DRAFT FOR CONSULTATION – June 2021

JOINT STANDARD 1 OF 2021

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

INFORMATION TECHNOLOGY RISK MANAGEMENT

Objectives and key requirements of Joint Standard – Information technology risk management

This Standard sets out the principles for information technology (IT) risk management that financial institutions must comply with sound practices and processes in managing IT.

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 Standard on a continuous basis.

Contents

DRAFT

1. Commencement

1.1 This Standard commences on 1 January 2022.

Version number	Commencement date
1	1 January 2022 (proposed)

2. Legislative authority

2.1 This Standard is made under section 107 read with sections 105, 106 and 108 of the Act.

3. Definitions and interpretation

3.1 In this 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 so assigned to it, and unless the context indicates otherwise;

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

'governing body' as defined in section 1 of the Act

'**FAIS Act'** means the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002)

'**financial institution'** means a bank, a branch of a foreign institution or a bank controlling company registered or authorised under the Banks Act, 1990 (Act No. 94 of 1990); a mutual bank registered under Mutual Banks Act, 1993 (Act No. 24 of 1993); an insurer licensed under the Insurance Act, 2017 (Act No. 18 of 2017); a manager of a collective investment scheme registered under the Collective Investment Scheme Control Act, 2002 (Act No. 45 of 2002); a market infrastructure registered in terms of the Financial Markets Act 2012 (Act No. 19 of 2012); a discretionary FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003; and an administrative FSP as contemplated in the Code of Conduct for Administrative and Discretionary FSPs, 2003, published in terms of the FAIS Act;

'fit and proper' means a person complying with any applicable fit and proper requirements imposed on such person by a financial sector law or by a financial institution who has authorised such person to access the financial institution's systems;

'fit and proper requirements' means requirements relating to —
(a) honesty and integrity;
(b) good standing;
(c) competence, including —

DRAFT

(i) experience or expertise;
(ii) qualifications; and
(iii) technical knowledge of IT solutions and IT risks as the case may be;

'FSP' means financial services provider as defined in section 1 of the FAIS Act;

'hardware' means physical components of a computer system;

'IT' means information technology;

'IT asset' means an asset of either software or hardware that is found in the business environment;

'**IT environment**' means the components which comprise the internal and external networks, hardware, software, applications, systems interfaces, operations and human elements of a financial institution;

'IT infrastructure' means a set of hardware, software, network or other IT components that integrate an enterprise's IT assets;[1]

'IT programme and project' means any project or programme, or part thereof, where IT systems and services are changed, replaced, dismissed or implemented. IT projects can be part of wider IT or business transformation projects or programmes;

'IT system' means any hardware, software, network or other IT component which is part of an IT infrastructure;

'material IT activity or function' is defined as that element which has the potential to have a significant impact on the financial institution's IT operations or its ability to manage risks effectively should it be disrupted;

'material incident' refers to 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;

'networks' means a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on, or provided by, the network nodes;

'RPO' is the recovery point object and refers to the acceptable amount of data loss for an IT system, should a disaster occur;

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

[1] Adapted from Information System Audit and Control Association (ISACA) fundamentals. https://www.isaca.org/resources/glossary

DRAFT

'risk identification' entails the determination of the threats and vulnerabilities to a financial institution's IT environment;

'**senior management'** means the

(a) chief executive officer or the person who is in charge of a financial institution; or

(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; or

(bb) have the capacity to significantly affect the financial standing of a financial institution; or

(ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted by the governing body; and

'software' means a set of programs and supporting documentation that enable and facilitate use of the computer;[2]

4. Application

4.1 This Standard applies to financial institutions as defined.

4.2 This Standard sets out the requirements for sound practices and processes of IT risk management.

4.3 The requirements of this Standard must be implemented in accordance with the nature, size and complexity of a financial institution.

4.4 This Standard must be read in conjunction with the relevant financial sector laws.

5. Roles and responsibilities

5.1 The governing body is ultimately responsible for ensuring that the financial institution complies with the requirements as set out in this Standard.

5.2 The governing body, together with senior management, must ensure that a sound and robust IT risk management framework and IT strategy is established and maintained.

5.3 The governing body must clearly define the roles and responsibilities of all management, oversight and control functions as well as committees established for the purpose of exercising oversight of IT risks.

6. IT strategy

6.1 A financial institution must ensure that its IT strategy is approved by the governing body and aligned with its overall business strategy.

[2] Adapted from ISACA fundamentals.

DRAFT

6.2 The IT strategy of a financial institution must be reviewed regularly at least annually.

6.3 A financial institution must -

(a) establish a set of action plans that contain measures to be taken in order to achieve the objective of its IT strategy. The action plans must be communicated to all relevant staff and must be reviewed regularly, but at least on a quarterly basis, to ensure their relevance and appropriateness;

(b) establish processes to monitor and measure the effectiveness of the implementation of its IT strategy; and

(c) ensure that the Authorities are informed when there is a deviation from the IT strategy that may contravene this Standard or any other legal requirements relating to IT risk management.

7. IT risk management framework

7.1 A financial institution must establish an IT risk management framework to manage IT risks in a systematic and consistent manner.

7.2 The IT risk management framework of a financial institution must be approved by the governing body and reviewed regularly, but at least annually.

7.3 The IT risk management framework of a financial institution must, at a minimum, encompass the following attributes and requirements -

(a) IT policies, standards and procedures in managing IT risks and safeguarding IT assets in the organisation;
(b) the ability to detect, control and limit all major risk, taking into consideration the principle of proportionality;
(c) IT policies, standards and procedures must be independently reviewed and updated to take into account, among others, rapid changes in the IT operating and security environment;
(d) roles and responsibilities in managing IT risks, in terms of which -
    (i) the governing body and senior management must oversee the design, implementation and effectiveness of IT risk management programmes;
    (ii) the governing body and senior management must ensure that financial institutions have adequate internal governance and internal control frameworks in place for their IT risk management;
    (iii) the governing body and senior management are fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability;
    (iv) there must be a function or department responsible for ensuring that proper risk management measures are implemented and enforced for a specific IT risk, and this function or department must be -

DRAFT

(aa) accountable for, and be given the authority to manage IT risks;
(bb) headed by an individual with requisite skills and experience, and who is part of senior management;

(e) identification and prioritisation of IT assets in terms of which -
(i) IT assets must be appropriately identified, recorded and protected from unauthorised access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure; and
(ii) criticality of IT assets must be identified and ascertained in order to develop appropriate plans to protect them;

(f) identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities in terms of which a financial institution must -
(i) following risk identification, perform an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations; and
(ii) develop a threat and vulnerability matrix to assess the impact of the threat to its IT environment. The matrix should also assist the financial institution in prioritising IT risks;

(g) implementation of appropriate practices and controls to mitigate risks in terms of which -
(i) the financial institution must, for each type of risk identified, develop and implement risk mitigation and control strategies that are consistent with the importance of the IT assets and the level of risk tolerance;
(ii) the financial institution must be able to manage and control risks in a manner that will maintain its financial and operational viability and stability;
(iii) the financial institution must, when deciding on the adoption of controls and security measures, also be conscious of the effectiveness of the controls with regard to the risks being mitigated; and
(iv) as a risk mitigating measure, a financial institution must consider taking insurance cover for various IT risks;

(h) periodic updates and monitoring of risk assessments must include changes in systems, environmental or operating conditions that would affect risk analysis in terms of which -
(i) the financial institution must maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity must be accorded top priority and monitored closely with regular reporting to senior management and the governing body on the actions that have been taken to mitigate such risks. A financial institution must update the risk register periodically, and institute a monitoring and review process for continuous assessment and managing of risks and to facilitate risk reporting to management;
(ii) a financial institution must develop IT risk metrics to identify systems, processes or infrastructure that have the highest risk exposure. An overall IT risk profile of a financial institution must also be provided to the governing body and senior management. In determining the IT risk metrics, a financial institution must consider risk events, regulatory requirements and audit observations;

(i) people management in terms of which -

DRAFT

(i) the financial institution must ensure careful screening and selection of staff, vendors and contractors in order to minimise IT risks due to system failure, internal sabotage or fraud;
(ii) staff, vendors and contractors, who are authorised to access the financial institution's systems, must be fit and proper and be contractually required to protect sensitive or confidential information;
(iii) training programmes, including training materials, must be acquired or developed and endorsed by senior management, and be conducted and reviewed regularly, but at least annually. The training programmes must be extended to all new and existing staff, contractors and vendors who have access to the financial institution IT resources, infrastructure and systems; and
(iv) any updates, made as a result of the review conducted in terms of item (iii) above, must ensure that the contents of the training programme and material remain current and relevant. Such updates must also take into consideration the evolving nature of technology as well as emerging risks.

8. Oversight of IT risk management

Oversight of IT risk management must be incorporated into the governance and risk management structures, processes and procedures of a financial institution, including provisions relating to direct reporting lines to the governing body.

9. IT operations

9.1 A financial institution must develop a robust IT service management framework which is essential for supporting IT systems, services and operations, managing changes, incidents and problems as well as ensuring the stability of the production IT environment.

9.2 The IT service management framework of a financial institution must comprise a governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management.

9.3 A financial institution must -

(a) manage its IT operations based on documented and implemented policies, processes and procedures that are approved by the governing body. The policies, processes and procedures must define how the financial institution operates, monitors and controls its information systems and services, including the documenting of critical IT operations and must enable financial institution to maintain an up-to-date IT asset inventory;
(b) maintain and improve efficiency of its IT operations, including, but not limited to the need to consider how to minimise potential incidents arising from the execution of manual tasks;
(c) implement appropriate logging and monitoring procedures for critical IT operations to allow the detection, analysis and correction of incidents;

DRAFT

(d) store the configuration of the IT assets and the links and interdependencies between the different IT assets, to enable a proper configuration management process;
(e) implement performance, capacity planning and monitoring processes to prevent, detect and respond to important performance issues of IT systems and IT capacity shortages in a timely manner;
(f) define and implement data and IT systems backup and restoration procedures to ensure that they can be recovered as required;
(g) establish and implement an effective change management process to ensure that all changes to IT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner; and
(h) establish and implement a problem and incident management process to identify, track (including timing), log, categorise and classify incidents according to a priority, based on business criticality. In addition, the problem management procedure must be able to analyse and solve the root cause behind the incidents.

9.4 The scope and frequency of backups, as referred to in paragraph 9.3(f) above, must be set out in line with business recovery requirements and the criticality of the data and the IT systems must be evaluated according to the performed risk assessment. Testing of the backup and restoration procedures must be undertaken regularly, but at least annually.

9.5 A financial institution must enforce segregation of duties for the development, testing and operations functions.

10. Information security

10.1 A financial institution must implement appropriate information security solutions at the data, application, database, operating systems and network layers to adequately address and contain all forms of security vulnerabilities.

10.2 A financial institution must establish measures that protect data at-rest, in-transit and in-storage, commensurate with the criticality of the information held, also extending to backup systems and offline data stores.

10.3 A financial institution must -

(a) configure IT systems and devices with security settings that are consistent with the expected level of protection. Baseline standards must be established to facilitate consistent application of security configurations for operating systems, applications, databases, network devices and enterprise mobile devices within the IT environment;
(b) conduct regular enforcement checks to ensure that the baseline standards referred to in item (a) are applied uniformly and instances of non-compliance are detected and raised for investigation. The frequency of enforcement reviews must be commensurate with the risk level of IT systems;
(c) establish and ensure that patch management procedures include the identification, categorisation and prioritisation of security patches. To ensure security patches are implemented in a timely manner, a financial

DRAFT

institution must establish the implementation timeframe for each category of security patches;

(d) deploy firewalls or other similar measures within internal networks to minimise the impact of security exposures originating from third party or offshore systems, as well as from the internal trusted network;

(e) deploy anti-virus software to servers and workstations. The anti-virus definition files must be regularly updated. An automatic anti-virus scanning must be scheduled on servers and workstations on a regular basis;

(f) regularly review security logs of systems, applications and network devices for anomalies following a risk-based approach; and

(g) reviews of the information security framework must be subject to independent audit assessments, and the results of the review must be reported to the governing body.

11. Sensitive or confidential information

11.1 A financial institution must define, document and implement appropriate measures to -

(a) protect sensitive or confidential information such as customer personal account and transaction data which are stored and processed in systems; and

(b) mitigate IT risks and protect information assets in accordance with their sensitivity classification.

11.2 A financial institution must -

(a) define, document and implement procedures for logical access control (identity and access management). These procedures must be implemented, enforced, monitored and periodically reviewed. The procedures must also include controls for monitoring anomalies;

(b) implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres;

(c) ensure that information processed, stored or transmitted between itself and its customers is accurate, reliable and complete;

(d) conduct independent reviews, annually, to assess compliance with its privacy policies. In addition, independent reviews may be used to identify vulnerabilities in compliance processes that can undermine confidential and sensitive information on its systems; and

(e) ensure that all personal information is processed in accordance with the requirements of all applicable legislation, including Protection of Personal Information Act, 2013 (Act No. 4 of 2013), and where applicable, the General Data Protection Regulation (EU) 2016/679 (GDPR) applicable in the European Union.

12. Risks associated with products and services

12.1 A financial institution must clearly identify risks associated with the types of products or services being offered, and formulate security controls, system

DRAFT

availability and recovery capabilities, which are commensurate with the level of risk exposure for all operations, including the internet platform.

