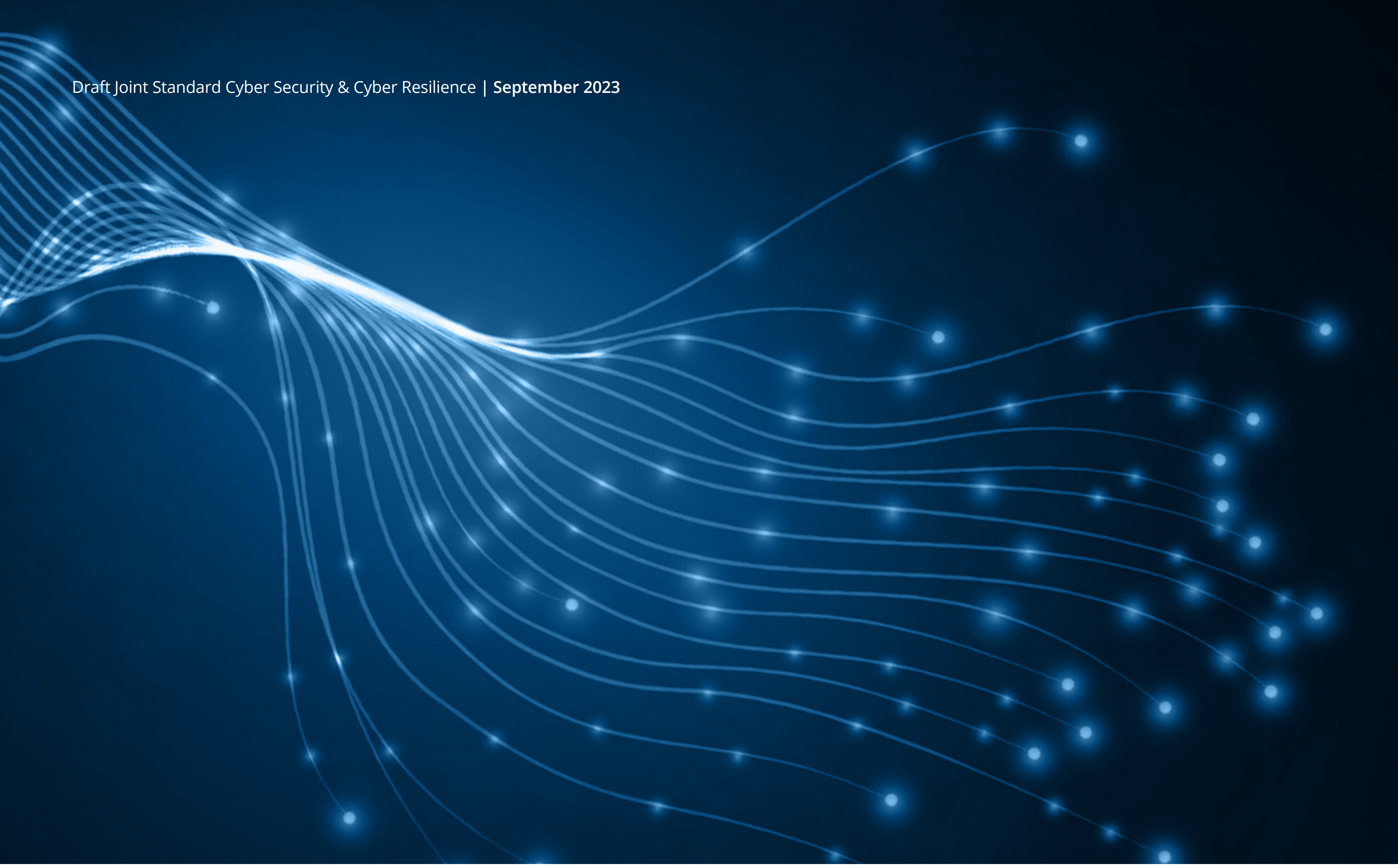
Deloitte.

September 2023

Draft Joint Standard
Cyber Security & Cyber Resilience

The Prudential Authority (PA) is mandated 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.

- The Joint Standard: Cyber Security and Cyber Resilience sets out the minimum requirements for sound practices and processes of Cyber Security and Cyber Resilience.
- It is the responsibility of the governing body of a financial institution to ensure that the financial institution meets the requirements set out in this Joint Standard on a continual basis.
- This Joint Standard addresses requirements relating to governance, Cyber Security strategy and framework, Cyber Security and Cyber Resilience fundamentals, Cyber Security hygiene practices, as well as regulatory reporting.



Legislative Authority and Applicability

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 have the power to make a standard.

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.

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:
- A draft of the joint standard;
- A statement explaining the need for and the intended operation of the joint standard;
- A statement of the expected impact of the joint standard;
- A notice inviting submissions concerning the joint standard, stating where, how, and by when submissions are to be made.

This Joint Standard is made under section 107 read with sections 105, 106 and 108 of the Financial Sector Regulation Act 2017.

The authoritative body referenced in the Joint Standard refers to the PA as established in terms of section 32 of the Act and the FSCA as established in terms of section 56 of the Act.
It is the responsibility of the governing body of a financial institution to ensure that the financial institution meets the requirements set out in this Joint Standard on a continual basis.

Governing body refers (FSR Act 2017): in relation to a financial institution, a person or body of persons, whether elected or not, that manages, controls, formulates the policy and strategy of the financial institution, directs its affairs or has the authority to exercise the powers and perform the functions of the financial institution, and includes:
- The general partner of an en commandite partnership or the partners of any other partnership;
- The members of a close corporation;
- The trustees of a trust;
- The board of directors of a company; and
- The board of a pension fund referred to in section 7A of the Pension Funds Act.

Financial institution refers (FSR Act 2017):
- A bank, a branch, a branch of a bank and a controlling company as respectively defined section 1 of the Banks Act, 1990 (Act No. 94 of 1990);
- A mutual bank as defined in section 1 of the Mutual Banks Act, 1993 (Act No. 24 of 1993);
- An insurer and a controlling company as defined in section 1 of the Insurance Act, 2017 (Act No. 18 of 2017);
- A manager as defined in section 1 of the Collective Investment Scheme Control Act, 2002 (Act No. 45 of 2002);
- A market infrastructure as defined in section 1 of the Financial Markets Act 2012 (Act No. 19 of 2012);
- A discretionary FSP as defined in Chapter II of the Notice on Codes of Conduct for Administrative and Discretionary FSPs, 2003;
- An administrative FSP as defined in Chapter I of the Notice on Codes of Conduct for Administrative and Discretionary FSPs, 2003;
- A pension fund registered under the Pension Funds Act, 1956 (Act No. 24 of 1956); and
- An Over-The-Counter (OTC) derivative provider as defined in the Financial Markets Act Regulations;
- 'FSP' means a financial services provider as defined in section 1 of the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002)No. 37 of 2002).

Statement of Need

1. Authorities have prepared the "Statement of the need for, expected impact and intended operation of the proposed Joint Standard on Cyber Security and Cyber Resilience requirements for financial institutions."

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

3. This Statement was published in conjunction with the proposed Joint Standard on Cyber Security and Cyber Resilience requirements for financial institutions (proposed Joint Standard) for industry consultation.

The Need

4th Industrial Revolution

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.

Evolving Customer Preferences

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.

Dynamic Threat Landscape

Rapidly changing technology and associated threat landscapes. Increased frequency and sophistication of targeted cyber-attacks. Given the growth of the threat landscape, Cyber Security risk has gained the necessary attention of the financial sector, as well as that of the Authorities.

Rising Threat

According to a Newsletter on Cyber Security, 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.

Consequences of Failure

The World Economic Forum (WEF) has noted that Cyber Security 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.

One For All & All For One

The Financial Stability Board (FSB) has empathised 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.

Expanding Attack Vectors

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 intercon-nected through payment systems.

Remote Work Broadens The Attack Surface

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.

The Need (continued)

Anticipate, Adapt, Respond, & Recover
Financial institutions need to strengthen their 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.

Resilient Financial Markets Enable Resilient Economies
According to the Committee on Payments and Market Infrastructures (CPMI) and The Board of the International Organisation on Securities Commissions (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 and efficient operation of financial market infrastructures must be guarded to maintain and promote financial stability and economic growth.

Rising Cyber Risks
The International Association of Insurance Supervisors (IAIS) in its Issues Paper on cyber risk to the insurance sector in 2016, raised concern over the growing Cyber Security risks across all sectors of the global economy. The IAIS pointed out that cyber risks have grown, and cyber criminals have become increasingly sophisticated.

Potential Reputational Impact
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.

