FSCA
Financial Sector Conduct Authority

South African Reserve Bank
Prudential Authority

DRAFT FOR PARLIAMENT

JOINT STANDARD X OF 2023

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

INFORMATION TECHNOLOGY GOVERNANCE AND RISK MANAGEMENT

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

This Joint Standard sets out the principles and minimum requirements for information technology (IT) governance and risk management that financial institutions must adhere to, in line 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 Joint Standard on a continuous basis.

Contents

1. Commencement

1.1 This Joint Standard commences on 1 January 2024 (proposed).

Version number	Commencement date
1	1 January 2024 (proposed)

2. Legislative authority

2.1 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) (the Act).

3. Definitions and interpretation

3.1 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 so assigned to it, 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 as established in terms of section 56 of the Act;
'**FAIS Act'** means the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002);
'**financial institution'** notwithstanding the definition of 'financial institution' in section 1 of the Act, for the purpose of this Joint Standard, means–

(a) a bank, a branch[1], a branch of a bank or a bank controlling company defined in 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 of an insurer 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. F45 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; and
(g) an administrative FSP as defined in Chapter I of the Notice on Codes of Conduct for Administrative and Discretionary FSPs, 2003.

'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 —

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

(i) experience or expertise; and
(ii) knowledge, qualifications or certification.

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

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

'hardware' means physical components of a computer system;

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

'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 data, hardware and software and excludes paper-based information;

'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 the IT assets, operations and human elements of a financial institution;

'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 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;

'network' 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;

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

'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;

'**senior management**' means -

(a) the 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;

'software' means a set of programs and supporting documentation that enable and facilitate use of any computing device such as computers and hand-held devices;[2] and

[2] Adapted from ISACA fundamentals.

'supporting documentation' means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

4. Application

4.1 This Joint Standard applies to financial institutions as defined.

4.2 A financial institution that is a bank, or a controlling company must ensure that any risks relating to IT risk from juristic persons and branches structured under the bank or the controlling company (both local and foreign), 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.

4.3 A financial institution that is an insurer or a controlling company of an insurance group must ensure that any risks relating to IT from juristic persons structured under the insurer or the controlling company (both local and foreign) and from 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.

4.4 The minimum requirements and principles set out in this Joint Standard, for the sound practices and processes of IT governance and risk management, must be implemented to reflect the nature, size, complexity and risk profile of a financial institution.

4.5 Where words such as, 'appropriate, adequate, effective, regular or periodic[3] 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.

4.6 This Joint Standard must be read in conjunction with all 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 Joint Standard.

5.2 The governing body must ensure, together with senior management, 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, execution, 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.

6.2 The IT strategy of a financial institution must be reviewed regularly, but at least annually, in consideration of market, industry, technology and other relevant developments.

6.3 A financial institution must -

[3] Including any derivatives of these words.

(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 relevance and appropriateness;
(b) establish processes to monitor and measure the effectiveness of the implementation of its IT strategy; and
(c) ensure that the responsible authority for the financial sector law in terms of which the financial institution is licensed or registered, is notified when a deviation from the IT strategy that may contravene this Joint Standard or any other financial sector law relating to IT risk management is discovered. The notification must be done in the form, manner and time-period determined by the Authorities.

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. The IT risk management framework may form part of the enterprise risk management framework of a financial institution.

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, incorporate the following -

(a) policies, standards and procedures in managing IT risks and safeguarding IT assets in the financial institution;
(b) the ability to identify, assess and manage all material risks, taking into consideration the principle of proportionality;
(c) policies, standards and procedures must be independently reviewed, and updated by the relevant business area 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 IT risk, and this function or department must be -
        (aa) accountable to the governing body, 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 and sensitivity 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 method of assessing impact of the threat and vulnerability to its IT environment which should also assist the financial institution in prioritising IT risks;

(g) implementation of appropriate practices and controls to manage 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 managed; and
  (iv) as a risk management measure, a financial institution must consider taking insurance cover for various IT risks;

(h) periodic updates and monitoring of risk assessments 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 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 assessment and managing of risks, and to facilitate risk reporting to management;
  (ii) the 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 -
  (i) the financial institution must ensure careful screening and selection of staff, service providers and contractors appointed for IT functions or services in order to minimise IT risks due to system failure, internal sabotage or fraud;
  (ii) staff, service providers and contractors appointed for IT functions or services must
    (aa) be fit and proper;
    (bb) have technical knowledge of IT solutions and IT risks; and
    (cc) be contractually required to protect sensitive or confidential information;

(iii) relevant 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, service providers and contractors who have access to the financial institution's IT 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

8.1 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 reporting lines to the governing body.

9. IT operations

9.1 A financial institution must develop a robust set of IT service management policies, standards, processes and procedures (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 referred to in paragraph 9.1 above must comprise a governance structure 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. The policies, processes and procedures must define how the financial institution operates, monitors and controls its information systems and services. This must include a register of critical IT operations and must enable the financial institution to maintain an up-to-date IT asset inventory;

(b) maintain 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;

(d) store the configuration of the IT assets and the links and interdependencies between the different IT assets, to enable an appropriate 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 IT system backup and restoration procedures to ensure recovery of IT systems as required;

(g) establish and implement an effective IT 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 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:

(a) business recovery requirements; and

(b) the criticality of the data and the IT systems, evaluated according to a performed risk assessment.

