FSCA

Financial Sector
Conduct Authority

SOUTH AFRICAN RESERVE BANK
Prudential Authority

FINANCIAL SECTOR REGULATION ACT, 2017

JOINT STANDARD 2 OF 2024

CYBERSECURITY AND CYBER RESILIENCE REQUIREMENTS

The Financial Sector Conduct Authority and Prudential Authority (Authorities), under section 107 read with sections 105, 106 and 108 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) hereby make the 'Joint Standard 2 of 2024 - Cybersecurity and Cyber Resilience Requirements for Financial Institutions' as per the Schedule below.

UNATHI KAMLANA

Commissioner:

FINANCIAL SECTOR CONDUCT AUTHORITY

FUNDI TSHAZIBANA

Chief Executive Officer:

PRUDENTIAL AUTHORITY

Date of publication: 17/05/24

SCHEDULE

JOINT STANDARD 2 OF 2024

FINANCIAL SECTOR REGULATION ACT, 2017 (Act No. 9 of 2017)

Cybersecurity and Cyber Resilience Requirements

Table of Contents

1 Legislative authority

1.1 This Joint Standard is made under section 107 read with sections 105, 106 and 108 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017).

2 Definitions and interpretation

2.1 In this Joint Standard, **'the Act'** means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) and any word or expression to which a meaning has been assigned in the Act bears the meaning assigned to it, and unless the context indicates otherwise -

'attack surface' means the sum of an IT system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to a financial institution;

'Authorities' means the Prudential Authority as established in terms of section 32 of the Act and the Financial Sector Conduct Authority as established in terms of section 56 of the Act;

'black box testing' means testing by testers that have no information about the environment they are testing;

'compromise' means the violation of the security of an IT system or information asset;

'critical or criticality' means a measure of the degree to which an organisation depends on the IT system or information asset for the success of a mission or of a business function;

'cryptography' means the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorised use, or prevent their undetected modification;

'cyber'[1] means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data and IT systems;

'cyber-related information' includes cyber incident, cyber threat intelligence and information on system vulnerabilities;

'cybersecurity'[1] means the preservation of confidentiality, integrity and availability of information and/or IT systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved;

'cyber event' means any observable occurrence in an IT system. Cyber events sometimes provide indication that a cyber incident is occurring;

'**cyber incident'**[1] means a cyber event that –
(a) jeopardises the cybersecurity of an IT system or the information processed, retrieved, stored or transmitted by the system; or
(b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not;

[1] Adapted from the Financial Stability Board Cyber Lexicon. Available at: http://www.fsb.org/wp- content/uploads/P121118-1.pdf.

'cyber resilience'[1] means the ability of a financial institution to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. It involves people, process and technology;

'cyber risk'[1] means the combination of the probability of cyber incidents occurring and their impact;

'cyber threat'[1] means a cyber event with the potential to exploit one or more vulnerabilities that adversely affect cybersecurity;

'data' means electronic representations of information in any form as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002);

'defence-in-depth'[1] means a security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of a financial institution;

'financial institution', notwithstanding the definition of 'financial institution' in the Act, for the purpose of this Joint Standard means –

(a) a bank, a branch[2], a branch of a bank and a controlling company as respectively defined section 1 of the Banks Act, 1990 (Act No. 94 of 1990);
(b) a mutual bank as defined in section 1 of the Mutual Banks Act, 1993 (Act No. 24 of 1993);
(c) an insurer and a controlling company as defined in section 1 of the Insurance Act, 2017 (Act No. 18 of 2017);
(d) a manager as defined in section 1 of the Collective Investment Scheme Control Act, 2002 (Act No. 45 of 2002);
(e) a market infrastructure as defined in section 1 of the Financial Markets Act 2012 (Act No. 19 of 2012);
(f) a discretionary FSP as defined in Chapter II of the Notice on Codes of Conduct for Administrative and Discretionary FSPs, 2003;
(g) 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;
(h) an administrative FSP as defined in Chapter I of the Notice on Codes of Conduct for Administrative and Discretionary FSPs, 2003;
(i) a pension fund registered under the Pension Funds Act, 1956 (Act No. 24 of 1956);
(j) an OTC derivative provider as defined in the Financial Markets Act Regulations;
(k) an administrator approved in terms of section 13B of the Pension Funds Act, 1956 (Act No 24 of 1956); and
(l) a registered credit rating agency as defined in section 1 of the Credit Rating Services Act, 2012 (Act No 24 of 2012).

