and risk profile, must be developed and implemented by a CFI or co-operative bank:
- 9.1.1 operational risk (specifically including information technology and cybersecurity);
  - 9.1.2 savings, including liquidity management; and
  - 9.1.3 loans, including credit risk management (if providing loans).
- 9.2 Board approved policies for Tier 2 and Tier 3
- 9.2.1 Tier 2 CFIs and co-operative banks must in addition to the policies mentioned in paragraph 9.1 above, develop and implement risk policies related to:
- (a) liquidity, including asset-liability management;
  - (b) outsourcing and third-party service provisioning, if applicable;
  - (c) capital management;
  - (d) compliance and legal;
  - (e) concentration;
  - (f) detection and prevention of criminal activities;
  - (g) risk arising from exposure to a related person;
  - (h) fitness and propriety;
  - (i) interest rate;
  - (j) investment;
  - (k) reputational; and
  - (l) cybersecurity and cyber resilience;
- 9.3 Board approved policies for Tier 3
- 9.4 The Authority may specify additional policies that must be developed and implemented by a CFI or co-operative bank as a result of supervisory observations.
- 9.5 A CFI or co-operative bank may combine one or more of the policies for addressing risks specified in paragraphs 9.1 to 9.3 above, provided the CFI or co-operative bank is satisfied that the specified risks do not justify a separate policy given the nature, scale and complexity of the financial institution's business and risks.

- 9.6 Attachment 1 (Policies for managing financial risks) outlines the minimum contents of certain risk management policies specified in paragraphs 9.1 to 9.3 above.
- 9.7 A CFI's and co-operative bank's risk management policies must be reviewed and kept updated in light of emerging risks as follows:
- 9.7.1 Tier 1: Biennially (every other year); and
- 9.7.2 Tier 2 and Tier 3: Annually.
- 9.8 Material changes to the risk management policies must be approved by the board, properly justified and documented. The documentation must be available for review by the audit committee, the auditor of the CFI or the co-operative bank and the Authority.
- 9.9 In terms of the loans policy, referred to in sub-paragraph 9.1.3 above, the policy must include the requirement that the terms and conditions of loans granted to board members, management, employees and related parties of a CFI or cooperative bank may not be more favourable than loans granted to members as well as how loan write-offs will be treated.

## **10 Risk management procedures and tools**

- 10.1 A Tier 1, Tier 2 and Tier 3 CFI or co-operative bank must maintain a suite of risk management procedures and tools that enable it to assess, monitor, mitigate and report the material risks to which it is exposed.
- 10.2 The risk management procedures must include both financial and non-financial risks in its scope.
- 10.3 The suite of risk management procedures must provide the board with an enterprise-wide view of its material risks both financial and non-financial.
- 10.4 A CFI's or a co-operative bank's suite of risk management procedures and tools must be proportionate to the nature, size, complexity and risk profile of the institution, and must, at a minimum include:
- 10.4.1 a process for identifying and assessing new and emerging risks;
- 10.4.2 procedures and tools for quantifying and managing specified individual material risks;
- 10.4.3 means to provides reliable and informative reports on the measurement, assessment and management of all material risks; and
- 10.4.4 a review process to ensure that the risk management system remains effective in identifying, quantifying, assessing and managing material risks to which the CFI or co-operative bank is exposed.
- 10.5 Tier 2 or 3 CFIs and co-operative bank may be requested by the Authority to:
- 10.5.1 apply scenario analysis and stress testing programs that are commensurate with the nature, size, complexity and risk profile of the financial institution's business; and
- 10.5.2 apply a forward-looking approach to assessing enterprise-wide financial risk.



10.6 A CFI or a co-operative bank's risk management procedures and tools must be reviewed regularly, but at least annually, and kept updated in light of emerging risks and changes in risk management tools and techniques.

10.7 Material changes to the risk management procedures and tools must be approved by the board, properly justified and documented. The documentation must be available for review by the audit committee, the auditor of the CFI or co-operative bank, and the Authority.

## **11 IT and cybersecurity risk**

11.1 A Tier 1, Tier 2 and Tier 3 CFI or co-operative bank must:

11.1.1 implement appropriate information security solutions at the data, application, database, operating systems and network layers to adequately address and contain all forms of security vulnerabilities;

11.1.2 establish measures that protect data at-rest, in-transit and in-storage, commensurate with the criticality of the information held, also extending to backup systems and offline data stores;

11.1.3 deploy firewalls or other similar measures within internal networks to minimise the impact of security exposures originating from third party or offshore systems, as well as from the internal trusted network;

11.1.4 deploy anti-virus software to servers and workstations. The anti-virus definition files must be regularly updated. An automatic anti-virus scanning must be scheduled on servers and workstations on a regular basis;

11.1.5 define and implement data and IT systems backup and restoration procedures to ensure that they can be recovered as required;

11.1.6 implement appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit or contain the impact of a potential cyber event.

