Information Technology Governance Framework

November 2021

Version 1.0

البنك المركزي السعودي
SAMA
Saudi Central Bank

Table of Contents

1. Introduction

1.1 Introduction to the Framework

The current digital society has high expectations of flawless customer experience and continuous availability of services. The advancement of information technology ("IT") has brought rapid changes to the way businesses and operations are being conducted in the financial sector. Although IT plays an essential role combined with today's environment, it also exposes financial institutions to dynamically evolving IT risks.

In this regard, Saudi Central Bank ("SAMA") has established an Information Technology Governance Framework ("the Framework") to enable organizations regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to IT. The objective of the Framework is as follows:

1. To create a common approach for addressing IT risks within the Member Organizations.
2. To achieve an appropriate maturity level of IT controls within the Member Organizations.
3. To ensure IT risks are properly managed throughout the Member Organizations.

The framework will be used to periodically assess the maturity level and evaluate the effectiveness of the IT controls at Member Organizations. The framework is based on the SAMA requirements and industry IT standards.

1.2 Definition of Information Technology Governance

An Information Technology (IT) governance ensures the effective and efficient use of IT to enable Member Organizations to achieve its goals and objectives. It enables Member Organizations formulating optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

1.3 Scope

The framework defines principles and objectives for initiating, implementing, maintaining, monitoring and improving IT governance controls within Member Organizations regulated by SAMA. The framework offers IT governance controls requirements which are applicable to the information assets of the Member Organizations. Additionally, the framework provides direction for IT Governance requirements for Member Organizations and its subsidiaries, staff, third parties and customers. The framework should be implemented in conjunction with SAMA's Cyber Security and Business Continuity framework respectively (figure 1). For specific Cyber Security and Business Continuity related requirements please refer to SAMA's Cyber Security Framework and Business Continuity Management Framework.

Figure 1 – Relationship between SAMA Frameworks

The Framework has an interrelationship with other corporate policies for related areas, such as change management and staff training. This framework does not address the non-IT requirements for those areas.

1.4 Applicability

The framework is applicable to Member Organizations regulated by SAMA.

1.5 Responsibilities

The framework is mandated by SAMA and will be circulated to Member Organizations for implementation. SAMA is the owner and is responsible for periodically updating the framework. The Member Organizations are responsible for implementing and complying with the framework.

1.6 Interpretation

SAMA, as the owner of the framework, is solely responsible for providing interpretations of the principles and Control Requirements, if required.

1.7 Target Audience

The Framework is intended for senior and executive management, business owners, owners of information assets, CIOs and those who are responsible for and involved in defining, implementing and reviewing IT controls within the Member Organizations.

1.8 Review, Updates and Maintenance

SAMA will review the Framework periodically to determine the Framework's effectiveness, including the effectiveness of the Framework to address emerging IT threats and risks. If applicable, SAMA will update the Framework based on the outcome of the review.

If a Member Organization considers that an update to the framework is required, the Member Organization should formally submit the requested update to SAMA. SAMA will review the requested update, and when applicable, the Framework will be adjusted on the next updated version.

The Member Organization will remain responsible to be compliant with the framework pending the next version update.

Please refer to 'Appendix A – How to request an Update to the Framework' for the process of requesting an update to the Framework.

Version control will be implemented for maintaining the framework. Whenever any changes are made, the preceding version shall be retired and the new version shall be published and communicated to all Member Organizations. For the convenience of the Member Organizations, changes to the framework shall be clearly indicated.

1.9 Reading Guide

The Framework is structured as follows. Chapter 2 elaborates on the structure of the Framework, and provides instructions on how to apply the Framework. Chapter 3 presents the actual framework, including the IT domains and subdomains, principles, objectives and Control Requirements.

2. Framework Structure and Features

2.1 Structure

The Framework is structured around four main domains, namely:

- Information Technology Governance and Leadership.
- Information Technology Risk Management.

- Information Technology Operations Management.
- System Change Management.