'grey box testing' means testing where the testers have limited information about the environment they are testing;

'independent review' means a review conducted by an internal or external audit function or an independent control function;

'indicators of compromise'[1] means indicators used for identifying signs that a cyber incident may have occurred or may be currently occurring;

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

‘information asset’ means any piece of data, device or other component of the environment that supports information-related activities. In the context of this Joint Standard, information assets include IT asset and excludes paper-based information;

'information security’ means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide—

(a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(b) confidentiality, which means preserving authorised restrictions on access and disclosure, including the protection of personal privacy and proprietary information; and
(c) availability, which means ensuring timely and reliable access to and use of information;

‘investment fund administration services’ means, read in the context of paragraph (b)(i) of the definition of “intermediary service” as defined in the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002), any act other than the furnishing of advice, performed by a financial services provider for or on behalf of a client or product supplier with a view to administering, maintaining or servicing a collective investment scheme or hedge fund purchased by a client from a product supplier or in which the client has invested.;

‘IT’ means information technology;

‘IT asset’ means an asset including software, hardware, internal and external-facing network system that are found in the business environment;

‘**IT environment’** means the IT components which comprise IT assets, operations and human elements of a financial institution;

‘IT systems’ means the integration of IT assets within the IT environment;

‘material incident’ means a disruption of a business activity, process or function which has, or is likely to have, a severe and widespread impact on the financial institution’s operations, services to its customers, or the broader financial system and economy;

‘penetration testing’[1] means a test methodology in which assessors, using all available documentation such as system design, source code, manuals and working under specific constraints, attempt to circumvent the security features of an IT system;

‘privileged account’ means a user account with approved authorisations of a privileged user. It also includes access to set “access rights” for users on a given system. Sometimes referred to as system or network administrative accounts;

‘privileged user’ means a user that is authorised (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorised to perform;

‘**responsible authority’** means the responsible authority for a financial sector law as defined in section 1 of the Act;

‘RPO’ means the recovery point objective and refers to the acceptable amount of data loss for an IT system, should a disaster or system disruption occur;

'RTO' means the recovery time objective and means the duration of time, from the point of disruption, within which a system should be restored;

'security' means both cyber and information security;

'security controls' means a prevention, detection or response measure to reduce the likelihood or impact of a cyber event or cyber incident;

'senior management' means –

(a) the chief executive officer or the person who is in charge of a financial institution;
(b) a person, other than a director or a head of a control function-
    (i) who makes or participates in making decisions that-
        (aa) affect the whole or a substantial part of the business of a financial institution;
        (bb) has the capacity to significantly affect the financial standing of a financial institution; and
    (ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted, by the governing body;

'sensitive information' means information or data where loss, misuse, unlawful disclosure or unauthorised access to or modification of could adversely affect the public interest or a financial institution or the privacy to which persons are entitled;

'sensitivity' means a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection;

'**threat intelligence'**[1] means threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes;

'user' means a financial institution's employees, contractors, consultants and third-party service providers with access to an IT system or information asset;

'vulnerability'[1] means a weakness in an information asset or security control that could be exploited to compromise cybersecurity;

'**vulnerability assessment'**[1] means a systematic examination of an IT system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation; and;

'white box testing' means testing where the testers are provided with relevant information about the environment they are testing.

3 Application

3.1 This Joint Standard applies to financial institutions as defined in this Joint Standard.

3.2 A financial institution that is a bank, or a controlling company must ensure that any risks relating to cybersecurity and cyber resilience from juristic persons (both local and foreign) and branches structured under the bank or the controlling company, including all relevant subsidiaries approved in terms of section 52 of the Banks Act, 1990 (Act No. 94 of 1990), are catered for and mitigated in the application of the requirements of this Joint Standard.

3.3 A financial institution that is an insurer or the controlling company of an insurance group must ensure that any risks relating to cybersecurity and cyber resilience from juristic persons (both local and foreign) structured under the insurer or the insurance group designated under section 10 of the Insurance Act, 2017 (Act No. 18 of 2017), are catered for and mitigated in the application of the requirements of this Joint Standard.

3.4 The minimum requirements and principles set out in this Joint Standard must be implemented to reflect the nature, size, complexity and risk profile of a financial institution.

3.5 Where words such as 'appropriate, adequate, effective, timely, regular, or periodic' are used in this Joint Standard, the implementation of the relevant requirement must be assessed in consideration of the nature, size, complexity and risk profile of a financial institution.

