



South African Reserve Bank

From the Office of
the Registrar of Banks

Ref: 15/8/2

G2/2016

2016-02-03

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

Guidance Note 2/2016 issued in terms of section 6(5) of the Banks Act 94 of 1990

Meetings to be held during the 2016 calendar year with the boards of directors of banks and controlling companies

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 during 2016.

A. Meetings with boards of directors

1. Introduction

In order to assist the Office of the Registrar of Banks (this Office) to discharge its supervisory responsibilities, the scope of the meetings with banks' boards of directors (boards) and, in terms of branches of foreign institutions, the executive committees, to be held during the 2016 calendar year, will consist of a discussion on the following two flavour-of-the-year topics:

1.1 IFRS 9: Financial Instruments and

1.2 Cyber security

2. Format of the meetings to be held with banks' boards of directors

All banks' boards will be required to make a presentation and engage in discussions on the above-mentioned flavour-of-the-year topics. The duration for each presentation should be targeted at roughly 45 minutes. It is intended that each presentation should cover only the key elements of the specific topic. This Office also requires to be provided with a copy of each presentation at least three weeks prior to the board or executive committee meeting. The two flavour-of-the-year topics are discussed in greater detail below.

3. IFRS 9: Financial Instruments

3.1 Background

During 2015, discussions with boards of directors and executive committees focused primarily on the planning and governance aspects related to the implementation of International Financial Reporting Standard (IFRS) 9. As communicated in this Office's Guidance Note 2 of 2015, the 2016 discussions with banks' boards and executive committees will continue to focus on the implementation of IFRS 9, with emphasis being placed again on the processes followed by banks, the impact analysis and post-implementation maintenance procedures to be adopted in preparing their financial accounting systems and oversight practices for reporting under IFRS 9, once the standard is effective in 2018.

Following the issuance of IFRS 9 by the International Accounting Standards Board, the Basel Committee on Banking Supervision (BCBS) issued a document titled 'Guidance on credit risk accounting for expected credit losses'¹ in December 2015 with the objective of setting out supervisory requirements on sound credit risk practices associated with the implementation and ongoing application of expected credit loss accounting frameworks. Such practices include all aspects of a bank's procedures for managing credit risk. It is expected that this guidance will significantly influence the manner in which banks manage credit risk and account for expected credit losses.

3.2 Format of discussion

The chairperson of either the capital and risk management subcommittee or the audit subcommittee (or equivalent) will be required to make a presentation to this Office, focusing on the progress made to date, impact of the standard and steps to be taken to ensure continued application and monitoring of the standard, specifically the credit impairment aspects, at both the bank solo and consolidated levels. The discussion should include, but not be limited to, the following:

3.2.1 Planning

- a. Progress made since initial discussions with management as part of the 2015 flavour-of-the-year discussions;
- b. Implementation readiness (this should include milestones reached and still to be achieved, gaps identified, challenges encountered, including plans to overcome such);
- c. The bank's interpretation of key terminology used in the standard e.g. significant increase in credit risk;
- d. Initial qualitative and quantitative impact assessment (including impact on credit practices, impairments by portfolio, earnings and capital adequacy);
- e. Impact of the BCBS's 'Guidance on credit risk and accounting for expected credit losses';
- f. Extent of involvement of internal and external audit both pre- and post-implementation;

¹ <http://www.bis.org/bcbs/publ/d350.pdf>

3.2.2 Post-implementation considerations

- g. Process(es) to be adopted to ensure continued application and monitoring of the standard; and
- h. Management's planned methodology and governance processes with regard to setting the bank's ongoing internal view of the macroeconomic outlook, including how this would be incorporated into the impairment methodology and the frequency thereof.

4. Cyber security

4.1 Background

The term 'cyber' refers to anything relating to or characteristic of the culture of computers, information technology and virtual reality. Cybercrime, which refers to any criminal activity carried out by means of computers or the internet, has been increasingly raised as a key concern in recent years within various industries, including financial services. Even governments have been stepping up their cyber vigilance in light of greater nation-state activities. Commensurate with growth in concern over the increased cyber threat has been the increased attention that regulatory bodies at a global level have been paying to cyber resilience.

This Office has previously included, and will continue to include, information security, including cyber security, in its supervisory programme. During earlier interactions, banks indicated that they have made concerted efforts into strengthening their cyber risk management processes as well as solidifying their cyber defence and response capabilities.

This Office would like to emphasise that IT governance and more specifically cyber security governance, as part of information security, is regarded as an integral and on-going element of banks' risk management processes. The board of directors consequently retains the ultimate accountability for ensuring that a bank identifies and manages its cyber threat landscape.

4.2 Format of discussion

The chairperson of the capital and risk management subcommittee (or equivalent) is required to make a presentation to this Office on the bank's governance and risk practices around cyber security. The following aspects, in relation to the involvement of the board, should be covered during the presentation:

- a. How the board ensures that it has the necessary awareness, knowledge and understanding in order to be able to provide oversight of cyber security and any possible impact on strategy;
- b. The frequency of cyber security discussions at the board or board subcommittee meetings and the topics/content covered during those sessions;
- c. The bank's approach to managing cyber security and its inclusion and integration in the bank's enterprise risk management framework;

- d. An overview of the bank's primary cyber security governance structures;
- e. Recent initiatives to bolster cyber defences and future plans;
- f. The bank's approach in addressing the shortage of cyber security skills, creating awareness with customers and employees and the availability of an adequate budget;
- g. How the board is addressing the legal implications of cyber risks and what considerations have been made with regard to cyber insurance;
- h. The bank's approach to managing cyber risks that are introduced through outsourcing and third party service provider arrangements; and
- i. The bank's approach in sharing of threat intelligence within the banking industry as well as the board's views in terms of the interaction with the proposed government cyber structures, such as the Cyber Hub.

B. Acknowledgement of receipt

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.



René van Wyk
Registrar of Banks

The previous guidance note issued was Guidance Note 1/2016, dated 2 February 2016.