Appendix B: The statement of need and expected impact - Cyber Security Joint Standard

Joint Standard Objectives

The following is set out in the Joint Standard:
- The minimum requirements for sound practices and processes of Cyber Security and Cyber Resilience.
- The requirements relating to governance, Cyber Security strategy and framework.
- Cyber Security and Cyber Resilience fundamentals.
- Cyber Security hygiene practices, as well as regulatory reporting.

Processes
Ensure that financial institutions establish sound and robust processes for managing cyber risks.

Fundamentals
Promote the adoption of Cyber Security fundamentals and hygiene practices to preserve confidentiality, integrity and availability of data and IT systems.

Testing & Assurance
Ensure that financial institutions undertake systematic testing and assurance regarding the effectiveness of their security controls.

Resilience & Reporting
Ensure that financial institutions establish and maintain Cyber Resilience capability, to be adequately prepared to deal with cyber threats.

Provide for notification by the regulated entities of material cyber incidents to the Authorities.

Joint Standard Current Status

This Statement covers the rationale for the proposed Joint Standard, the expected impact, and 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 – completed.

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 – completed.

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 be submitted to Parliament for a period of at least 30 days while Parliament is in session – not started.

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 – not started.

Approximate Implementation Cost

The statement of need makes a high-level reference to the initial implementation cost and the annual operating costs post implementation

- 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 (6 entities provided this estimate).
- 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 (4 entities provided this estimate).
- The ranges provided above, in addition to the lack of information concerning the size, complexity and current information security maturity of the submitting entities, does not provide sufficient budgetary guidance.

General Comments

1. The exact date that the Joint Standard will come into effect remains unknown, however it is our understanding that the standard will be published in the near future, within approximately six to eight months from September 2023 and dependent on the following considerations:
   - The number of changes to the standard for example, in excess of 300 comments were received in relation to the control requirements.
   - The complexity of the changes required.
   - Whether a third round of public consultation will materialise.
   - The parliamentary approval process and associated timeline.
2. The Joint Standard places significant emphasis on control and capability effectiveness testing versus traditional compliance based standards.
3. The body of evidence is excepted to be significantly larger than other compliance assessments.
4. No general exemptions will be permitted, however financial organisations may apply for exemption to specific control requirements, which will be reviewed and approved on a case by case basis as per section 281 of the Financial Sector Regulation Act.
5. The Standard does not contain clauses pertaining to non compliance or penalties, however non compliance and penalties may be enforced as it pertains to the Financial Sector Regulation Act.
6. The standard is a combination of International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27001, 22301, 31000, National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), CPMI-IOSCO. The Joint Standard contains approximately 137 control and sub controls statements. The controls are structured across five core functions namely, identify, protect, detect, respond and recover.
7. Although similarities can be drawn between the Joint Standard and the NIST CSF, organisations should be cautious as the Joint Standard contains additional operational effectiveness controls that are not native to the NIST CSF.
8. It is our point of view that Financial Services Industry (FSI) clients should perform their own budgetary exercise to determine (1) the approximate implementation cost, and (2) the post implementation operating cost.

Recommendations

Perform a Gap Assessment

- Determine the current state of the implemented information security controls against the requirements of the Joint Standard.
- Identify areas of improvement and potential non-compliance.
- Prioritise remedial efforts and identify the implementation timeline.
- The output of the gap assessment should serve as input to the budgetary exercise.

Determine the Implementation Cost

- Determine the resources (people, process, and technology) required to implement the standard.
- Determine the post implementation operational cost.
- Determine the regulatory reporting costs such as internal/external audit.
- Determine or provide for ad hoc costs.

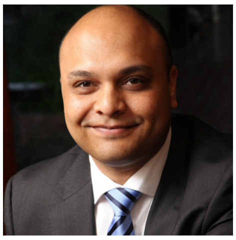
Identify Stakeholders

- Implementations of this nature, size and complexity would be best achieved through a structured project, endorsed and managed by executive management with the support of senior stakeholders across the organisation.

Consider the Short Implementation Timeline

- Given the size, complexity and nature of the organisation, FSI clients should consider the relatively short implementation timeline (12 months) and plan appropriately to achieve compliance within the stipulated time.

Meet Our Team



Samresh Ramjith
Cyber Risk Africa Leader
+27 78 456 2278
sramjith@deloitte.co.za

Mary-Ann Labuschagne
Senior Manager Cyber Strategy & Transformation
+27 82 881 8570
mlabuschagne@deloitte.co.za

Wynand Pretorius
Senior Subject Matter Expert
+27 79 892 0444
wpretorius@deloitte.co.za