11.1.7 protect sensitive or confidential information such as customer personal account and transaction data which are stored and processed in systems; and

11.1.8 mitigate IT risks and protect information assets in accordance with their sensitivity classification.

11.2 A financial institution must establish a sound IT continuity process and IT continuity plan to ensure the ability to return the IT components /telecommunication services and other specific IT essential operations, functions or process, and so on, to a state of normality in the event of severe business disruption.

## **12 IT and cybersecurity strategy**

12.1 A Tier 1, Tier 2 and Tier 3 CFI or co-operative bank must have a board approved IT and cybersecurity strategy that is aligned with its overall business strategy.

12.2 The IT and cybersecurity strategy of a CFI or co-operative bank must be reviewed regularly but at least annually.

12.3 As part of its overall risk management framework, a CFI or co-operative bank must establish an IT and cybersecurity risk management framework to manage IT and cybersecurity risks in a systematic and consistent manner.

12.4 The IT and cybersecurity risk management framework of a CFI or co-operative bank must be approved by the board and reviewed regularly, but at least annually.

- 12.5 The IT and cybersecurity risk management framework of a CFI or co-operative bank must, at a minimum, encompass the following attributes and requirements:
- 12.5.1 IT and cybersecurity policies, standards and procedures in managing IT and cybersecurity risks and safeguarding IT assets in the organisation;
  - 12.5.2 the ability to detect, control and limit all major risk, taking into consideration the principle of proportionality;
  - 12.5.3 IT and cybersecurity policies, standards and procedures reviewed and updated to take into account, among others, rapid changes in the IT and cybersecurity operating and security environment;
  - 12.5.4 roles and responsibilities in managing IT and cybersecurity risks, in terms of which:
  - 12.5.5 the board and senior management must oversee the design, implementation and effectiveness of IT and cybersecurity risk management programmes;
  - 12.5.6 the board and senior management must ensure that CFI or co-operative bank have adequate internal governance and internal control frameworks in place for their IT and cybersecurity risk management;
  - 12.5.7 the governing body and senior management are fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability;
  - 12.5.8 a Tier 3 CFI or co-operative bank must have a function responsible for ensuring that proper risk management measures are implemented and enforced for a specific IT and cybersecurity, and this function or department must be:
    - (a) accountable for, and be given the authority to manage IT and cybersecurity risks; and
    - (b) headed by an individual with requisite skills and experience, and who is part of senior management;
  - 12.5.9 identification and prioritisation of IT assets in terms of which:
    - (a) IT assets must be appropriately identified, recorded and protected from unauthorised access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure; and
    - (b) criticality of IT assets must be identified and ascertained in order to develop appropriate plans to protect them;
  - 12.5.10 identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities in terms of which a CFI or co-operative bank must:
    - (a) following risk identification, perform an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations; and
    - (b) develop a threat and vulnerability matrix to assess the impact of the threat to its IT and cybersecurity environment. The matrix should also assist the CFI or co-operative bank in prioritising IT and cybersecurity risks;
  - 12.5.11 implementation of appropriate practices and controls to mitigate risks in terms of which:
    - (a) the CFI or co-operative bank must, for each type of risk identified, develop and implement risk mitigation and control strategies that are consistent with the importance of the IT assets and the level of risk tolerance;
    - (b) the CFI or co-operative bank must be able to manage and control risks in a manner that will maintain its financial and operational viability and stability;
    - (c) the CFI or co-operative bank must, when deciding on the adoption of controls and security measures, also be conscious of the effectiveness of the controls with regard to the risks being mitigated; and
    - (d) as a risk mitigating measure, a financial institution must consider taking insurance cover for various IT risks.

## **13 Internal controls**

- 13.1 Internal controls are a critical component of a financial institution's risk management framework, and these are the policies, procedures and processes established by the board and management to provide reasonable assurance on the safety, effectiveness and efficiency of the financial institutions operations, the reliability of financial and managerial reporting, and compliance with regulatory requirements.
- 13.2 As part of the risk management system, a Tier 1, Tier 2 and Tier 3 CFI or co-operative bank must develop and implement a board-approved framework of effective internal controls to address the scope of risks faced by the financial institution.
- 13.3 An internal control system must be appropriate to the nature, size, complexity and risk profile of the CFI or the co-operative bank's business and risks.
- 13.4 At a minimum, a CFI's and co-operative bank's internal control system must provide for the following:
  - 13.4.1 appropriate segregation of duties and controls to ensure that segregation and independence is observed;
  - 13.4.2 effective controls over commitments of, and payments by, the CFI or co-operative bank;
  - 13.4.3 effective controls over conflict of interests;
  - 13.4.4 appropriate controls for all key business processes and policies, including for major business decisions;
  - 13.4.5 controls to provide reasonable assurance over the fairness, accuracy, reliability and completeness of the CFI's and co-operative bank's financial, regulatory and non-financial information (reported both internally and externally);
  - 13.4.6 board-approved delegations of authority, (these should also be reviewed regularly by the board);
  - 13.4.7 regular monitoring of all controls to ensure they remain effective;
  - 13.4.8 a centralised inventory of all key policies and procedures, and the controls in respect of each policy and procedure; and
  - 13.4.9 training in respect of relevant components of the internal control system, particularly for employees in positions of trust or responsibility, or who carrying out activities that involve significant risk.
- 13.5 The Authority may specify additional policies that must be developed and implemented by a CFI or co-operative bank as a result of supervisory observations.