12.2 A financial institution must -

(a) properly evaluate security requirements associated with its internet systems and adopt encryption algorithms which subscribe to well-established and adopted international standards;
(b) establish appropriate security monitoring systems and processes to detect or monitor risk exposure from services offered;
(c) implement measures to plan and track capacity utilisation as well as guard against online attacks; and
(d) implement appropriate measures to protect customers who use online systems to interact with the financial institution and access and transact with its products and services. Additionally, a financial institution must ensure customer awareness of security measures that are put in place by the financial institution to protect the customers in an online environment.

13. IT programme and/or project management

13.1 A financial institution must develop a framework and approach for IT programme and/or project management that incorporates the governance structures, stakeholder engagement, risks and issues management, change control, integration, and cost and benefit realisation. The framework must be maintained and utilised consistently.

13.2 A financial institution must -

(a) establish and implement an IT programme and project management policy that includes, as a minimum -
    (i) IT programme and project objectives;
    (ii) roles and responsibilities, including governance and decision-making structures;
    (iii) IT programme and project risk assessment;
    (iv) IT programme and project plan, timeframe and steps;
    (v) key milestones; and
    (vi) change management requirements.

(b) ensure that its IT programme and project management policy confirms that IT security requirements are analysed and approved by a function that is independent from the development function;
(c) identify, monitor and mitigate risks deriving from their portfolio of IT programmes and projects, considering risks that may result from interdependencies between different IT programmes and projects and from dependencies of multiple projects utilising the same resources and/or expertise;
(d) ensure that, before any acquisition or development of IT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management;

DRAFT

(e) follow an approved methodology for testing and approval of IT systems prior to implementation into the production environment. This methodology must consider the criticality of business processes and assets. The testing must ensure that new IT systems perform as intended. It must also use test environments that adequately reflect the production environment;
(f) where feasible, implement separate IT environments to ensure adequate segregation of duties and implement a pre-production environment that is a mirror of the production environment to mitigate the impact of unverified changes to the production systems. Specifically, a financial institution must ensure the segregation of production environments from development, testing and other non-production environments;
(g) ensure the integrity and confidentiality of production data in non-production environments and ensure that access to production data is restricted to users that are authorised.
(h) implement appropriate measures to protect the integrity of the source codes of IT systems that are developed in-house. In addition, a financial institution must document the development, implementation, operation and/or configuration of the IT systems comprehensively to reduce any unnecessary dependency on subject matter experts;
(i) ensure that the documentation of the IT system contains, where applicable, user documentation, technical system documentation and operating procedures;
(j) ensure that processes for acquisition and development of IT systems applied by the department responsible for IT must also apply to IT systems acquired by business functions outside the IT department, using a risk-based approach; and
(k) maintain a register of the critical applications, business functions and processes.

14. System recovery and business resumption

14.1 A financial institution must -

(a) define system recovery and business resumption priorities and establish specific recovery objectives including RTO and RPO for IT systems and applications;
(b) identify and establish a disaster recovery site that is geographically separate from the primary site to enable the recovery of critical systems and continuation of business operations, should a disruption occur at the primary site;
(c) establish a sound IT continuity management process to maximise its abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption in line with any existing requirements issued in terms of a financial sector law and applicable to financial institutions; and
(d) establish appropriate measures in respect of a strategy and resources to ensure effective communication to stakeholders, in response to a crisis or disaster involving IT risk.

14.2 As part of sound IT continuity management, a financial institution must conduct a business impact analysis by analysing its exposure to severe

DRAFT

business disruptions and assessing its potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third-party provider data relevant to a business process or publicly available data that may be relevant to the business impact analysis) and scenario analysis.

14.3 A business impact analysis referred to in paragraph 14.2 above must also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies.

14.4 A financial institution must ensure that its IT continuity plan is aligned to the business impact analysis referred to in paragraph 14.2 above, for example, with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

14.5 A financial institution must develop IT continuity plans. The IT continuity plans must specifically consider risks that could adversely impact IT systems and services and support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of its business functions, supporting processes and information assets.

14.6 A financial institution must test its IT continuity plans periodically. In particular, it must ensure that IT continuity supports critical business functions, business processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually. Various scenarios, including total shutdown or incapacitation of the primary site as well as component failure at the individual system or application cluster level, must be covered in IT continuity tests.

14.7 A financial institution must review its IT continuity plans regularly, but at least annually, based on testing results, current threat intelligence and lessons learnt from previous events.