3.6 The Joint Standard must be read and applied in conjunction with the relevant financial sector laws.

4 Roles and responsibilities

4.1 The governing body is ultimately responsible for –

4.1.1 ensuring that the financial institution complies with the requirements set out in this Joint Standard; and

4.1.2 the oversight of cyber risk management, but may delegate primary oversight activities to an existing or new committee.

4.2 The governing body must –

4.2.1 together with senior management, ensure that a sound and robust cybersecurity strategy and framework is established, implemented and maintained;

4.2.2 require management to co-operate with other stakeholders, as relevant and appropriate, in order to enable financial sector cyber resilience; and

4.2.3 ensure that roles and responsibilities for security are clearly defined in the contract or Service Level Agreement with third-party service providers.

5 Governance

5.1 A financial institution must –

5.1.1 clearly define the roles and responsibilities of all management functions (including lines of defence) as well as committees established for the purposes of exercising oversight of cyber risks;

5.1.2 ensure cyber risk management is incorporated into the governance and risk management structures, processes and procedures of a financial institution. Direct reporting line to the governing body should be established in terms of the governance framework; ensure that a function(s) responsible for cyber and information security is established with adequate resources and appropriate authority;

5.1.3 ensure that the oversight of the function(s) referred to in subparagraph 5.1.3 above, including control functions, has access to the governing body and is structured in a manner that ensures adequate segregation of duties and avoids any potential conflicts of interest.

5.2 In reference to subparagraphs 5.1.3 and 5.1.4 above, the responsible authority may require a financial institution based on its nature, scale, complexity and risk profile to have an independent oversight function.

6 Cybersecurity strategy and framework

6.1 A financial institution must –

6.1.1 establish and maintain a cybersecurity strategy that is approved by the governing body and aligned with its overall business strategy;
6.1.2 review the cybersecurity strategy regularly, but at least annually, to address changes in the cyber threat landscape, allocate resources, identify and remediate gaps, and incorporate lessons learnt;
6.1.3 establish a cybersecurity framework to manage cyber risks;
6.1.4 align its cybersecurity framework with its enterprise risk management framework;
6.1.5 establish cybersecurity policies, standards, processes and procedures that are informed by industry standards and best practices to manage cyber risks and safeguard IT systems and information assets, taking into consideration the evolving technology and cyber threat landscape;
6.1.6 define and reassess regularly business risk tolerance relative to cybersecurity and ensure that it is consistent with the business strategy and risk appetite; and
6.1.7 establish metrics to track and manage cybersecurity risks and to inform related reporting from both a technical and business context.

6.2 The cybersecurity framework referred to in subparagraph 6.1.3 above must –

6.2.1 be approved by the governing body;
6.2.2 be reviewed regularly, but at least annually, for adequacy and effectiveness through an independent review; and
6.2.3 clearly articulate how a financial institution will identify cyber risks and determine the controls required to keep those risks within acceptable limits.

7 Cybersecurity and cyber resilience fundamentals

7.1 Identification

7.1.1 A financial institution must –

(a) identify business processes and information assets that support business and delivery of services, including those managed by third-party service providers;
(b) in reference to item (a) above, classify the business processes and information assets in terms of criticality and sensitivity, which in turn must guide the prioritisation of its protective, detective, response and recovery efforts;
(c) carry out security risk assessments on its critical operations and information assets to ensure that they are protected against compromise; and
(d) maintain an inventory of all its information assets which includes location, ownership, the roles and responsibilities of managing the information assets.

7.1.2 The inventory, referred to in subparagraph 7.1.1(d) above must be updated when changes are required and reviewed regularly but at least biennially.

7.2 Protection

7.2.1 A financial institution must implement appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit and/or contain the impact of a potential cyber event or cyber incident.

7.2.2 Identity and access management:

(a) A financial institution must –

(i) ensure that access to information assets and associated facilities is limited to users, processes, and devices authorised by the financial institution;
(ii) ensure that access to information assets and associated facilities is managed commensurate with the assessed risk of unauthorised access;
(iii) establish identity management and access control mechanisms to provide effective and consistent user administration, accountability and authentication;
(iv) establish security and access control policies and procedures;
(v) ensure remote access to information assets is only allowed from devices or connections that have been secured according to the financial institution's security standards; and
(vi) ensure that strong authentication is implemented for users performing remote access to safeguard against unauthorised access to the financial institution's IT environment.