For each domain, several subdomains are defined. A subdomain focusses on a specific IT governance topic. Per subdomain, the Framework states a principle and Control Requirements.

- A **Principle** summarizes the main set of required IT controls related to the subdomain.
- The **Control Requirements** reflects the mandated IT controls that should be considered.

The framework should be implemented in view of principles mentioned in per subdomains along with its associated Control Requirements.

Control Requirements have been uniquely numbered according to the following numbering system throughout the Framework:

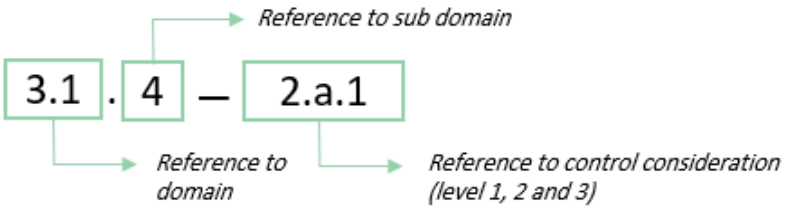


Figure 2 – Control requirements numbering system

The figure below illustrates the overall structure of the Framework and indicates the IT Governance Framework domains and subdomains, including a reference to the applicable section of the Framework.

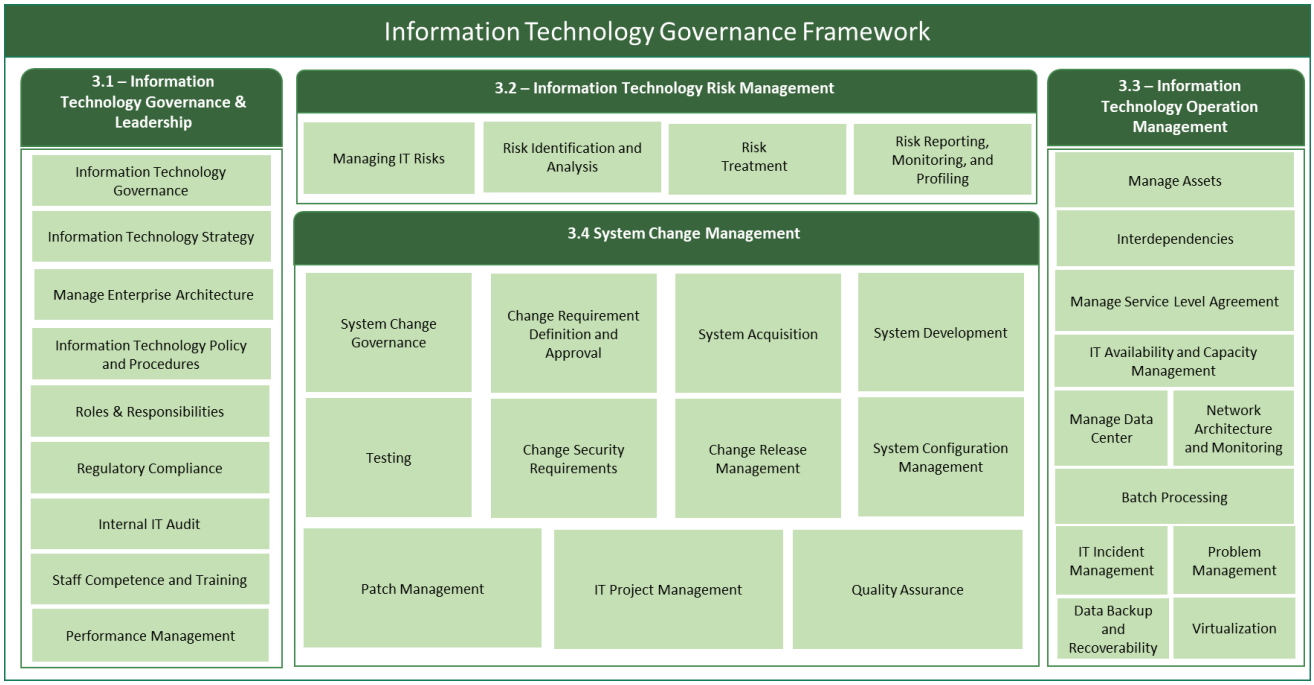


Figure 3 – Information Technology Governance Framework

2.2 Principle-based

The framework is principle based, also referred to as risk based. This means that it prescribes key IT governance principles and objectives to be embedded and achieved by the Member Organizations. The list of mandated Control Requirements provides additional direction and should be considered by the Member Organizations in achieving the objectives. When a certain control requirements cannot be tailored or implemented, the

Member Organizations should consider applying compensating controls, pursuing an internal risk acceptance and requesting a formal waiver from SAMA. Please refer to Appendix D for details for the – How to request a Waiver from the Framework – process.

2.3 Self-Assessment, Review and Audit

The implementation of the framework at the Member Organizations will be subject to a periodic self-assessment. The self-assessment will be performed by the Member Organizations based on a questionnaire. The self-assessments will be reviewed and audited by SAMA to determine the level of compliance with the framework and the IT maturity level of the Member Organizations. Please refer to '2.4 Information Technology Governance Maturity Model' for more details about the information technology governance maturity model.

2.4 Information Technology Governance Maturity Model

The Information Technology Governance maturity level will be measured with the help of a predefined maturity model. The information technology governance maturity model distinguishes 6 maturity levels (0, 1, 2, 3, 4 and 5), which are summarized in the table below. In order to achieve levels 3, 4 or 5, Member Organizations should first meet all criteria of the preceding maturity levels.

