



## Prudential Communication 5 of 2026

### Financial Sector Regulation Act 9 of 2017

### Banks Act 94 of 1990

### The 2026 Flavour-of-the-year topic communication to banks

#### ***Objective of this Prudential Communication***

This communication provides information on the Prudential Authority's 2026 Flavour-of-the-year topic, which focuses on *'the effectiveness of anti-money laundering, counter-financing of terrorism and counter-proliferation financing (AML/CFT/CPF) controls'*.

#### **1. Application**

- 1.1 This Prudential Communication is applicable to banks, controlling companies and branches of foreign institutions as defined in the Banks Act, 1990 (Act No. 94 of 1990) (hereinafter collectively referred to as banks).

#### **2. Purpose**

- 2.1 The purpose of this Prudential Communication is to provide information on the 2026 Flavour-of-the-year topic for banks.

#### **3. Introduction**

- 3.1 The Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) (FSR Act) mandates the Prudential Authority (PA) to promote and enhance the safety and soundness of financial institutions that provide financial products and securities services as well as market infrastructures. In accordance with the provisions of section 34(4)(a) of the FSR Act, the PA is required to follow a risk-based, forward-looking (pre-emptive), outcome-focused and integrated approach to supervision.
- 3.2 In consideration of the above, the PA annually reviews whether any ongoing developments or emerging risks affecting regulated financial institutions at industry level warrant increased supervisory attention. The selected theme, known as the flavour-of-the-year topic, is then communicated to these institutions.

- 3.3 The PA has determined that the 2026 Flavour-of-the-year topic will be *'the effectiveness of anti-money laundering, counter-financing of terrorism and counter-proliferation financing (AML/CFT/CPF) controls'*.
- 3.4 It is important to note that these controls should be informed by a comprehensive understanding of money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks.
- 3.5 The PA requires all banks to address the flavour-of-the-year topic at their annual Board prudential (or equivalent committee) meeting.

#### **4. Background**

- 4.1 The objective of the FSR Act is to achieve a stable financial system that works in the interests of financial customers and supports balanced and sustainable economic growth in the Republic. This is achieved by establishing, together with the specific financial sector laws, a regulatory and supervisory framework that promotes, among others, the prevention of financial crime<sup>1</sup>.
- 4.2 The Financial Intelligence Centre Act 38 of 2001 (FIC Act) requires all accountable institutions<sup>2</sup> to identify, assess, monitor, mitigate and manage the risk that their products or services, whether new or existing, may be used to facilitate ML, TF or PF activities.
- 4.3 These requirements are in line with international standards as set out by the Financial Action Task Force (FATF).<sup>3</sup>
- 4.4 To fulfil these obligations, accountable institutions must establish, document, maintain and implement a comprehensive risk management and compliance programme (RMCP) for AML/CFT/CPF.
- 4.5 It is necessary for accountable institutions to provide clear, tangible evidence that demonstrate their ability to detect, deter and address criminal abuse of their products and services. This includes preventing terrorist financing, disrupting financial flows that may support proliferation activities and enabling the Board of Directors or its equivalent committee (Board) to critically evaluate the adequacy and effectiveness of preventive controls and the institution's overall success in mitigating ML/TF/PF risks.
- 4.6 This process enables the Board to stay informed of recurring or persistent control failures and thematic areas of concern (identified through internal or external audits, supervisory inspections, or assurance exercises), and to provide strategic direction on necessary corrective actions or enhancements.

---

<sup>1</sup> The FSR Act defines 'financial crime' as including an offence in terms of:

(a) a financial sector law;

(b) sections 2, 4, 5 and 6 of the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);

(c) the FIC Act; or

(d) section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004);

<sup>2</sup> As per Schedule 1 of the Schedules to the FIC Act

<sup>3</sup> International intergovernmental body responsible for setting standards in AML/CFT/CPF

## 5. Engagement approach

- 5.1 A non-executive member of the Board must provide a presentation to the PA on the effectiveness of their institution's AML/CFT/CPF controls during the scheduled prudential meeting. The presentation should last approximately 45 minutes.
- 5.2 The PA must receive a copy of the presentation at least three weeks before the scheduled prudential meeting.
- 5.3 The PA endeavours to communicate the overall thematic outcome of these engagements to the industry at an aggregate level.

## 6. Minimum aspects to be addressed in the presentation

- 6.1 The bank must provide information demonstrating the effectiveness of its AML/CFT/CPF controls over the past five years, focusing on the following:
  - 6.1.1 Board oversight and assurance: Effectiveness of Board oversight regarding the bank's AML/CFT/CPF control framework, including independent assurance.
  - 6.1.2 Understanding of ML/TF/PF risks: Demonstrate how ML/TF/PF risks have evolved over the past five years, particularly in relation to the accountable institution.
  - 6.1.3 Consideration of national and sector risk assessments: Explain the extent to which the findings from the national and banking sector risk assessments have been incorporated into the RMCP of the accountable institution.
  - 6.1.4 Due diligence and record-keeping: Outline measures that show the effectiveness of customer due diligence, enhanced due diligence, ongoing due diligence and record-keeping (e.g. number of rejections at onboarding and cases where client risk ratings were changed due to new data).
  - 6.1.5 Politically exposed persons and prominent influential persons: Effectiveness of controls to identify politically exposed persons and prominent influential persons and the management of such relationships, including enhanced monitoring as required.
  - 6.1.6 Transaction monitoring detection systems: Effectiveness of transaction monitoring systems and their capacity to proactively detect suspicious and unusual transactions or activities, including independent assurance processes.
  - 6.1.7 TF risk: Effectiveness of TF risk mitigation measures (other than targeted financial sanctions), including transaction monitoring.
  - 6.1.8 PF risk: Effectiveness of PF risk mitigation measures (other than targeted financial sanctions), including transaction monitoring.
  - 6.1.9 Correspondent banking relationships: Effectiveness of risk management in correspondent banking relationships (CBR), including monitoring cross-border flows for suspicious and unusual activities and provide assurance that controls are in place to mitigate exposure to sanctioned entities and high-risk jurisdictions.

- 6.1.10 High-risk countries: Explain how high-risk countries identified by FATF are measured and how risk mitigation measures are implemented when dealing with these jurisdictions.
- 6.1.11 Wire transfers (FATF Recommendation 16): Outline adherence to wire transfer rules and compliance with FATF Recommendation 16.
- 6.1.12 New technologies: Describe the extent to which ML/TF/PF risks are considered when implementing new technologies for products, services, onboarding and transactions. The bank must also describe how governance controls are independently tested and how they mitigate ML/TF/PF risks.
- 6.1.13 Cross-border subsidiaries: Assess the effectiveness of oversight for ensuring cross-border subsidiaries adhere to group AML/CFT/CPF policies.

## **7. Acknowledgement of receipt**

- 7.1 A written acknowledgement, signed by the Chief Executive Officer (or equivalent) of the bank, must be submitted to the PA Frontline team and AML/CFT/CPF team responsible for supervising the bank within 10 working days of receiving this communication. Please direct any related queries to the PA AML/CFT/CPF team on [AML-Mutualevaluation@resbank.co.za](mailto:AML-Mutualevaluation@resbank.co.za).

Fundi Tshazibana  
**Chief Executive Officer**

Date: