FSCA
Financial Sector
Conduct Authority

South African Reserve Bank
Prudential Authority

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

(Draft for Consultation)

Initially published in December 2021 and updated in November 2022

Table of Contents

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 integrity of financial markets, as well as to protect financial customers. Both the PA and the FSCA (jointly referred to as the 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., a 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. In this light, the Authorities have prepared this “Statement of the need for, expected impact and intended operation of the proposed joint standard on cybersecurity and cyber resilience requirements for financial institutions” (Statement).

1.6. The Statement is intended to communicate the policy context, intended outcomes and expected impact of the proposed Joint Standard.

1.7. This Statement is being 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, which increasingly deploy 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 worldwide continually refining their efforts to compromise systems, networks and information. 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 of the financial sector, as well as that of the Authorities. If these growing threats are not properly mitigated and managed, cybersecurity breaches could trigger a breakdown in systems that keep financial institutions functioning.

2.5 In its 16th edition of The Global Risks Report[1], the World Economic Forum (WEF) has noted that cybersecurity risk failure is among the highest risks of the next ten years; other risks 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 disruptive potential, accompanied by rising financial impact[2]. According to the WEF, attacks

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

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 cybersecurity[3] 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 Board[4] (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 an information technology (IT) intensive sector that is also highly interconnected through payment systems. Since the onset of the Covid-19 pandemic, these concerns have heightened, and have also been exacerbated by remote working arrangements which have further increased the provision of financial services using digital channels. This has enlarged the attack surfaces of banks and added 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 infrastructures[5]. According to the CPMI and IOSCO, the level of cyber resilience, which contributes to the operational resilience of a financial market infrastructure can be a decisive factor in the overall resilience of the financial system and the broader economy. The safety

[3] https://www.bis.org/publ/bcbs_nl25.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

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 risks 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 stressed the importance of cyber resilience to 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.

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.

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

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 on the broader economy.

3.12 South Africa has seen a rising number of cyber incidents. Recent cyber incidences have impacted a range of providers such as fund investment administrators, market infrastructures, insurers and banks. Although the impact cannot be quantified, the "cost factor" is extensive and demonstrated in inability to timeously price assets; provide fund valuation; and settlements. Therefore, the interconnectedness of the South African financial ecosystem and impact on the various sectors within the value chain, strengthens the need for this Joint Standard.

3.13 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.

3.14 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 risks.

3.15 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.

3.16 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 fundamentals and hygiene practices to preserve confidentiality, integrity and availability of data and IT 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 by the regulated entities of material cyber incidents to the Authorities.

5. Statement of the expected impact of the Joint Standard

5.1 As part of the consultation process, the Authorities prepared a set of questions to solicit industry input on the expected impact of the proposed Joint Standard. Interested stakeholders were requested 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. The comments received were used to ascertain the expected impact or any other unintended consequences of the proposed Joint Standard. A total of 5 industry bodies and associations as well as 31 supervised entities and organisations provided comments.

5.2 An analysis of the comments indicated that while it is expected that the proposed Joint Standard will place an additional administrative burden, particularly on the smaller industry players, the draft Joint Standard was welcomed by the majority of the supervised entities and industry bodies.

5.3 The respondents indicated that the proposed Joint Standard would provide a benchmark for the approach to cybersecurity and strengthen the management of cybersecurity risk. In addition, it was indicated that the Joint Standard would ensure consistency in the management of cybersecurity risks across the board, through enhanced and standardised cybersecurity requirements, which would enhance the

protection of financial customers and improve the overall resilience of the financial services ecosystem.

5.4 Majority of the respondents indicated that the controls contained in the proposed Joint Standard are based on the industry best practices already in place and therefore compliance will not present a huge challenge for most of the supervised entities, particularly the larger financial institutions. While the requirements contained in the draft Joint Standard are similar to the current security controls in place, particularly for many larger players, some areas would require enhancements. To allow ample time for the enhancements of the security controls, the Authorities have provided for a 12-month transitional period following the publication of the Joint Standard. This transitional period would provide the industry with an opportune time to remediate existing gaps and implement necessary enhancements to fully comply with the requirements of the Joint Standard.

5.5 While 30 out of the 36 respondents confirmed that the implementation of the proposed Joint Standard will lead to additional costs, they also generally indicated that they did not expect that these would be significant, particularly for larger financial institutions. Though some had not conducted a detailed gap assessment to ascertain the exact additional costs, it was indicated that how the Authorities envisaged implementing and assessing compliance with the Joint Standard would impact the level of the expected costs.