Maturity Level	Definition and Criteria	Explanation
0 Non-existent	• No documentation. • There is no awareness or attention for certain information technology control.	• IT controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such IT controls.
1 Ad-hoc	• IT controls is not or partially defined. • IT controls are performed in an inconsistent way. • IT controls are not fully defined.	• IT control design and execution varies by department or owner. • IT control design may only partially mitigate the identified risk and execution may be inconsistent.
2 Repeatable but informal	• The execution of the IT control is based on an informal and unwritten, though standardized, practice.	• Repeatable IT controls are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideration for a structured review or testing of a control.
3 Structured and formalized	• IT controls are defined, approved and implemented in a structured and formalized way. • The implementation of IT controls can be demonstrated.	• IT policies, standards and procedures are established. • Compliance with IT documentation i.e., policies, standards and procedures is monitored, preferably using a governance, risk and compliance tool (GRC). • Key performance indicators are defined, monitored and reported to evaluate the implementation.
4 Managed and measurable	• The effectiveness of the IT controls are periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of IT controls are measured and periodically evaluated. • Key risk indicators and trend reporting are used to determine the effectiveness of the IT controls. • Results of measurement and evaluation are used to identify opportunities for improvement of the IT controls.
5 Adaptive	• IT controls are subject to a continuous improvement plan.	• The enterprise-wide IT governance program focuses on continuous compliance, effectiveness and improvement of the IT controls. • IT controls are integrated with enterprise risk management framework and practices. • Performance of IT controls are evaluated using peer and sector data.

Table 1 - Information technology governance Maturity Model

2.4.1 Maturity Level 3

To achieve level 3 maturity, a Member Organization should define, approve and implement IT controls. In addition, it should monitor compliance with the IT documentation. The IT documentation should clearly indicate “why”, “what” and “how” IT controls should be implemented. The IT documentation consists of IT policies, standards and procedures.

