

Statement of the need for, intended operation and expected impact of the proposed Joint Standard on cybersecurity and cyber resilience requirements for financial institutions

(Draft for Consultation)

December 2021

Table of Contents

| | |
|--|----|
| 1. Introduction..... | 2 |
| 2. Background..... | 3 |
| 3. Statement of the need for the Joint Standard..... | 4 |
| 4. The objectives of the proposed Joint Standard | 6 |
| 5. Statement of the expected impact of the Joint Standard..... | 7 |
| 6. Statement on the intended operation of the Joint Standard | 8 |
| 7. Way forward..... | 10 |

1. Introduction

- 1.1. The Prudential Authority (PA) has the mandate to promote and enhance the safety, and soundness of regulated financial institutions and market infrastructures. The Financial Sector Conduct Authority (FSCA) has a responsibility to enhance and support the efficiency and market integrity of financial markets as well as protect financial customers. Both the PA and the FSCA (jointly referred to as Authorities) have a responsibility to assist the South African Reserve Bank (SARB) in maintaining financial stability.
- 1.2. Section 107 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) (FSR Act) empowers the Authorities to make joint standards on any matter in respect of which either of them has the power to make a standard.
- 1.3. Under section 108(1) of the FSR Act, the Authorities may make standards on specified additional matters, including risk management and internal control requirements, and reporting by financial institutions.
- 1.4. Before making a regulatory instrument i.e., joint standard, in terms of section 98 of the FSR Act, the Authorities are required to publish the following documents:
 - (i) a draft of the joint standard;
 - (ii) a statement explaining the need for and the intended operation of the joint standard;
 - (iii) a statement of the expected impact of the joint standard; and
 - (iv) a notice inviting submissions concerning the joint standard, stating where, how and by when submissions are to be made.
- 1.5. To commence industry engagements in order to finalise on some of the above-mentioned legislative requirements for making regulatory instruments, the Authorities have prepared this 'Statement of the need for, intended operation and expected impact of the proposed joint standard on cybersecurity and cyber resilience requirements for financial institutions' (Statement).
- 1.6. The Statement is intended to communicate to the identified financial institutions, the policy context, intended outcomes and expected impact of the proposed Joint Standard.

- 1.7. This Statement will be published together with the proposed Joint Standard on Cybersecurity and cyber resilience requirements for financial institutions (proposed Joint Standard) for industry consultation.
- 1.8. The proposed Joint Standard sets out the requirements for sound practices and processes of cybersecurity and cyber resilience for financial institutions.

2. Background

- 2.1 The introduction of the fourth industrial revolution has transformed how financial institutions interact with their customers, increasingly deploying more advanced technology and online systems. Financial institutions are confronted with the challenge of keeping pace with the needs and preferences of their customers who are embracing financial modernisation as well as the improved use of technology in the delivery of financial products and services.
- 2.2 While technological advancement has brought with it numerous benefits, however, as technology advances, the threat landscape also evolves.
- 2.3 The biggest challenge to every institution today is the frequency and sophistication of targeted cyber-attacks, with perpetrators continually refining their efforts to compromise systems, networks, and information, worldwide. Cyber-attacks have been targeted at critical infrastructure and strategic industry sectors such as the financial sector.
- 2.4 The financial sector is one of the more prominent targets for attacks. Given the growth of the threat landscape, cybersecurity risk has gained the necessary attention in the financial sector as well as the Authorities. If these threats are not properly mitigated and managed, cybersecurity risk could trigger a breakdown in systems that keep financial institutions functioning.
- 2.5 The World Economic Forum (WEF) in its 16th edition of The Global Risks Report¹ has noted that cybersecurity risk failure is among the highest likelihood risks of the next ten years that also include extreme weather, climate action failure and human-led environmental damage among others. The WEF has also previously noted, in 2018, that cybersecurity risks were growing, both in their prevalence and in their

¹ World Economic Forum, The Global Risks Report, 16th Edition (January 2021), available at https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

disruptive potential, accompanied by rising financial impact². According to the WEF, attacks against businesses have been on the rise over the years, and incidents that would once have been considered extraordinary are becoming more and more common.

3. Statement of the need for the Joint Standard

3.1 According to a Newsletter on cybersecurity³ published by the Basel Committee on Banking Supervision (BCBS), cyber threats and incidents, have emerged as a growing concern for the banking sector over the past several years, posing risks to the safety and soundness of individual banks and the stability of the financial system. This has been reiterated by the Financial Stability Board⁴ (FSB) which has also pointed out that cyber incidents pose a threat to the stability of the global financial system. According to the FSB, in recent years, there have been several cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate.

