South African Reserve Bank

Prudential Authority

Ref.: 15/8/1/3

D2/2019

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

Directive 2/2019 issued in terms of section 6(6) of the Banks Act 94 of 1990

Reporting of material information technology and/or cyber incidents

Executive summary

Regulation 39 of the Regulations relating to Banks requires banks, controlling companies and branches of foreign institutions (hereinafter collectively referred to as 'banks') to establish and maintain an adequate and effective process of corporate governance. This includes the maintenance of effective risk management processes by banks and the continual management of material exposures to risk such as operational risk, including technological risk.

This Directive sets out the Prudential Authority's reporting requirements in relation to material information technology and/or cyber incidents.

1. Introduction

1.1 The Prudential Authority (PA) is cognisant of the different participants in the financial services sector, including regulators, industry associations, financial institutions and other role players reporting on information technology (IT) incidents to different forums/committees within the South African Reserve Bank (SARB). The focus areas, purpose of reporting and the level of detail reported to these forums are often substantially different from the requirements of the PA.

1.2 The PA is aware that there are general IT and cyber incidents which could cause significant disruptions to the operations of a bank or have a material impact on the bank.

1.3 The Bank for International Settlements' Financial Stability Institute (FSI) published a paper titled 'FSI Insight on policy implementation No 2: regulatory approaches to enhance bank's cyber-security frameworks'[1], which requires banks to establish a sound governance framework with clear accountabilities with regard to cyber-risk, as IT exposes banks to cyber-risk and cyberattacks.

[1] https://www.bis.org/fsi/publ/insights2.pdf

1.4 In this regard, the PA has decided to implement minimum reporting requirements with regard to material IT and cyber incidents.

1.5 The classification of materiality should be performed in accordance with the bank's risk profile based on the nature, size and complexity of its business.

1.6 For the purpose of this Directive:

1.6.1 A 'material incident' refers to a disruption of a business activity, process or function which has, or is likely to have, a severe and widespread impact on the bank's operations, services to its customers, or the broader financial system and economy.

1.6.2 An 'IT incident' is defined as an event, occurrence or circumstance that is not expected or planned as part of the normal operations of a bank and has an effect of disrupting the normal operations of the bank's IT systems or services.

1.6.3 A 'cyber incident'[2] is any observable occurrence in an information system that (i) jeopardises the cybersecurity of an information system or the information processed, stored or transmitted by the system; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

1.6.4 An 'information system'[3] is a set of applications, services, information technology assets or other information-handling components, which includes the operating environment.

1.7 The purpose of this Directive is to set out the PA's minimum reporting requirements in relation to material incidents that are IT and/or cyber related.

2. Directive

2.1 Based on the aforesaid, and in accordance with the provisions of section 6(6) of the Banks Act 94 of 1990, banks are hereby directed to:

2.1.1 comply with the reporting requirements set out in this directive in relation to material IT and/ or cyber incidents;

2.1.2 establish and maintain robust governance structures, which includes the coverage of IT, to ensure adequate management and operational oversight over critical business functions, resources and infrastructure;

2.1.3 implement a sufficiently robust incident management framework to manage and report IT and cyber incidents;

2.1.4 notify the PA, as soon as practically possible but not later than one day, following the discovery of a material IT and/or cyber incident;

---

[2] http://www.fsb.org/wp-content/uploads/P121118-1.pdf
[3] http://www.fsb.org/wp-content/uploads/P121118-1.pdf

2.1.5 complete the form titled 'Material IT and cyber incident report' (Annexure A) in accordance with the relevant instructions specified on the form, and submit the duly completed form to: SARB-PA-ITIncidentReporting@resbank.co.za; and

2.1.6 submit a root cause and impact analysis report, with available information to the PA within 14 calendar days from the date of notification to the PA referred to in paragraph 2.1.4. Subsequent updates are to be sent to the PA based on the timelines agreed with the PA.

3. Acknowledgement of receipt

3.1 Kindly ensure that a copy of this Directive is made available to your institution's external auditors. The attached acknowledgement of receipt duly completed and signed by both the chief executive officer of the institution and the said auditors should be returned to the PA at the earliest convenience of the aforementioned signatories.

Kuben Naidoo
Deputy Governor and CEO: Prudential Authority

Date: 10 SEPTEMBER 2019

Encl. 1

The previous directive issued was Directive 1/2019 dated 20 May 2019.