## **14 Governance – general requirements for control functions**

- 14.1 To provide appropriate governance over the risk management system, a Tier 3 CFI or co-operative bank must establish and adequately resource staff to be able to effectively deliver on the responsibilities regarding control functions.
- 14.2 The authority and responsibilities of each control function must be documented and subject to regular review.
- 14.3 The board must approve the roles and responsibilities, and any changes to the roles or responsibilities of the control functions and must ensure that each function has the resources, authority and independence needed to meet its responsibilities.

- 14.4 A financial institution's control functions must be adequately staffed by appropriately qualified and competent persons who have sufficient authority to perform their roles effectively.
- 14.5 The board may outsource a control function subject to the prior written approval of the Authority.
- 14.6 Each control function must conduct regular self-assessments of their respective functions and implement or monitor the implementation of any identified improvements.
- 14.7 The Authority may require the CFI or co-operative bank to appoint an internal audit function.
- 14.8 Control functions should operate without conflicts of interest; where a conflict arises, it must be brought to the attention of the board for resolution.
- 14.9 Control functions must have the right to conduct investigations of possible breaches and to request assistance for such investigations from specialists within the CFI or co-operative bank, or external specialists.

## **15 The risk management function**

- 15.1 A CFI or co-operative bank must have an effective risk management function, capable of assisting the financial institution to identify, assess, monitor, and mitigate its material risks, and promote a sound risk culture. This function may be carried out by the audit committee in a Tier 1 and Tier 2 CFI or co-operative bank on application to the Authority. Tier 3 CFIs or co-operative banks must have a dedicated resource to carry out this function.
- 15.2 The risk management and compliance functions will be required to have a member of current staff that will discharge such functions.
- 15.3 A CFIs risk management function is responsible for assisting the board directors and management to develop and maintain the financial institution risk management system, including promptly informing the board of any circumstance that may have an adverse material effect on the risk management system of the CFI or co-operative bank.

## **16 The compliance function**

- 16.1 A CFI or co-operative bank must have an effective compliance function capable of assisting the CFI or co-operative bank to meet its legal, regulatory and supervisory obligations and promote and sustain a sound compliance culture. This function may be carried out by the audit committee in a Tier 1 and Tier 2 CFIs or co-operative banks on application to the Authority. Tier 3 CFIs or co-operative banks must have a dedicated resource to carry out this function.
- 16.2 A CFIs or co-operative bank's compliance function is responsible for assisting the board and management to identify and meet their legal and regulatory obligations.
- 16.3 The responsibilities of a CFIs or co-operative bank's compliance function include implementing a risk-based compliance plan for monitoring compliance with the

financial institution system of internal controls, as well as legal and regulatory obligations.

- 16.4 The compliance function must monitor compliance shortcomings and in instances of non-compliance report such to the Authority or other relevant regulatory authorities.
- 16.5 A CFI or co-operative bank's compliance function 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.

## **17 Audit committee**

- 17.1 A Tier 1, Tier 2 and Tier 3 CFI or co-operative bank must have an effective audit committee which is enabled to provide the members and the board with independent assurance in respect of the quality and effectiveness of the financial institutions corporate governance framework, and systems for risk management.
- 17.2 Members of the audit committee must be elected by the members of the CFI or the co-operative bank at the annual general meeting and should not have operational business line responsibilities.
- 17.3 In instances, where members of the audit committee are remunerated, their remuneration should not be linked to the financial performance of the CFI or the co-operative bank subject to approval by the Authority.
- 17.4 Members of the audit committee must:
  - 17.4.1 be approved by the Authority<sup>2</sup>;
  - 17.4.2 be fit and proper;
  - 17.4.3 have sufficient seniority and authority within the CFI's or co-operative bank's governance structure to be effective;
  - 17.4.4 have reporting lines that support their independence;
  - 17.4.5 have unrestricted access to relevant information;
  - 17.4.6 have direct access to the board of directors or relevant Committees, without the presence of senior management if so requested, for the purpose of raising concerns about the effectiveness of the risk management system; and
  - 17.4.7 have the freedom to report to the general members, board of directors or relevant Committees without fear of intimidation and retaliation from the board or management.
- 17.5 The audit committee must report regularly to the general members or relevant Committees.
- 17.6 The audit committee must report in writing to the members, board of directors or relevant committees any suspected contravention of any financial sector law that applies to the CFI or co-operative bank. The suspected contravention must also be immediately reported to the Authority if, in the opinion of the audit committee, the contraventions is affecting the safety and soundness of the financial institution.