3.2 According to the BCBS, the financial sector faces significant exposure to cyber risk given that it is information technology-intensive and highly interconnected through payment systems. Since the onset of the Covid-19 pandemic, these concerns have heightened, and they have also been exacerbated by remote working arrangements which have further increased the provision of financial services using digital channels. This has enlarged banks' attack surfaces and given more points of access to their systems.

3.3 Financial institutions need to strengthen the ability to continue to carry out their activities by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

3.4 In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) jointly issued guidance on cyber resilience for financial market infrastructures⁵. According

² World Economic Forum, The Global Risks Report, 13th Edition (January 2018), available at https://www3.weforum.org/docs/WEF_GRR18_Report.pdf

³ https://www.bis.org/publ/bcbs_ni25.htm

⁴ Financial Stability Board, Effective Practices for Cyber Incident Response and Recovery, (October 2020) available at <https://www.fsb.org/wp-content/uploads/P191020-1.pdf>

⁵ CPMI and IOSCO, Guidance on cyber resilience for financial market infrastructures, (June 2016), available at <https://www.bis.org/cpmi/publ/d146.pdf>

to the CPMI and IOSCO, the level of cyber resilience, which contributes to a financial market infrastructure's operational resilience can be a decisive factor in the overall resilience of the financial system and the broader economy. The safe and efficient operation of financial market infrastructures must be guarded to maintain and promote financial stability and economic growth. If this is threatened by lax cybersecurity measures, financial market infrastructures can be sources of financial shocks.

- 3.5 The International Association of Insurance Supervisors (IAIS) in its Issues Paper on cyber risk to the insurance sector in 2016,⁶ raised concern over the growing cybersecurity risk across all sectors of the global economy. The IAIS pointed out that cyber risks have grown, and cyber criminals have become increasingly sophisticated.
- 3.6 The IAIS also warned that cybersecurity incidents can harm the ability of insurers to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector.
- 3.7 Regardless of the size of the IAIS members across different jurisdictions, given the growing frequency and severity of cybersecurity incidents, the IAIS has stressed that cyber resilience must be achieved by all insurers.
- 3.8 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, or data integrity is compromised, the business operations of a financial institution may immediately come to a halt.
- 3.9 Cyber-attacks can pose a major impact on financial institutions, potentially compromising their sustainability. Due to the interconnectedness of the financial system, a cyber incident or failure at one interconnected entity may not only impact the safety and soundness of that entity but other financial institutions as well, with potentially systemic consequences.

⁶ <https://www.iaisweb.org/page/events/stakeholder-meetings/previous-meetings/file/61254/cybersecurity-issue-paper-post-public-consultation-clean/>

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

3.11 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 to the financial sector can have additional consequences to the broader economy.

3.12 In light of the above, there is a need for the Authorities to provide an appropriate and comprehensive regulatory framework for managing cyber risks from both a prudential and conduct perspective. It is against this background that the proposed Joint Standard on cybersecurity and cyber resilience requirements has been drafted and is being released for consultation with the industry.

3.13 The advancement of the threat landscape requires financial institutions to fully understand the extent and intensification of cyber risks. In this regard, financial institutions must put in place adequate and robust processes for managing cyber risk.

3.14 Furthermore, cyber resilience capabilities must be established to ensure the ability of financial institutions to continue to carry out their operations by anticipating and adapting to cyber threats and other relevant changes in the environment as well as by withstanding, containing and rapidly recovering from cyber incidents.

3.15 It has been noted that organisations that have a comprehensive cybersecurity strategy, that is governed by best practices, and are aided by advanced technologies are likely to fight cyber-attacks more effectively and can reduce the lifecycle and consequently the impact of cyber-attacks when they occur.

4. The objectives of the proposed Joint Standard

4.1 Financial institutions must have adequate cybersecurity and cyber resilience measures. The proposed Joint Standard sets out the requirements for sound practices and processes of cybersecurity and cyber resilience for financial institutions.

4.2 At a high level, the proposed Joint Standard seeks to:

- ensure that financial institutions establish sound and robust processes for managing cyber risks.
- promote the adoption of cybersecurity fundamental and hygiene practices to preserve confidentiality, integrity and availability of data and information technology systems;
- ensure that financial institutions undertake systematic testing and assurance regarding the effectiveness of their security controls;
- ensure that financial institutions establish and maintain cyber resilience capability, to be adequately prepared to deal with cyber threats; and
- provide for notification of material cyber incidents by the regulated entities to the Authorities.

5. Statement of the expected impact of the Joint Standard

5.1 Under this section of the Statement, the impact, benefits, and areas of concern regarding the proposed Joint Standard are analysed and considered.