7.2.3 Data security

(a) A financial institution must –

(i) develop comprehensive data loss prevention policies for its sensitive information whether in motion, at rest or in use;
(ii) implement appropriate measures to prevent and detect unauthorised access to data, modification, copying, transmission as well as data theft in systems and endpoint devices;
(iii) ensure that information assets managed by third-party service providers are accorded the same level of protection and subject to security standards that are commensurate to information assets' sensitivity and criticality;
(iv) ensure that sensitive information stored in systems and endpoint devices is encrypted or protected by access control mechanisms commensurate to the risk exposure. Based on the nature, scale, complexity and risk profile of the financial institution the responsible authority may require that stored sensitive information is encrypted;
(v) ensure that only authorised IT systems, endpoint devices and data storage mediums, are used to process, retrieve, communicate, transmit or store sensitive information;
(vi) ensure that security controls are implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store sensitive data;
(vii) ensure that the use of sensitive information in non-production environments is restricted, unless equivalent controls to the production environment are in place. In exceptional situations where production data needs to be used in non-production environments, adequate processes and safeguards must be in place for the data request and approval must be obtained from senior management;
(viii) ensure appropriate controls are implemented in production and non-production environments to manage the access and removal of sensitive information to prevent data leakages. Where possible, such data must be masked in the production and non-production environments;
(ix) ensure sensitive information is permanently deleted from storage media, IT systems and endpoint devices before it is disposed of or redeployed;
(x) have an agreement in place for the secure return or transfer of data in instances where the contract, including a contract with a third-party service provider, is terminated and data must be returned. If return is impossible, there must also be processes in place for the permanent deletion of all copies of the financial institution's information as well as the

secure destruction of storage media containing the financial institution's information. Where data is required to be retained for a period of time in accordance with the requirements of legislation, the data may be retained, but must be destroyed immediately upon the expiration of the retention period; and

(xi) have appropriate non-disclosure or confidentiality provisions included in the relevant agreements in place with users.

7.2.4 Application and system security

(a) A financial institution must –

(i) implement security-by-design approach which refers to building security in every phase of software development in order to minimise system vulnerabilities and reduce the attack surface;
(ii) determine the acceptable level of security required to meet its business needs and assess the potential threats and risks related to the applications and systems;
(iii) ensure that security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking and exception handling are clearly specified at the initial stages of system development/acquisition; and
(iv) ensure that changes to business-critical applications are reviewed and tested to ensure that there is no adverse impact on operations or security.

7.2.5 Network security

(a) A financial institution must –

(i) install network security devices to secure the network between the financial institution and the internet, as well as connections with third-party service providers;
(ii) deploy network intrusion detection or prevention systems to detect and block malicious traffic;
(iii) review its network architecture, including the network security design; as well as systems and network interconnections on a periodic basis to identify potential vulnerabilities;
(iv) implement network access controls to detect and prevent unauthorised devices from connecting to its network. Network access mechanisms must be reviewed regularly, but at least annually, to ensure they are kept up-to-date;
(v) review firewall rules on a periodic basis and test network perimeter controls and posture at least annually;
(vi) isolate internet web browsing activities from its sensitive IT systems through the use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks; and
(vii) encrypt remote connections to prevent data leakages through network sniffing and eavesdropping.

7.2.6 Cryptography

(a) Where a financial institution uses cryptography, it must –

(i) establish cryptographic key management policies, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry;

(ii) adopt cryptographic algorithms from well-established international standards;
(iii) ensure cryptographic keys are securely generated and protected from unauthorised disclosure in hardened and tamper resistant systems. Any cryptographic key or sensitive information used to generate or derive the keys must also be protected or securely destroyed after the key is generated;
(iv) use a secure key destruction method to ensure the keys are not recoverable when cryptographic keys have expired or have been revoked;
(v) determine the appropriate lifespan of each cryptographic key based on factors, such as the sensitivity of the data, the criticality of the system to be protected, and the threats and risks that the data or system may be exposed to. The cryptographic key must be securely replaced, before it expires at the end of its lifespan;
(vi) maintain backups of cryptographic keys for recovery purposes and accord them a high level of protection since cryptographic keys can be corrupted or unintentionally deleted; and
(vii) ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.