5.6 The set-up cost as a percentage of the total average annual operating cost for the last three years for the six financial institutions that provided their expected set-up costs ranged between 1% and 6.6%. The weighted average set-up cost for these institutions accounted for 2.3% of the average annual operating costs for the last three financial years. However, the set-up costs will be once-off. The recurring cost of maintenance of the IT systems and ongoing compliance with the Joint Standard was estimated to range between 1.5% and 4.4% of the average annual operating cost incurred in the last three years. This is for the four entities that provided this information. This translated to an annual weighted average of 2.9%. The majority of the respondents indicated that they had not conducted a detailed gap assessment to determine the cost implication of the proposed Joint Standard.

5.7 One of the key considerations raised by particularly the smaller entities is the lack of resources and skills to implement the proposed Joint Standard. This also applies to Category I FSPs by extension. According to the responses received, the Joint

Standard sets a high baseline for smaller institutions which on its own has cost and capacity implications as smaller institutions would need to contract with IT security firms or IT infrastructure to ensure compliance with the Joint Standard. The Authorities do acknowledge this concern and have sought to address it by ensuring that the minimum requirements and principles set out in the Joint Standard must be implemented in a proportional manner that reflects the nature, size, complexity, and risk profile of a financial institution[7].

5.8 During the consultation process, an argument was made for bringing into the scope of the proposed Joint Standard, pension fund administrators licensed in terms of the Pension Funds Act. This was in light of the governance and operational structures of pension funds. Where a pension fund uses a third-party administrator, the IT systems belong to the administrator. The exception would be for pension funds that do not outsource the administration of the funds and have developed internal capacity for this.

5.9 Furthermore, the implementation of the relevant requirements contained in the Joint Standard will also be assessed in consideration of the nature, size, complexity and risk profile of a financial institution. In light of this, the expectation is that the costs that will be incurred by the smaller institutions will be commensurate with their size. The Authorities also note that smaller non-systemic institutions would not have the same control environment compared to larger financial institutions. Supervisory discretion will be applied during compliance assessments and the Authorities will also be monitoring any unintended consequences as the Joint Standard is implemented.

5.10 As much as 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, it is equally critical to ensure that regulatory requirements mitigate the relevant risks and an appropriate balance in this regard must therefore be achieved.

5.11 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.

[7] Refer to clauses 3.4 and 3.5 of the draft Joint Standard.

5.12 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, on application.

5.13 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 financial customers due to reduced cyber-attacks and better protection of their personal information.

5.14 It is the view of the Authorities that the unintended consequences, as well as the concerns that have been raised by the industry that have implications on the costs, have been addressed sufficiently in the Joint Standard. The Joint Standard seeks to reduce cyber risks and the potential of losses (which can be significant) as a result of weaknesses in cybersecurity and cyber resilience. The Authorities assess that the benefits that would accrue to the financial ecosystem through the implementation of the proposed Joint Standard would outweigh the costs that will be incurred in implementing the Joint Standard.

5.15 When the proposed Joint Standard was published for the informal consultation process, the credit rating agencies, benefit administrators and Cat I FSP's that provide investment fund administration services, were not covered under the scope of the proposed Joint Standard. The Authorities would be interested to receive comments from the above entities regarding any expected impact or unintended consequences that might be posed by the proposed Joint Standard.

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 in 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;
- a Category I FSP as contemplated in section 3(a) of the Determination of Fit and Proper Requirements for Financial Services Providers, 2017, that provides investment fund administration services;
- 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;
- an over-the-counter (OTC) derivative provider as defined in the Financial Markets Act Regulations;
- an administrator approved in terms of section 13B of the Pension Funds Act, 1956 (Act No 24 of 1956); and
- a registered credit rating agency as defined in section 1 of the Credit Rating Services Act, 2012 (Act No 24 of 2012).

6.2 Financial institutions are expected to implement security controls that are commensurate with their risk appetite, based on the nature, complexity, risk profile 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 an insurer or a controlling company of an insurance group must ensure that any potential risks relating to cybersecurity and cyber resilience from juristic persons under the insurer or 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, microinsurers 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 to 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 in terms of Section 98 of the FSR Act, for public comment and consultation for a period of six weeks.

7.2 This Statement covers the rationale for the proposed Joint Standard, the expected impact as well as the intended operation of the proposed Joint Standard. The Statement also takes into account all the responses that were received through the questionnaire published in December 2021.

7.3 Following the consultation process, the Authorities will make any necessary changes to the draft Joint Standard and this Statement, taking into account all submissions received. 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 the third round of public comment and consultation before the Joint Standard can be made.

7.4 The submission to Parliament will only be made if the decision by the Authorities is to proceed and after taking into consideration all the comments received.

7.5 Written submissions on this Statement and the proposed Joint Standard may be sent via e-mail to FSCA.RFDStandards@fsca.co.za for the attention of Mr Andile Mjadu and PA-Standards@resbank.co.za for the attention of Ms Kalai Naidoo, on or before 28 February 2023.