---

<sup>2</sup> Refer to the requirements outlined in the Prudential Standard CBA-01 – Registration and operational requirements for CFIs and co-operative banks.

- 17.7 The Authority may require the audit committee to provide a report on the matters being considered by the Committee as well as the intended actions or actions taken.
- 17.8 The audit committee must have a signed committee charter that will govern how the committee operates as well as outlines the role, responsibilities, composition and operating guidelines of the committee.
- 17.9 The audit committee must have a three-year plan, that outlines what the committee plans to achieve, and should be revised annually.
- 17.10 The audit committee must also provide independent assurance to the board of directors, through regular audit activities, on matters such as:
- 17.10.1 compliance with anti-money laundering (AML), counter-financing of terrorism (CFT) and proliferation of financing requirements;
  - 17.10.2 the means by which the financial institution preserves its assets and those of members, and seeks to prevent fraud, misappropriation or misapplication of such assets;
  - 17.10.3 the reliability, integrity and completeness of the accounting, financial and risk reporting information, as well as the capacity and adaptability of the financial institution's information technology architecture to provide that information in a timely manner to the board and management;
  - 17.10.4 the design and operational effectiveness of the financial institution's controls in respect of matters referred to in paragraph 17.10;
  - 17.10.5 other matters as may be requested by the board of directors, management, the Authority or the auditor; and
  - 17.10.6 other matters which the audit function determines should be reviewed to fulfil its responsibilities as set out in its charter.
- 17.11 A CFI's or co-operative bank's audit committee is responsible for proposing an auditor to perform the annual audit of the financial records and books of the financial institution, coordinating with the auditors and, to the extent requested by the board and consistent with applicable law, evaluating the quality of performance of the auditors.
- 17.12 In addition, the audit committee as mandated by the members, must:
- 17.12.1 regularly review the systems for governance and risk management, and provide an independent assurance to the members and the board of directors that the systems and processes are effective;
  - 17.12.2 must provide an independent assurance to the members and the Authority, if requested, that the CFI or co-operative bank complies with the requirements of the Act and prudential standards issued under the Act;
  - 17.12.3 must report to the members, board of directors and the Authority any matters identified during the performance of its responsibilities that are contrary to the Act or the prudential standards issued under the Act or will negatively affect the maintenance of a sound risk management framework; and
  - 17.12.4 ensure that the CFI or co-operative bank has an internal process to address all the issues raised by the audit committee, an auditor.
- 17.13 The audit committee must provide a detailed report to the board and the annual general meeting on its activities and requirements set out in this Standard.

17.14 In its reporting, the audit committee should address at least the following areas:

- 17.14.1 the committee's annual or other periodic risk-based audit plan, detailing the proposed areas of audit focus, and any significant modifications to the audit plan;
- 17.14.2 any factors that may adversely affect the Supervisory/Audit function's independence, objectivity or effectiveness;
- 17.14.3 verification of the member deposit, share, and loan accounts with the records;
- 17.14.4 receiving and investigation of any complaint or appeal by members concerning the operations of the CFI or co-operative bank;
- 17.14.5 material findings from audits or reviews conducted; and
- 17.14.6 the extent of senior management's compliance with agreed corrective or risk mitigating measures in response to identified control deficiencies, system weaknesses, or compliance violations.

## **18 Regulatory reporting**

- 18.1 The form, manner and period for regulatory reporting on this Standard will be determined by the Authority and published on its website.
- 18.2 The Authority may specify with the relevant CFI or co-operate bank, other areas of reporting when it becomes necessary based on the nature, size, complexity and risk profile of the CFI or co-operative bank.

## **19 Short title**

- 19.1 This Standard shall be called 'Prudential Standard CBA-03 – Risk management requirements for co-operative financial institutions and co-operative banks.'

## **Attachment 1: Policies for managing financial and non-financial risks**

1. As part of prudent business management, a CFI or co-operative bank must have board-approved policies that address the identification and management of the risks it faces, that are proportionate to the nature, scale or complexity of the CFI or co-operative bank.
2. This Attachment provides details on the minimum required content of the risk management policies set out in paragraph 9 of this Standard.
3. Unless otherwise approved by the Authority, the CFI or co-operative bank must adopt the following policies and must address at least the issues raised in this Attachment.