7.2.7 Cybersecurity awareness and training

(a) A financial institution must –

(i) establish a comprehensive cybersecurity awareness training programme to maintain a high level of awareness among all users in the financial institution;
(ii) ensure that user refresher training is conducted at least annually and training on new content is done regularly in consideration of the evolving risks;
(iii) ensure that the governing body undergo training to raise their awareness on risks associated with the use of technology and enhance their understanding of cyber risk management practices; and
(iv) ensure that the training programme is reviewed periodically to ensure its contents remain current and relevant. The review must take into consideration changes in the financial institution's security policies, prevalent and emerging risks, and the evolving threat landscape.

7.3 Detection

7.3.1 A financial institution must maintain effective cyber resilience capabilities to –

(a) systemically monitor and detect cyber events and cyber incidents on IT systems, information assets and business services as well as effectively respond to attacks;
(b) periodically evaluate the effectiveness of identified controls, including through network monitoring, testing and audits;
(c) establish security monitoring capabilities such as a security operations centre (or similar) or acquire managed security services in order to facilitate continuous monitoring and analysis of cyber events as well as prompt detection and response to cyber incidents; and
(d) define processes, roles and responsibilities for security operations.

7.3.2 A financial institution, when implementing the requirements in subparagraph 7.3.1(a) above, must consider –

(a) establishing a process to collect, review and retain IT system logs to facilitate security monitoring operations. These logs must be protected against unauthorised access, editing, and deletion;
(b) configuring IT system events or alerts to provide an early indication of issues that may affect its security. Security events or alerts must be actively monitored so that prompt measures can be taken to address the issues early;
(c) performing correlation of multiple events registered on IT system logs to identify suspicious or anomalous activity patterns; and
(d) establishing a process for timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behaviour.

7.4 Response and recovery

7.4.1 A financial institution must –

(a) implement capabilities to rapidly respond and recover from cyber-attacks as well as mitigate the potential systemic risks;
(b) establish effective cyber incident management policies and processes that will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact;
(c) establish data backup strategy, and develop a plan to perform regular backups and testing so that IT systems and data can be recovered in the event of a cyber incident or when data is corrupted or deleted;
(d) ensure any sensitive information stored in the backup media is secured (e.g. encrypted). Backup media must be stored offline or at an offsite location (including cloud storage);
(e) implement a clear communication strategy to financial customers impacted by cyber-attacks, including details on any recourse available to financial customers; and
(f) sets its RPO and RTO based on its nature, scale, complexity, and risk profile.

7.5 Incident response and management

7.5.1 A financial institution must –

(a) establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber incident and to securely resume affected services. The plan must describe communication, coordination, and response procedures to address plausible cyber threat scenarios;
(b) as part of the plan, establish a process to investigate and identify the security control deficiencies that resulted in the compromise. The investigation must also evaluate the full extent of the impact to the financial institution;
(c) ensure that information from cyber intelligence and lessons learnt from cyber incidents is used to enhance the existing security controls or improve the cyber incident response and management plan; and
(d) ensure that the cyber incident response and management plan is tested to address all plausible cyber threats, including the latest cyber threats and is aligned to the set RPO and RTO requirements.

7.6 Situational awareness

7.6.1 A financial institution must understand the threat landscape and its implications in an environment within which it operates as well as the adequacy of its cyber risk mitigation measures.

7.6.2 Threat intelligence and information sharing

(a) A financial institution must –

(i) establish a process to collect and analyse cyber-related information for its relevance to and potential impact on the business and IT environment in order to maintain good cyber situational awareness;
(ii) implement cyber intelligence monitoring capabilities for both internal and external threats; and
(iii) participate in cyber threat information-sharing arrangements with trusted external parties to –
(a) share reliable, actionable cybersecurity information regarding threats, vulnerabilities, and incidents to enhance defences; and
(b) receive timely and actionable cyber threat information.

7.7 Testing

7.7.1 Testing control effectiveness

(a) A financial institution must test all elements of its cyber resilience capacity and security controls to determine the overall effectiveness, whether it is implemented correctly, operating as intended and producing desired outcomes. The nature and frequency of the testing must be commensurate with –
(i) the rate at which the vulnerabilities and threats change;
(ii) the criticality and sensitivity of IT systems and information assets;
(iii) the consequences of a cyber incident;
(iv) the risks associated with exposure to environments where a financial institution is unable to enforce its security policies; and
(v) the materiality and frequency of change to IT systems and information assets.
(b) Where a financial institution's IT systems or information assets are managed by a third-party service provider, and a financial institution is reliant on that party's information security control testing, the financial institution must be satisfied that the nature and frequency of testing of controls in respect of those IT systems or information assets is commensurate with items (a)(i) to (v) above.
(c) A financial institution must –
(i) ensure that security control assurance is provided by personnel appropriately skilled in providing such assurance;
(ii) escalate and report to the governing body any testing results that identify security control deficiencies that cannot be remediated in a timely manner; and
(iii) ensure that a remediation plan, with timelines is followed to address identified control deficiencies.