9.5 Testing of the backup and restoration procedures must be undertaken regularly, but at least annually.

9.6 A financial institution must implement appropriate segregation of duties between development, testing and operations environments, as applicable.

10. Handling of sensitive or confidential information

10.1 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 its sensitivity classification.

10.2 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 to assess compliance with the measures implemented in terms of subparagraphs (a), (b) and (c) above. 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 the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

11. Risks associated with financial products and financial services

11.1 A financial institution must clearly identify IT risks associated with the types of financial products or financial services being offered, and formulate security controls, system availability and recovery capabilities, which are

commensurate with the level of risk exposure for all operations, including the internet-facing operations.

11.2 A financial institution must -

(a) properly evaluate security requirements associated with its internet facing systems and adopt encryption algorithms which align with well-established practices and international standards;

(b) establish appropriate security monitoring systems and processes to detect or monitor IT risk exposure in relation to financial services offered;

(c) implement measures to plan and track capacity utilisation as well as guard against online attacks; and

(d) implement reasonable measures to protect IT users, including customers, who use online systems to interact with the financial institution and access and transact with its financial products and financial 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.

12. IT programme and/or project management

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

12.2 A financial institution must -

(a) establish and implement an IT programme and project management policies, procedures and processes 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 its portfolio of IT programmes and projects, considering risks that may result from interdependencies between different IT programmes and projects and from dependencies of multiple programmes and 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 governance structure;

(e) follow its 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 controls in the IT environment to ensure adequate segregation of duties between the pre-production environment that is a mirror of the production environment to mitigate the impact of risks introduced to the production systems. A financial institution must also ensure the segregation of production environments from development, testing and other non-production environments;

(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(s) 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.

13. IT resilience and business continuity

13.1 A financial institution must -

(a) define system recovery and business resumption priorities and establish specific Service Level Objectives including RTOs and RPOs for critical services and business processes;

(b) identify and establish a disaster recovery site(s) 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 resilience 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) ensure that the organisation's business resilience planning and crisis management frameworks, including effective communication, adequately address crises and disasters related to IT risk.

13.2 A financial institution must conduct a business impact assessment by analysing its exposure to severe business disruptions and assessing its potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (for example a third-party provider of data relevant to a business process or publicly available data that may be relevant to the business impact assessment) and scenario analysis.

13.3 A business impact assessment referred to in paragraph 13.2 above must also consider the criticality of the identified and classified business functions, supporting processes, third parties and IT assets, and their interdependencies.

13.4 A financial institution must develop a sound IT resilience plan.

13.5 The IT resilience plan must -

(a) specifically consider risks that could adversely impact IT systems and services;
(b) support the objective to protect and, if necessary, re-establish the confidentiality, integrity and availability of its business functions, supporting processes and IT assets;
(c) supports critical business functions, business processes, IT assets and its interdependencies (including those provided by third parties, where applicable);
(d) cater for processes to enable the return to a state of normality in the event of severe business disruption;
(e) be aligned to the business impact assessment referred to in paragraph 13.2 above, for example, with redundancy of certain critical components to prevent disruptions caused by events impacting those components.
(f) be tested regularly, but 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 resilience tests; and
(g) be reviewed regularly, but at least annually. The review must be based on, amongst others, testing results, current threat intelligence and lessons learnt from previous events.

13.6 To achieve data centre resilience, 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.

13.7 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.

13.8 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, where applicable. If bilateral or multilateral recovery testing is not possible due to significant risks, the responsible authority[4] for the financial sector law in terms of which the financial institution is licensed or registered, must be notified. The notification must be done in the form, manner and time-period determined by the Authorities.

13.9 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. IT assurance

14.1 The control functions and/or external assurance providers, must, have the capacity to independently review and provide objective assurance of compliance with all IT-related activities as outlined in the financial institution's policies and procedures as well as with external requirements.

14.2 A financial institution must through the control functions or an external assurance provider -

(a) establish an organisational structure and reporting lines for IT assurance within the control functions, where appropriate, in a way that preserves the independence and objectivity of the control functions;

[4] The responsible authority for the respective financial sector law is identified in Schedule 2 of the Act.

(b) determine whether changes in the existing operational environment influence the existing IT controls 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

(c) maintain an IT assurance plan to examine and evaluate the adequacy and effectiveness of the financial institution's IT systems, internal control mechanisms and governance arrangements.

15. Notification and reporting requirements

15.1 A financial institution must notify the responsible authority of the financial sector law in terms of which the financial institution is licensed or registered, in the form and manner determined by the Authorities, of any systems failure, malfunction, delay or other disruptive event, within the determined timeframe, after classifying the event as a material incident.

15.2 In addition, to the requirements of paragraph 15.1 above, the Authorities may, through ongoing supervisory review and evaluation processes, request for specific information or regulatory reports as well as assurance in terms of compliance with this Joint Standard.

16. Short-title

16.1 This Joint Standard is called 'IT Governance and Risk Management for Financial Institutions, 2023'.