### **A. Strategic risk management policy (including capital management)**

A CFI's or co-operative bank's Strategic Risk Management Policy must:

1. Include strategic plans which shall be supported by appropriate organisational and functional structures, skilled and experienced personnel, an adequate budget, management information systems, as well as risk monitoring and controlling systems.
2. Be consistent with the organisational goals and shall be adjustable to changing environmental factors.
3. Provide for clear responsibility for the Strategic plan and the strategic planning process to the board of directors or a delegated committee. If the strategic planning process is not appropriate or if the assumptions are not realistic, the strategic plan will be flawed thereby exposing the institution to strategic risk.
4. Set an appropriate budget and provide for development of operational plans consistent with the overall CFI or co-operative bank's strategy by management.
5. Provide for a Capital Management Policy which must:
  - (a) Provide for an internal capital planning process.
  - (b) Set out the CFI's or co-operative bank strategy for ensuring adequate capital is maintained over time, including specific, quantifiable internal capital targets. These targets should be set in the context of the results of the CFI's or co-operative bank's reviews, the CFI's risk profile, the board of directors' risk appetite, and regulatory capital requirements. The strategy should include plans for how target levels of capital are to be met and the means available for sourcing additional capital where required. The strategy should be consistent with the CFI's or co-operative bank's overall business and risk management strategy.
  - (c) Provide for the identification and measurement of risks that may result in capital shortfalls.
  - (d) Establish procedures for monitoring the CFI's or co-operative bank's compliance with its regulatory and internal capital requirements and targets, including triggers to alert management to potential breaches of the regulatory and target capital requirements.
  - (e) Set out the actions to be taken where capital shortfalls occur or are likely to occur.
  - (f) Provide for appropriate management and regular review of capital and the capital management process (including independent review).



## **B. Credit risk policy**

A CFI's or co-operative bank's credit risk policy must:

1. Set out the CFI's or co-operative bank's approach to the identification, assessment, monitoring, management, and reporting of credit risk (including credit concentration risk). The CFI's or co-operative bank's approach to managing credit risk should be consistent with the complexity, risk profile, and scope of operations of the CFI or co-operative bank.
2. Identify the full range of credit exposures the CFI or co-operative bank is likely to encounter in its normal course of business.
3. Identify the range of credit exposures the CFI or co-operative bank is willing to take on, and the ways in which it will avoid taking on those risks that it is unwilling to retain.
4. Provide for quantification of credit risks, using a methodology that is consistent with the complexity, risk profile, and scope of operations of the CFI or co-operative bank.
5. Identify risk mitigation strategies for managing credit exposures to ensure they are kept within the credit risk limits set by the board. Where risk mitigation involves risk transfer to another party, the CFI or co-operative bank should ensure that the credit risk of the transferee is appropriately factored into the CFI's or co-operative bank's assessment of residual credit risk.

## **C. Interest rate risk policy**

CFIs and co-operative banks are not expected to have significant equity and currency risk on their balance sheets without prior approval by the Authority. Consequently, emphasis is placed on the interest rate risk component of market risk as it is the predominant factor.

A CFI's or co-operative bank interest rate risk policy must:

1. Specify clear responsibilities of the board with respect to:
  - (a) setting out the CFI's or co-operative bank's approach to the definition, identification, measurement, management and reporting of interest rate risk. The CFI's or co-operative bank approach to managing interest rate risk should be consistent with the complexity, risk profile, and scope of operations of the CFI or co-operative bank;
  - (b) reviewing the overall objectives of the CFI or co-operative bank with respect to interest rate risk and ensuring the provision of clear guidance regarding the level of interest rate risk acceptable to the CFI or co-operative bank;
  - (c) approving broad business strategies of the CFI or co-operative bank with respect to interest rate risk and ensuring that management takes the steps necessary to identify, measure, monitor, and control interest rate risk.
  - (d) approving policies that identify lines of authority and responsibility for managing interest rate risk exposures; and
  - (e) delegating responsibility for establishing interest rate risk policies to the relevant board committee.
2. Clear responsibility of management to maintain and ensure:
  - (a) appropriate limits on risk taking;
  - (b) adequate management information systems and standards for measuring interest rate risk;
  - (c) standards for valuing positions and measuring performance;
  - (d) a comprehensive interest rate risk reporting and management review process; and
  - (e) effective internal controls.

3. Provide for a mechanism to annually review the CFI's or co-operative bank's interest rate risk management policies and procedures to ensure that they remain appropriate and sound.
4. Periodically update members and the Authority with respect to interest rate risk measurement, reporting and management procedures.