7.7.2 Vulnerability assessment

(a) A financial institution must –

(i) establish a process to conduct regular vulnerability assessments on its IT systems and information assets to identify security vulnerabilities and ensure that vulnerabilities are addressed in a timely manner; and
(ii) ensure that the frequency of vulnerability assessments is commensurate with the criticality of the IT system and information assets and the security risk to which it is exposed.

7.7.3 Penetration testing

(a) A financial institution must –

(i) carry out penetration testing on critical IT systems and information assets to obtain an in-depth evaluation of its cybersecurity defences. The

responsible authority may, based on the nature, scale, complexity and risk profile of the financial institution specify that a black box, grey box and white box testing or a combination thereof be conducted for critical IT systems and information assets;

(ii) ensure that the frequency of penetration testing is determined based on factors such as criticality and exposure to cyber risks; and

(iii) conduct penetration testing to validate the adequacy of the security controls for IT systems and information assets that are directly accessible from the internet, whenever such IT systems and information assets undergo major changes or updates. If no major changes or updates are made, penetration testing must be conducted at least annually.

7.7.4 Simulation exercises

(a) A financial institution must –

(i) carry out regular scenario-based simulation exercises to validate the financial institution's response and recovery capabilities, as well as communication plans against prevalent cyber threats. The simulation exercise must include, but is not limited to, an adversarial attack and defence simulation exercise; and

(ii) design the scenario-based simulation exercise by using threat intelligence that is relevant to the financial institution's IT environment in order to identify –

(aa) threat actors who are most likely to pose a threat to the financial institution; and

(bb) the tactics, techniques and procedures most likely to be used in such attacks.

7.7.5 Application security testing

(a) A financial institution must –

(i) carry out testing of security functionality on web-based and critical applications during the development and implementation in a robust manner to ensure that they satisfy business policies or rules of the financial institution as well as regulatory and legal requirements;

(ii) adopt standards on secure coding, source code review and application security testing to minimise the bugs and vulnerabilities in its software;

(iii) establish a policy and procedure on the use and update of third-party and open-source software code to ensure these codes are subject to review and testing before they are integrated into the financial institution's software; and

(iv) ensure that the policy and procedures are reviewed regularly.

7.7.6 Remediation management

(a) A financial institution must establish a comprehensive remediation process to track and resolve issues identified from the cybersecurity testing or exercises, third-party assessments, self-assessments as well as findings from internal and external assurance.

(b) The remediation process referred to in item (a) above must at a minimum –

(i) include the following:

(aa) severity assessments and classification of issues;

(bb) prioritisation of issues based on the risk posed;

(cc) timeframes to remediate issues of different severity;

(dd) risk assessments where appropriate; and

(ee) mitigation strategies to manage deviations from the cybersecurity framework;

(ii) ensure all issues identified from cybersecurity testing or exercises, as well as software defects discovered from source code review and application security testing, are tracked. Known major issues and security flaws must be remediated before production deployment; and

(iii) keep track of updates and reported vulnerabilities on in-house developed, third-party and open-source software that are utilised by the financial institutions in order to facilitate the remediation of vulnerabilities in a timely manner.

7.8 Learning and evolving

7.8.1 A financial institution must –

(a) Implement an adaptive cyber resilience capability that learns and evolves with the dynamic nature of cyber risks and allows the institution to identify, assess and manage security threats and vulnerabilities; systematically identify and distil key lessons from cyber incidents that have occurred within and outside the institution in order to advance resilience capabilities;

(b) actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber-attack; and

(c) ensure that cyber risk management practices go beyond reactive controls and include proactive protection against future cyber events.