14.8 To achieve data centre resiliency, a financial institution must assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications, to the extent applicable.

14.9 To ensure there is sufficient backup electrical power, a financial institution must install appropriate backup electrical power facilities consisting of uninterruptible power supplies, battery arrays and/or generators.

14.10 A financial institution must establish a sound IT continuity process and IT continuity plan to ensure the ability to return the IT components /telecommunication services and other specific IT essential operations, functions or process, and so on, to a state of normality in the event of severe business disruption.

14.11 A financial institution must define, document and implement physical security measures to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

DRAFT

14.12 A financial institution must test the recovery dependencies between systems. Bilateral or multilateral recovery testing must be conducted where networks and systems are linked to specific service providers and vendors.

14.13 A financial institution must ensure that it implements appropriate network redundancy contingency plans such as arrangements with different network service providers or a network service provider with alternate network paths.

14.14 A financial institution must -

(a) install appropriate network security devices such as firewalls as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure to protect the network perimeters;
(b) ensure IT continuity capabilities to ensure redundancy in the event of system/network failure; and
(c) implement network surveillance and security monitoring procedures with the use of network security devices such as intrusion detection and prevention systems, to protect the financial institution against network intrusion attacks as well as to provide alerts when an intrusion occurs.

15. Outsourcing

15.1 A financial institution must ensure that its IT outsourcing is aligned to, and where applicable complies with, any requirements relating to outsourcing contained in financial sector laws.

15.2 A financial institution must, to the extent that such requirement is not in conflict with a requirement in a financial sector law, comply with the following requirements:

(a) the governing body and senior management of the financial institution must fully understand risks associated with IT outsourcing. IT management must perform risk assessments surrounding the outsourcing of material IT activities and functions; and
(b) a financial institution must -
    (i) have a formally defined and governing body-approved outsourcing strategy and governance framework that includes IT. The outsourcing strategy and governance framework in relation to IT must also include outsourced cloud services;
    (ii) have a governing body-approved approved policy in place, that would deal specifically with outsourcing of IT activities and functions;
    (iii) have due diligence processes in place for the selection of service providers. Before an outsourced service provider is appointed, due diligence must be carried out to determine its viability, capability, reliability, track record and financial position prior to the entering into the outsourcing arrangement;
    (iv) when outsourcing any specific IT function, identify and manage all risks introduced by the outsourcing arrangement;
    (v) have a legal contract in place for all outsourcing of IT activities and functions with third parties;

DRAFT

(vi) require the outsourced service provider to have in place an IT contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures;
(vii) have administrative measures and reporting in place that facilitate oversight, accountability and monitoring of the outsourced service provider; and
(viii) require the outsourced service provider to implement security policies, procedures and controls that are at least as stringent as those in place by the financial institution for its own operations.

15.3 A financial institution must ensure that it has the ability to recover outsourced systems and IT services within the financial institution's stipulated RTO and RPO prior to contracting with the service provider.

15.4 Business continuity requirements relating to the outsourced service provider, including RTOs and RPOs, must be identified through a business impact assessment which is documented. Where a cloud service provider is involved, it must also be agreed with the cloud service provider.

16. IT assurance

16.1 The internal control functions of a financial institution, including the three lines of defence, must, following a risk-based approach, have the capacity to independently review and provide objective assurance of compliance with all IT and IT security-related activities as outlined in the financial institution's policies and procedures as well as with external requirements.

16.2 A financial institution must -

(a) establish an organisational structure and reporting lines for IT audit within the internal audit control function, where appropriate, in a way that preserves the independence and objectivity of the IT audit function;
(b) analyse IT operational or IT security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and must consider key lessons learnt from these analyses and update the IT security measures accordingly;
(c) determine whether changes in the existing operational environment influence the existing IT security measures or require the adoption of additional measures to mitigate the risks involved. These changes must be in accordance with the financial institution's formal change management process; and
(d) maintain an IT audit plan to examine and evaluate the adequacy and effectiveness of the financial institution's IT systems, internal control mechanisms and governance arrangements.

DRAFT

17. Reporting

17.1 A financial institution must, unless such a reporting obligation already exists in another financial sector law, notify the Authorities, in the form and manner determined by the Authorities, of any material systems failure, malfunction, delay or other disruptive event, or any breach of IT security, integrity or confidentiality, within 24 hours of classifying the event as material.

17.2 The Authorities may, through ongoing supervisory review and evaluation processes, request for specific information or reports as well as assurance in terms of compliance with this Standard.

DRAFT