**D. Liquidity Management Policy (including asset-liability management)**

A CFI's or co-operative bank's liquidity management policy must:

1. Set out the CFI's or co-operative bank's approach to the definition, identification, measurement, management and reporting of short-term and long-term liquidity risk, to ensure that the financial institution is able to meet its obligations as they fall due. The CFI's or co-operative bank approach to managing liquidity risk should be consistent with the complexity, risk profile, and scope of operations of the CFI or co-operative bank. The approach must include early warning indicators, triggers, action plans, and clear responsibilities for responding to liquidity stresses, should they arise.
2. Include stress testing in order to determine the impact on the CFI's or co-operative bank's liquidity position of a range of adverse scenarios. These scenarios should include major trigger events such as catastrophes, counterparty defaults, and other adverse events.
3. Take specific account of the liquidity consequences of financial difficulties or default by its counterparties, and the types of events that could lead to such difficulties.
4. Take specific account of the nature of the CFI's or co-operative bank's investments and the impact of adverse scenarios on the liquidity of these investments.
5. Clearly specify the nature, role and extent of the CFI's or co-operative bank's liquidity risk activities and their relationship with product development, pricing functions and investment management.
6. Co-ordinate the management of risks associated with liquidity risk and the complexity of those risks.
7. Recognise the interdependence between the CFI's or co-operative bank's assets and liabilities and take into account the correlation of risk between different asset classes and the correlations between different products and business lines.
8. Specify clear responsibilities of the board with respect to:
  - (a) Reviewing the overall objectives of the CFI or co-operative bank with respect to liquidity and ensuring the provision of clear guidance regarding the level of liquidity risk acceptable to the CFI or co-operative bank;
  - (b) Approving broad business strategies of the CFI or co-operative bank with respect to liquidity risk and ensuring that management takes the steps necessary to identify, measure, monitor, and control liquidity risk;
9. Delegating responsibility for establishing liquidity risk policies to the relevant board committee.
10. Clear responsibility of management to maintain and ensure:
  - (a) Appropriate limits on risk taking;
  - (b) Adequate management information systems and standards for measuring liquidity risk;
11. Effective internal controls.
12. Provide for a mechanism to annually review the CFI or co-operative bank's liquidity risk management policies and procedures to ensure that they remain appropriate and sound.

## **E. Operational Risk Policy**

A CFI's or co-operative bank operational risk policy must:

1. Set out the CFI's or co-operative bank's approach to the identification, assessment, monitoring, management and reporting of relevant operational risk exposures (including the risks associated with inadequate or failed internal processes, people or systems, or from external events).
2. Policies and procedures shall contain processes, among others, to identify, assess, monitor and control/mitigate operational risk such as:
  - (a) Risk and Control Self-Assessments, its methodology, the frequency with which it has to be done and the persons involved in the process;
  - (b) Key Risk Indicator identification and assessment methodology;
  - (c) The methodology for the capture and use of internal and external operational risk loss data; and
  - (d) Documented risk monitoring and reporting procedures.
3. Provide for the development and implementation of an information technology internal control framework that:
  - (a) addresses planning, implementation, delivery, support, monitoring and reporting;
  - (b) addresses effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance; and
  - (c) provides for independent assurance on the effectiveness of the information technology internal controls, including data management systems.
4. Address critical technology-related risk areas such as:
  - (a) The information technology policy must address the way in which the CFI or co-operative bank monitors, manages and responds to cyber risk (which is risk of major disruption from a cyber-attack);
  - (b) CFIs or co-operative banks must have a Cyber Attack Response Plan, with clear assignment of roles and responsibilities for responding to the attack; and
  - (c) Integration risk - the risk arising from participation in a networked banking platform/system.
5. Provide for processes to ensure the promotion of an ethical information technology governance culture and awareness.
6. Provide for processes and procedures to ensure the effective management and utilisation of information technology assets.
7. Keeping members informed of cyber-attacks.
8. Provide for the development, implementation and management of systems for the management of information and data, including systems in respect of information security.
9. Provide for contingency plans in cases of business disruptions commensurate to the nature, scale and complexity of the CFI or co-operative.
10. Provide for controls and processes relating to money-laundering and other financial crimes including processes and controls relating to Know-Your-Customer.

## **F. Legal and Compliance Risk Policy**

A CFI's or co-operative bank's legal and compliance risk policy must:

1. Include the nature and level of legal & compliance risk to which the CFI or co-operative bank is exposed and how its risk profile fits within the overall business strategy.
2. Clear responsibility for legal and compliance risk, including sufficient board and committee oversight;

3. Include a clear process for the review of the constitution, adherence to democratic process, including the annual general meeting.
4. Include mechanisms to review the representational responsibilities and terms of the board annually and review and develop board policies, including aspects of board succession planning.
5. In general, the policies and procedures shall provide for the following among other considerations:
  - (a) a framework for dealing with legal matters of varying complexity;
  - (b) maintenance of a central inventory of key documents such as contracts, licenses, policy statements and others;
  - (c) regular review and assessment of legal risk in the CFI or co-operative bank's activities including new products;
  - (d) adequate documentation on all significant transactions including security administration;
  - (e) record maintenance in line with relevant statutory requirements; and
  - (f) maintenance of confidentiality provisions.
6. Include reporting mechanisms for deviations and non-compliance to the Authority.