8 Cybersecurity hygiene practices

8.1 Access management

8.1.1 A financial institution must –

(a) establish a security access control policy[3] and a process to enforce strong password security controls for users' access to IT systems and information assets;

(b) ensure that the security access control policy is reviewed regularly;

(c) establish a user access management process to provision, change and revoke access rights to IT systems and information assets;

(d) apply the principles of 'segregation of duties' and 'least privilege' when granting user access to IT systems and information assets. Access rights and privileges must be granted according to the roles and responsibilities of the user;

(e) ensure appropriate parties such as IT systems and information assets owners perform periodic user access reviews to verify the appropriateness of privileges that are granted to users; and

(f) subject its third-party service providers and contractors who are given access to the financial institution's IT systems and information assets, to the same monitoring and access restrictions as the financial institution's employees.

8.2 Privileged access management

8.2.1 A financial institution must –

(a) ensure that every administrative account in respect of any operating system, database, application, security appliance, network device, cloud tenant or

[3] In terms of the access control policy this will include aspects such as identity and access management functionality e.g. passwords, biometrics, tokens etc.

authentication system is secured to prevent any unauthorised access to or use of such account;
(b) grant access to privileged accounts on a need-to-use basis; activities of these accounts must be logged and reviewed as part of the financial institution's ongoing monitoring; and
(c) establish a process to manage and monitor the use of IT systems, information assets and service accounts for suspicious or unauthorised activities.

8.3 Multi-factor authentication (MFA)

8.3.1 A financial institution must –

(a) ensure that MFA is implemented for users with access to critical system functions;
(b) ensure that MFA or at least privilege access management mechanisms are implemented for all administrative and privileged accounts;
(c) ensure that MFA is implemented for all user accounts utilised to access applications containing sensitive information through the internet.

8.4 Network perimeter defence

8.4.1 A financial institution must –

(a) ensure that the network is protected from unauthorised access and disruption;
(b) implement security controls at its network perimeter to restrict all unauthorised network traffic; and
(c) adopt a 'defence in depth' approach or implement multiple layers and types of controls to ensure that if one security control fails, other controls limit the impact of a security compromise.

8.5 Vulnerability and patch management

8.5.1 A financial institution must ensure that–

(a) security patches are applied to address vulnerabilities to every IT asset, by applying such security patches or other mitigating controls as possible within a timeframe that is commensurate with the risks posed by each vulnerability;
(b) compensating security controls are instituted to reduce any risk posed where there is no security patch available to address vulnerabilities identified;
(c) security patches are tested before they are applied to the IT assets in the production environment to ensure compatibility with existing IT assets or such patches do not introduce problems to the IT environment; and
(d) where patches are not compatible with existing IT systems or such patches introduce problems to the IT environment, ensure that mitigating controls are in place and a remediation plan, with timelines is implemented to address identified control deficiencies.

8.6 Secure configurations

8.6.1 A financial institution must –

(a) ensure that there is a written set of security standards for hardware and software;
(b) ensure that the security standards must outline the configurations that will minimise the financial institution's exposure to cyber threats;
(c) ensure that security standards are reviewed periodically for relevance and effectiveness;

(d) establish a process to verify that the security standards are applied uniformly and to identify deviations from the security standards; and
(e) ensure that controls are instituted to reduce any risk posed where there is non-conformity to the security standards.

8.7 Malware protection

8.7.1 A financial institution must –

(a) implement endpoint protection to protect a financial institution from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media;
(b) ensure that anti-malware signatures are kept up-to-date and the IT systems and information assets are regularly scanned for malicious files or anomalous activities; and
(c) implement detection and response mechanisms to perform scanning for indicators of compromise in a timely manner, and proactively monitor systems', including endpoint devices', processes for anomalies and suspicious activities in order to facilitate early detection and prompt remediation of suspicious or malicious activities.

9 Notifications and regulatory reporting

9.1 A financial institution must notify the responsible authority in the form and manner determined by the Authorities, after classifying the following as a material incident –

9.1.1 cyber incidents; or
9.1.2 information security compromise.

9.2 In addition to the requirements of paragraph 9.1 above, a financial institution must report such information related to the requirements in this Joint Standard to the Authorities, as may be determined by the Authorities.

9.3 For the purposes of paragraph 9.2 above, the Authorities may determine the form, manner, content and period of reporting by notice on the websites of the Authorities.

10 Short title and commencement

10.1 This Joint Standard is called Cybersecurity and Cyber Resilience Requirements for Financial Institutions, 2024 and comes into effect on the date indicated in paragraph 10.2 below.

10.2

Version number	Commencement date
1	At a date to be determined by the Authorities through a notice published on the websites of the Authorities.