5.2 While it is expected that the proposed Joint Standard will place an additional administrative burden on the financial institutions affected by the proposed Joint Standard, however, at this stage, the Authorities cannot ascertain the full extent of the expected impact or any other unintended consequences.

5.3 As part of the consultation process, the Authorities have also prepared a set of questions to solicit industry inputs on the expected impact of implementing the proposed Joint Standard. The responses to Section C of the Comments matrix, in particular, will be used to ascertain the expected impact or any other unintended consequences of the proposed Joint Standard.

5.4 Information relating to the expected impact is important to assist the Authorities to determine the extent to which the requirements can or should be applied in the context of small to medium-sized financial institutions. 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.

- 5.5 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.
- 5.6 As an additional mechanism to facilitate proportionality, e.g., 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.
- 5.7 Specific input on the scope of the Joint Standard (see paragraph 6.1 below) and the issue of proportionality is also being requested.
- 5.8 Subsequent to this consultation process, a revised Statement will be prepared, taking into account the feedback that will be received from the industry.
- 5.9 Interested stakeholders are encouraged to respond to the questions under Section C of the Comments template as well as identify any potential risks or unintended consequences that might arise from the implementation of the proposed Joint Standard and submit those to the Authorities as part of this consultation process.
- 5.10 It is envisaged that the proposed Joint Standard will lead to sound practices and processes for cybersecurity and cyber resilience for financial institutions as well as improved outcomes for customers due to reduced cyber-attacks and better protection of their personal information.

6. Statement on the intended operation of the Joint Standard

- 6.1 The proposed Joint Standard will apply to all:
- banks, branches of foreign institutions, branches of a bank and controlling companies as respectively defined section 1 of the Banks Act 94 of 1990;
 - mutual banks registered under the Mutual Banks Act 24 of 1993;
 - insurers and controlling companies as defined 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;

- an administrative FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPS, 2003;
- pension funds licensed under the Pensions Funds Act 24 of 1956; and
- an over-the-counter (OTC) derivative provider as defined in the Financial Markets Act Regulations.

6.2 Financial institutions are expected to implement security controls that are commensurate with their risk appetite, based on the nature and size of the financial operations.

6.3 It is the responsibility of the governing body of a financial institution to ensure that the financial institution meets the requirements set out in the proposed Joint Standard.

6.4 For the avoidance of doubt, a financial institution that is a bank, or a controlling company must ensure that any potential risks relating to cybersecurity and cyber resilience from juristic persons and branches structured under the bank or the controlling company, including all relevant subsidiaries approved in terms of section 52 of the Banks Act 94 of 1990 are catered for and mitigated in the application of the requirements of this Joint Standard.

6.5 In addition, a financial institution that is the controlling company of an insurance group must ensure that any potential risks relating to cybersecurity and cyber resilience from the insurance group designated under section 10 of the Insurance Act 18 of 2017 are catered for and mitigated in the application of the requirements of this Joint Standard.

6.6 The Authorities will in the future, as part of their supervisory programs, review and assess the adequacy of financial institutions' policies, processes, and practices related to cybersecurity and cyber resilience.

6.7 Appropriate and proportionate regulatory instruments and/or guidance on cybersecurity and cyber resilience will be considered for co-operative financial institutions and cooperative banks, in the future.

6.8 The Authorities will continuously assess and evaluate the effectiveness of the Joint Standard to ensure that any unintended consequences of the draft Joint Standard on the industry are adequately addressed.

6.9 The Authorities will also develop a reporting framework and data obtained through that process will be used as an offsite supervisory tool to identify risks and trends specific to a particular category of supervised entities and for benchmarking purposes across the financial sector.

7. Way forward

7.1 The draft Joint Standard and this Statement are prepared and published for consultation with the industry.

7.2 Following the consultation process, the Authorities will make any necessary changes to the draft Joint Standard and this Statement to better reflect the expected impact of the draft Joint Standard based on the submissions received under Section C of the Comments template. After the conclusion of the consultation process, the revised proposed Joint Standard and Statement will be released for another round of public comment and consultation, for a period of at least six weeks.

7.3 After the conclusion of the aforementioned process, the updated proposed Joint Standard and the accompanying documents will either be submitted to Parliament for a period of at least 30 days while Parliament is in session or, depending on the materiality of any such changes, publish the draft Joint Standard for a third round of public comment and consultation before the Joint Standard can be made.

7.4 Written submissions on this Statement and proposed Joint Standard may be sent via e-mail to PA-Standards@resbank.co.za for the attention of Mrs Kalai Naidoo or Mr Andile Mjadu, on or before 15 February 2022.