**G. Outsourcing policy**

A CFI's or co-operative bank's outsourcing policy must provide for the following:

1. Establish criteria and procedures for appointing and renewing outsourcing service providers;
2. Provide guidance on how to assess, monitor and managed outsourcing risk;
3. Stipulate that management and the board retains all the responsibility for all regulatory obligations, and ensuring that the outsourced activity does not increase the risk profile of the CFI or co-operative bank;
4. A risk assessment on the potential service provider to form part of the due diligence process, prior to the on-boarding of the service provider;
5. Provide for open communication channels between the CFI or co-operative bank and the outsourcing service provider; and
6. Annual review and approval by the board.



SOUTH AFRICAN RESERVE BANK  
Prudential Authority

## Attachment 2: Summary of requirements across tiers

		Tier 1 (Basic)	Tier 2 (Maturing)	Tier 3 (Established)
5.2	<b>Roles and responsibilities</b>	The board for the overall risk appetite and ensuring it has implemented effective systems for risk management to address risks		
CBA02 5.3		Board and Audit committee to provide written report contraventions of principles and requirements		
5.4	Approval of auditor (comments section)	Approval of Auditor	Approval of Auditor	Approval of Auditor
CBA03 7.2	<b>Risk management strategy</b>	Once registered and established, work toward adopting a risk strategy. PA can direct conditions if necessary	Sets out the type of risk and the way it will manage its risks and risk tolerances	Set out types of risk and the way it will manage its risks and risk tolerances
7.1		Proportionate to the nature, size, complexity and risk		
CBA03 7.5			Objectives, material risks and mitigants, policies and procedures, roles and risk management and responsibilities of the board, board committees and senior management; board approval for deviations; risk culture and annual review	Objectives, material risks and mitigants, policies and procedures, roles and risk management and responsibilities of the board, board committees and senior management; board approval for deviations; risk culture and annual review
CBA03 8.2	<b>Risk management framework</b>	Required, as they become established to work toward developing such a framework. The Authority will monitor the developments of Tier 1 in this regard and may specify to the relevant Tier 1 requirements or conditions as deemed necessary.	Required, as they become established to work toward developing such a framework. The Authority will monitor the developments of Tier 2 in this regard and may specify to the relevant Tier 2 requirements or conditions as deemed necessary.	Risk Framework must be approved by the board and incorporate the following: risk strategy and appetite; policies and procedures and tools for assessing, monitoring, reporting and mitigating risks; resources and systems for aggregating risks; reporting of material risks to governance structures; integrated and measurable.
CBA03 8.2		Effective system of internal controls is in from a control perspective that consistent with its strategies, policies and procedures to attain their intended outcomes	Effective system of internal controls is in from a control perspective that consistent with its strategies, policies and procedures to attain their intended outcomes	Effective system of internal controls is in from a control perspective that consistent with its strategies, policies and procedures to attain their intended outcomes
CBA03 8.1		Risk framework must be approved by the board	Risk framework must be approved by the board	Risk framework must be approved by the board and incorporates the following risk strategy and risk appetite to assess, monitor, report and mitigate risks; resources and systems for aggregating risks; reporting of material risks governance

		Tier 1 (Basic)	Tier 2 (Maturing)	Tier 3 (Established)
				structures; integration into organization and measures the risk exposure against risk appetite limits
				Must establish and adequately resource risk management, compliance and internal audit functions
9.1	<b>Policies</b>	Operational risk including information technology and cybersecurity	Operational risk including information technology and cybersecurity	Operational risk including information technology and cybersecurity
9.1.1		savings, including liquidity management; and	savings, including liquidity management; and	savings, including liquidity management; and
9.1.2		loans, including credit risk management (if providing loans).	loans, including credit risk management (if providing loans).	loans, including credit risk management (if providing loans).
9.1.3 (a)			Liquidity, including ALM	Liquidity, including ALM
9.2.1 (b)			Outsourcing and third party risk	Outsource risk
9.2.1 (c)			capital management	capital management;
9.2.1 (d)			compliance and legal risk	compliance risk;
9.2.1 (e)			concentration	concentration risk;
9.2.1 (f)			detection and prevention of criminal activities	detection and prevention of criminal activities risk;
9.2.1 (g)			risk arising from exposure to a related person	risk arising from exposure to a related person;
9.2.1 (h)			Fitness and propriety	Fitness and propriety risk;
9.2.1 (i)			interest rate	interest rate risk;
9.2.1 (j)			investment risk	investment risk;
9.2.1 (k)			reputational risk	reputational risk;
9.2.1 (l)			cybersecurity and cyber resilience; and	cybersecurity and cyber resilience; and
9.3.1 (a)				market risk
9.7.1		Biennially review	Annually	Annually
10	<b>Risk management procedures and tools</b>	Maintaining a suite of risk management tools to monitor, assess, mitigate and report all risks	Maintaining a suite of risk management tools to monitor, assess, mitigate and report risks	Maintaining a suite of risk management tools to monitor, assess, mitigate and report risks
10.5.1			May need to apply scenario analysis and testing	Scenario analysis and stress testing
			Forward-looking enterprise risk approach	Forward-looking enterprise risk approach
11.1.1	<b>IT and cybersecurity risk</b>	implement security solutions to contain all forms of security vulnerabilities;	implement security solutions to contain all forms of security vulnerabilities;	implement security solutions to contain all forms of security vulnerabilities;
11.1.2		protect data including backup systems and offline data stores;	protect data including backup systems and offline data stores;	protect data including backup systems and offline data stores;
11.1.2		deploy firewalls to minimize security exposures to networks	deploy firewalls to minimize security exposures to networks	deploy firewalls to minimize security exposures to networks
11.1.4		deploy anti-virus software to servers and workstations.	deploy anti-virus software to servers and workstations.	deploy anti-virus software to servers and workstations.

