



South African Reserve Bank
From the Office of
the Registrar of Banks

Ref.: 15/8/2

G4/2017

2017-05-15

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

Guidance Note G4/2017 issued in terms of section 6(5) of the Banks Act 94 of 1990

Cyber resilience

Executive summary

On 29 June 2016 the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) issued guidance on cyber resilience for financial market infrastructures (FMIs).¹

Since cyber risk and cyber resilience is also important to banks, controlling companies and branches of foreign institutions (hereinafter collectively referred to as 'banks') the purpose of this guidance note is to bring to the attention of banks the latest international best practice related to cyber resilience.

This Office will in future, as part of its supervisory review and evaluation process (SREP), assess the adequacy of banks' policies, processes and practices related to cyber risk and cyber resilience, based on, among other things, the practices contained in the aforementioned CPMI-IOSCO guidance document.

1. Introduction

1.1 On 29 June 2016, the CPMI and IOSCO issued guidance on cyber resilience for FMIs.

1.2 The CPMI-IOSCO cyber resilience guidance to FMIs (guidance) highlights the importance of their safe and efficient operation to maintaining and promoting financial stability and economic growth. The level of cyber resilience contributes to operational resilience, which can be a decisive factor in the overall resilience of the financial system and the broader economy.

¹ Available online at www.bis.org/cpmi/publ/d146.htm

- 1.3 The guidance outlines five primary risk management categories and three overarching components that should be addressed across any cyber resilience framework. The risk management categories are: (i) governance; (ii) identification; (iii) protection; (iv) detection; as well as (v) response and recovery. The overarching components are: (i) testing; (ii) situational awareness; as well as (iii) learning and evolving.
- 1.4 Regulation 39 of the Regulations relating to Banks (the Regulations) requires all banks to establish and maintain a robust process of corporate governance that is consistent with the nature, complexity and risk inherent in the bank's on-balance sheet and off-balance sheet activities and that responds to changes in the bank's environment and conditions. This process includes the maintenance of effective risk management and capital management by the bank. In order to achieve the objective relating to the maintenance of effective risk management and capital management, every bank is required to have in place comprehensive risk management processes, practices and procedures, and board-approved policies.
- 1.5 Consequently cyber risk should form part of the enterprise risk management processes, practices and procedures, and board-approved policies of banks.

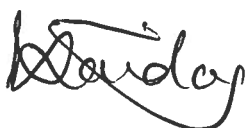
2. Cyber resilience guidance for banks

- 2.1 This Office is of the opinion that the aforementioned principles applied in the risk management categories and overarching components, as set out in the guidance, is also relevant for the banking industry.
- 2.2 As such, banks are requested to assess the adequacy and robustness of their current policies, processes and practices against the CPMI-IOSCO cyber resilience guidance principles.
- 2.3 In this regard, this Office wishes to highlight the following with regard to banks' operations:
- 2.3.1 This Office expects all cyber controls implemented by a bank to follow a risk-based approach that is aligned with the bank's risk appetite, based on the nature and size of its operations.
- 2.3.2 The guidance is principles based and, as such, this Office also expects banks to balance the cost of implementing controls against benefits to be derived. It is therefore not expected that all banks would, for example, have their own full-time security operations centre, incident response team or forensic investigation capability. Banks should however ensure that all the necessary services are either catered for by means of outsourcing/third party agreements or should be available to it in-house without undue delay.
- 2.3.3 The recovery time objectives for a bank should be based on a thorough business impact assessment and take all other relevant legislative and regulatory requirements into consideration. In addition, high availability and failover should be taken into account when designing resilience principles to minimise the impact on customers.

- 2.3.4 With regards to security testing, specifically also referring to penetration testing, when using third parties banks are required to make use of reputable external service providers for such testing which may, for instance, be evidenced through certification or accreditation.
- 2.3.5 This Office does not require banks to join specific information sharing initiatives. However, the bank's situational awareness must include cyber threat intelligence which is applicable to the local market and its operations in South Africa. Participation in a banking sector computer security incident response team is strongly encouraged.
- 2.4 As part of its SREP, this Office will be reviewing banks' policies, processes and practices on a continual basis in order to assess their appropriateness, in line with the practices contained in the aforementioned CPMI-IOSCO document.
- 2.5 Should the outcome of the SREP conducted by this Office be unsatisfactory, this Office may require the relevant bank to strengthen its risk management policies, processes or procedures, or to hold additional capital, calculated in such a manner and subject to such conditions as may be specified in writing, as envisaged in regulation 38(4) of the Regulations.

3. Acknowledgement of receipt

- 3.1 Two additional copies of this guidance note are enclosed for use by your institution's independent 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 this Office at the earliest convenience of the aforementioned signatories.



Kuben Naidoo
Deputy Governor and Registrar of Banks

Date: 17/5/2017

The previous guidance note issued was Guidance Note 3/2017, dated 2 May 2017.