

 P O Box 427 Pretoria 0001 South Africa
 370 Helen Joseph Street Pretoria 0002
 +27 12 313 3911 / 0861 12 7272
 www.resbank.co.za



Ref.: 15/8/1/2

G2/2023

To: All banks, controlling companies, branches of foreign institutions, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Flavour of the year meetings are to be held during the 2023 calendar year with the boards of directors of banks and controlling companies as well as executive management of South African banks and representatives from branches of foreign institutions

Executive summary

This guidance note serves to inform all banks, controlling companies and branches of foreign institutions (hereinafter collectively referred to as 'banks') of the flavour-of-the-year topics for the discussions to be held with the respective boards of directors and executive management of South African (SA) banks and representatives from branches of foreign institutions during 2023.

1. Introduction

- 1.1 Annually, the Prudential Authority (PA) considers whether any current developments affecting regulated institutions at an industry level are of such significance that additional focus from a supervisory perspective is required. The topic(s), selected through the PA's governance processes, are communicated to regulated institutions at the beginning of the year and are referred to as 'flavour-of-the-year' (FOTY) topics.
- 1.2 The PA has determined that for the 2023 calendar year, the FOTY topics will be organisational resilience and climate-related risks. This guidance note will focus solely on organisational resilience.

2. Organisational resilience

2.1 Background

- 2.1.1 Organisational resilience is defined as the ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organisations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external

context. Enhancing resilience can be a strategic organisational goal and is the outcome of good business practice and the effective management of risk.

2.1.2 More recently, there is increasing occurrence of events, including economic shocks, cyber incidents, changing weather patterns, negative publicity and disclosures related to bad governance practices, that directly affect the operations and reputation of organisations.

2.1.3 A commitment to enhanced organisational resilience contributes to the preservation of core functions and the ability to recover from adversity. The unprecedented disruption caused by the Covid-19 pandemic to economies, organisations, and individuals, tested organisational resilience. Agile and resilient solutions to address potentially devastating crises will need to be identified, implemented, embedded and managed.

2.1.4 Although the PA-regulated institutions remained resilient during the pandemic, there remain significant risks in the longer term economic outlook. There is therefore a need to further explore institutions' capabilities to ensure business continuity and resilience. The FOTY engagements will require the institutions to unpack the end-to-end business models as well as the board's awareness and involvement.

2.2 Format of discussion

2.2.1 The chairperson of the capital and risk management subcommittee (or equivalent) is required to make a high-level presentation to the PA on organisational resilience. The duration of the presentation should be targeted at approximately 45 minutes.

2.2.2 The PA requires to be provided with a copy of the presentation at least three weeks prior to the meeting.

3. Aspects that should be covered during the presentation

3.1 Governance and leadership

3.1.1 How organisational resilience is defined and adopted to strengthen the culture of the institution.

3.1.2 The strategy to operate under normal circumstances as well as respond to and recover from disruption, uncertainty, and change affected by the increase in volatility, uncertainty, complexity, and ambiguity of risks from both the internal and external environment.

3.1.3 The role of oversight and assurance providers in the organisational resilience process.

3.2 Risk management

3.2.1 The organisation's risk appetite in relation to organisational resilience.

3.2.2 The risk management processes to inform the resilience plan, which covers the following:

i) Identification and assessment of threats/risks.

- ii) Monitoring and responding to these threats/risks.
- iii) Reporting and escalation to the appropriate governance structures/committees.

3.3 Mapping of interconnections and interdependencies

- 3.3.1 The organisation's critical operations identified, considered, and mapping of its interconnectedness and interdependencies (both internal and external, including local, regional and international financial sectors) that are necessary for the delivery of critical operations.

3.4 Change readiness

- 3.4.1 The process adopted by the organisation to improve its adaptability, innovation, and willingness to embrace change at all levels, so that products, services, and business processes better fit the new conditions brought about by long-term changes to its environment.

3.5 Situational awareness

- 3.5.1 The institution's ability to ensure it has adequate processes and procedures to respond during normal and stress events including considering the Principles for the Sound Management of Operational Risk (PSMOR), Principles for Operational Resilience (POR) and Risk Data Aggregation and Risk reporting (RDARR).
- 3.5.2 Strong crisis leadership to provide good management and decision-making during times of crisis as well as continuous evaluation of strategies and work programmes in line with organisational goals.
- 3.5.3 Outline the process for testing/validating the organisation's resilience plan against a range of scenarios. e.g., operational, financial, solvency and so forth.
- 3.5.4 The organisation's ability to leverage on lessons learnt from past incidents and the results of scenario testing.

3.6 Information and communication technology (ICT), including cybersecurity

- 3.6.1 The process and defined framework developed by the institution to ensure resilient Information and Communications Technology (ICT), including cybersecurity.

3.7 Third party dependency and supply chain

- 3.7.1 The strategy in place to ensure that the organisation obtains comfort and satisfies itself that appropriate resilience conditions are in place with partners, third party providers, outsourced services, suppliers and other key interested parties to safeguard the institution's critical operations.
- 3.7.2 How the organisation leverage from its supply chain partners.
- 3.7.3 Processes are in place to assess concentration risk in relation to third party service provisioning.

4. Additional topic

- 4.1 As referenced in paragraph 1.2, the FOTY includes a secondary topic on climate-related risks; however, this topic will only be discussed with selected financial institutions. The selected institutions will receive a letter from the Prudential Authority. The items to be covered are attached as Annexure A, for general information purposes only.

5. Acknowledgement of receipt

- 5.1 A written acknowledgement of receipt of this guidance note, signed by the Chief Executive Officer, should be submitted to the PA Frontline team responsible for the supervision of the bank within 10 working days of receipt. Should you have any queries in this regard, please contact the relevant PA Frontline team.

Fundi Tshazibana

Fundi Tshazibana
Chief Executive Officer

Date: 08/03/23

The previous guidance note issued was Guidance Note 1/2023, dated 22 February 2023