South African Reserve Bank

Prudential Authority

Ref.:15/8/1/3

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

Proposed directive issued in terms of section 6(6) of the Banks Act 94 of 1990

Reporting of material information technology (including cyber) failures or 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 (including cyber) failures or 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 (FIs) and other role players reporting on information technology (IT) failures or incidents to different fora/committees within the South African Reserve Bank (SARB). The focus areas and the level of detail reported to these fora are often substantially different from the requirements of the PA.

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

1.3 The Bank of International Settlements' Financial Stability Institute (FSI) – in its "*FSI Insight on policy implementation No.2: Regulatory approaches to enhance bank's cyber-security frameworks*"[1] – requires banks to establish a sound governance framework and clear accountabilities with regard to cyber-risk, as IT exposes them to cyber-risk and cyber-attacks.

[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 (including cyber) failures or incidents.

1.5 For the purpose of this Directive:

1.5.1 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 or services to its customers or the entire financial services sector.

1.5.2 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 operational processes. An incident may involve a failure of a feature or service that should have been delivered or some other type of operation failure.

1.5.3 A 'cyber incident'[2] is an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system; the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

1.5.4 An 'information system'[3] is any hardware, software, network or other IT component which is part of an IT infrastructure.

1.6 The purpose of this Directive is to set out the PA's minimum reporting requirements in relation to material IT (including cyber) failures or incidents.

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 implement the reporting requirements set out in this directive in relation to material IT (including cyber) failures or incidents;

2.1.2 establish and maintain robust governance structures to ensure adequate management and operational oversight over critical business functions, resources and infrastructure;

2.1.3 implement a sufficiently robust incident management framework that includes processes and procedures to identify, classify, manage and report system activities;

2.1.4 validate and document how they perform their technology recovery testing of their critical business functions, resources and infrastructures – at least once every calendar year. The recovery time objectives, as defined by the banks, must be validated during this technology recovery testing;

---

[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 notify the PA, as soon as practically possible, but not later than one day following the discovery of a material IT (including cyber) failure or incident;

2.1.6 complete the Material IT (including cyber) failure or incident report form (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

2.1.7 submit a root cause and impact analysis report to the PA – within 14 days or such longer period as the PA may permit – from the discovery of the material IT (including cyber) failure or incident.

3. Invitation for comment

3.1 Banks and all other interested persons are hereby invited to submit their comments in respect of the proposed Directive to: SARB-PA@resbank.co.za, for the attention of Mr J Henning by no later than 31 January 2019.

3.2 All comments received will be published on the PA website, unless a respondent specifically requests confidential treatment.

Kuben Naidoo
Deputy Governor and CEO: Prudential Authority

Date: 7/12/2018

Encl. 1