		<b>Tier 1 (Basic)</b>	<b>Tier 2 (Maturing)</b>	<b>Tier 3 (Established)</b>
11.1.5		implement data and IT systems backup and restoration procedures	implement data and IT systems backup and restoration procedures	implement data and IT systems backup and restoration procedures
11.1.6		implement capabilities to prevent, limit or contain the impact of a potential cyber event.	implement capabilities to prevent, limit or contain the impact of a potential cyber event.	implement capabilities to prevent, limit or contain the impact of a potential cyber event.
11.1.7		protect sensitive or confidential information	protect sensitive or confidential information	protect sensitive or confidential information
11.1.8		protect information assets	protect information assets	protect information assets
12.1	<b>IT and cybersecurity strategy</b>	Approved IT and cybersecurity strategy	Approved IT and cybersecurity strategy	Approved IT and cybersecurity strategy
12.2		reviewed annually	reviewed annually	reviewed annually
12.3		Establish an IT and cybersecurity risk management framework	Establish an IT and cybersecurity risk management framework	Establish an IT and cybersecurity risk management framework
12.4		reviewed annually	reviewed annually	reviewed annually
12.5.1-6		Framework Includes: policies, standards and procedures to safeguard org, proportionality, changing environment, responsibilities, oversight and controls	Framework Includes: policies, standards and procedures to safeguard org, proportionality, changing environment, responsibilities, oversight and controls	Framework Includes: policies, standards and procedures to safeguard org, proportionality, changing environment, responsibilities, oversight and controls
12.5.8				Have an IT function (dept) to implement IT and cybersecurity risk management
13.2	<b>Internal Controls</b>	Board approved framework of effective internal controls	Board approved framework of effective internal controls	Board approved framework of effective internal controls
14.	<b>Governance of control function</b>			Must establish and adequately resource staff to deliver on control function.
				May be outsourced with PA approval
				May be required to establish an internal audit function
15	<b>Risk management function</b>	Done by audit (supervisory) committee	Done by audit (supervisory) committee	Done by audit (supervisory) committee and a dedicated resource to assist the board develop and maintain the risk management function
16	<b>Compliance function</b>	May apply to the PA to combine the compliance function with that of the audit (supervisory) committee	May apply to the PA to combine the compliance function with that of the audit (supervisory) committee	Done by audit (supervisory) committee and a dedicated resource to assist the board in legal and compliance matters
17.2	<b>Audit committee</b>	Elected by the members at an AGM	Elected by the members at an AGM	Elected by the members at an AGM
		Remuneration of the audit committee with approval of the PA	Remuneration of the audit committee with approval of the PA	Remuneration of the audit committee with approval of the PA
17.6		Report irregularities to members and the PA	Report irregularities to members and the PA	Report irregularities to members and the PA
17.12.2		Provide independent assurance to members and the PA	Provide independent assurance to members and the PA	Provide independent assurance to members and the PA
17.13 17.14		Provide a report to its member covering its annual plan and implementation, verifications done, complaints received and	Provide a report to its member covering its annual plan and implementation, verifications done, complaints received and	Provide a report to its member covering its annual plan and implementation, verifications done, complaints received and

		<b>Tier 1 (Basic)</b>	<b>Tier 2 (Maturing)</b>	<b>Tier 3 (Established)</b>
		findings, material findings and managements attendance to issues identified	findings, material findings and managements attendance to issues identified	findings, material findings and managements attendance to issues identified
18	<b>Regulatory reporting</b>	PA may require additional areas of reporting become necessary based on the nature scale, and risk profile of the institution	PA may require additional areas of reporting become necessary based on the nature scale, and risk profile of the institution	PA may require additional areas of reporting become necessary based on the nature scale, and risk profile of the institution