FSCA
Financial Sector
Conduct Authority

SOUTH AFRICAN RESERVE BANK
Prudential Authority

Statement* of the need for, intended operation and expected impact of the proposed Joint Standard on information technology governance and risk management

As initially published in June 2021 and minor revisions made in April 2022

*This statement is prepared and published in accordance with and in fulfilment of the requirements under sections 98(1) and 103 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)

Table of Contents

1. Introduction

1.1 Information Technology (IT) risks can pose significant adverse technology failures to financial institutions, potentially compromising their viability. For this reason, IT governance and risk management are fundamental for a financial institution to achieve its strategic, corporate, operational, and reputational objectives.

1.2 The introduction of the fourth industrial revolution further changed how financial institutions interact with their customers, increasingly deploying more advanced technology and online systems. Financial institutions are also faced with the challenge of keeping pace with the needs and preferences of their customers who are embracing financial innovation as well as the improved use of technology in the delivery of financial products and services.

1.3 Digitisation, digitalisation and other emerging technologies have promoted IT to become an integral part of the business enablement of strategies including the ability to incorporate customer needs. Technologically enabled financial innovation has also resulted in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services. These developments have also led to an increased change in the nature and scope of risks in the financial sector. Such risks include strategic risk, operational risk, cyber-risk and compliance risk.

1.4 The advancement of IT requires financial institutions to fully understand the magnitude and intensification of IT risks from these developments. In this regard, financial institutions must put in place adequate and robust risk management systems as well as operating processes to ensure that they appropriately identify, manage and monitor IT risks.

2. Statement of the need for the Joint Standard

2.1 In order for the Prudential Authority (PA) and the Financial Sector Conduct Authority (FSCA) (jointly referred to as the Authorities) to achieve their respective objectives, the Financial Sector Regulation Act 9 of 2017 (FSR Act) provides for

the Authorities to make risk management and internal control requirements in addition to other matters specified, that apply to financial institutions.

2.2 Information Technology is at the centre of many financial institutions concerning how they conduct their business and deliver financial products and services to their customers. When critical systems fail and customers cannot access financial products and services, the business operations of a financial institution may immediately come to a standstill.

2.3 The impact on customers would be immediate, with significant consequences to the financial institution, including reputational damage, regulatory breaches, and revenue and business losses.

2.4 Also, given the role played by the financial sector in the economy, offering access to the payment system, transformation of assets, and managing risks, such disruptions can have additional consequences on the broader economy.

2.5 In light of the above, there is a need for financial institutions and supervisors to be vigilant and monitor practices and risks that might inhibit beneficial innovations in the financial sector. It is important that financial institutions put in place robust IT risk management frameworks to manage IT risks ensuring that they have effective governance structures and risk management processes that appropriately identify, manage and monitor IT risks.

2.6 As a result, there is a need to provide an appropriate and comprehensive regulatory framework governing IT risk management from both a prudential and conduct perspective.

2.7 It is against this background that the proposed Joint Standard on information technology governance and risk management has been drafted and published for public consultation.

3. The objectives of the proposed Joint Standard

3.1 The proposed Joint Standard sets out the IT risk management principles that financial institutions must comply with for achieving sound practices and processes in managing IT risks.

3.2 The proposed Joint Standard seeks to address the following:

- ensure that financial institutions have established a sound and robust IT risk management framework;
- assist financial institutions in integrating technology risk management into their overall management system; and
- ensure that oversight of IT risk management is incorporated into the governance and risk management structures, processes and procedures of a financial institution.

4. Statement of the expected impact of the Joint Standard

4.1 Commentators raised concerns that the cost of compliance with the Joint Standard may be relatively low to moderate, however when aggregated together with the overall cost of compliance and governance, may result in increased pressure on the economic viability of small to medium enterprises. The need for additional staff with the requisite skills has also been identified.

4.2 The requirements in the Joint Standard were considered in light of the impact and considering the cost of compliance. The Authorities remain of the view that the risk of inadequate IT Risk Management framework and strategy may have dire consequences on the entire operation of the financial institution especially as the financial sector operates in a highly digitalised environment.

4.3 The Authorities are of the view that it is critical to ensure that regulatory requirements do not place an undue regulatory burden and/or barriers to entry in respect of smaller financial institutions. However, it is equally critical to ensure that regulatory requirements mitigate the relevant risks and an appropriate balance in this regard must therefore be struck.

4.4 In practice, the FSCA and PA will adopt a risk-based approach to supervision of the Joint Standard, which means that focus and regulatory interventions will be commensurate to the risks and impact that entities pose to the financial sector. The FSCA and PA may also support compliance with the Joint Standard, helping especially smaller entities to understand their regulatory obligations, by providing additional regulatory guidance through for example a Guidance Notice. In an

attempt to strike this balance, the proposed requirements facilitate the proportional application of the Joint Standard and provide that the requirements must be implemented in accordance with the risk appetite, nature, size and complexity of a financial institution.

4.5 As an additional mechanism to facilitate proportionality, for example, if there are still instances where a specific requirement is too onerous on a small financial institution despite the application of the aforementioned principle of proportionality, an exemption from a specific requirement of the Joint Standard might be considered. However, the Authorities are mindful of not "regulating by exemption" and so this option may only be used in limited circumstances.

5. Statement on the intended operation of the Joint Standard

5.1 The proposed Joint Standard will apply to:

- a bank, a branch[1], a branch of a bank, or a bank controlling company (banks) registered under the Banks Act 94 of 1990;
- mutual banks registered under the Mutual Banks Act 24 of 1993;
- insurers and controlling companies of insurance groups (insurers) licensed under the Insurance Act 18 of 2017;
- market infrastructures licensed under the Financial Markets Act 19 of 2012;
- managers of collective investment schemes licensed under the Collective Investment Scheme Control Act 45 of 2002;
- a discretionary FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPS,2003; and
- an administrative FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPS, 2003.

5.2 Financial institutions are expected to implement IT controls that are commensurate with their risk appetite, based on the nature and size of the financial institution's operations.

[1] Commonly referred to as a 'branch of a foreign institution'.

5.3 The Authorities will in future, as part of their supervisory programmes, review and assess the adequacy of financial institution's policies, processes, and practices related to IT risk concerning financial institutions covered in terms of this proposed Joint Standard as well as the financial institutions not covered by the Joint Standard. Appropriate and proportionate regulatory instruments and/or guidance on IT risk management will be developed for co-operative financial institutions, co-operative banks, and micro-insurers in the future.

5.4 In terms of the commencement date of the Joint Standard, the Authorities agree with the requests for a revised date. Accordingly, the Standard becomes effective 12 months after the date of publication for financial institutions to prepare for compliance with the Joint Standard:

6. Conclusion

Following the consultation process, the draft Joint Standard and the accompanying documents will be submitted to Parliament for at least 30 days while it is in session before the Joint Standard is subsequently made.