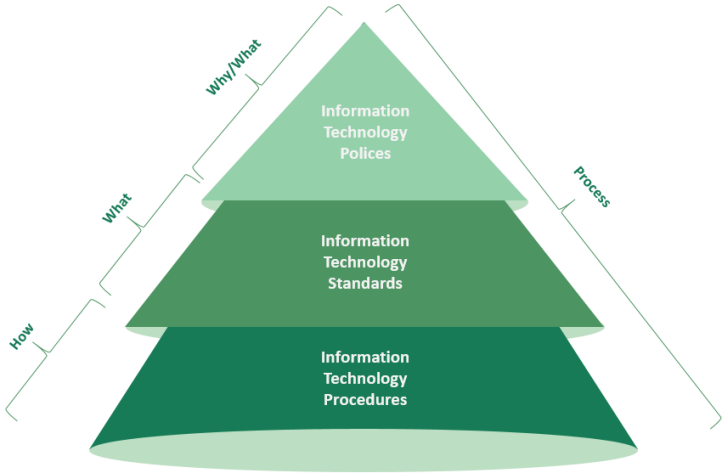


Figure 4 – Information Technology Documentation Pyramid

The IT policy should be endorsed and mandated by the board of the Member Organization and stating “why” IT is important to the Member Organization. The policy should highlight which information assets should be protected and “what” IT principles and objectives should be established.

Based on the IT policy, IT standards should be developed. These standards define “what” IT controls should be implemented, such as, segregation of duties, back-up and recovery rules, etc. The standards support and reinforce the IT policy and are to be considered as IT baselines.

The step-by-step tasks and activities that should be performed by staff of the Member Organization are detailed in the IT procedures. These procedures prescribe “how” the IT controls, tasks and activities have to be executed in the operating environment.

The process in the context of this framework is defined as a structured set of activities designed to accomplish the specified objective. A process may include policies, standards, guidelines, procedures, activities and work instructions, as well as any of the roles, responsibilities, tools and management controls required to reliably deliver the output.

The actual progress of the implementation, performance and compliance of the IT controls should be periodically monitored and evaluated using key performance indicators (KPIs).

2.4.2 Maturity Level 4

To achieve maturity level 4, Member Organizations should periodically measure and evaluate the effectiveness of implemented IT controls. In order to measure and evaluate whether the IT governance controls are effective, key risk indicators (KRIs) should be defined. A KRI indicates the norm for effectiveness measurement and should define thresholds to determine whether the actual result of measurement is below, on, or above the targeted norm. KRIs are used for trend reporting and identification of potential improvements.

2.4.3 Maturity Level 5

Maturity level 5 focuses on the continuous improvement of IT controls. Continuous improvement is achieved through continuously analyzing the goals and achievements of IT governance and identifying structural improvements. IT controls should be integrated with enterprise risk management practices and supported with automated real-time monitoring. Business process owners should be accountable for monitoring the compliance of the IT controls, measuring the effectiveness of the IT controls and incorporating the IT controls within the enterprise risk management framework. Additionally, the performance of IT controls should be evaluated using peer and sector data.

3. Control domains

3.1 Information Technology Governance and Leadership

Member Organizations board is ultimately responsible for setting the Information Technology (IT) Governance and ensuring that IT risks are effectively managed within the Member organization. The board of the Member Organization can delegate its IT Governance responsibilities to senior management or IT steering committee (ITSC). The ITSC could be responsible for defining the IT governance and setting the Member Organization's IT strategy.

3.1.1 Information Technology Governance

Principle

An IT Governance structure should be defined, endorsed and supported with appropriate resources to oversee and control the Member Organization's overall approach to Information Technology.

Control Requirements

1. Member organizations should establish ITSC and be mandated by the board.
2. The ITSC should be headed by senior manager responsible for Member Organizations operations.
3. The following positions should be represented in the ITSC:
   a. senior managers from all relevant departments (e.g., CRO, CISO, compliance officer, heads of relevant business departments);
   b. Chief Information Officer (CIO); and
   c. Internal Audit may attend as an "observer".
4. An ITSC charter should be developed, approved and reflect the following:
   a. committee objectives;
   b. roles and responsibilities;
   c. minimum number of meeting participants;
   d. meeting frequency (minimum on quarterly basis); and
   e. documentation and retention of meeting minutes and decisions.
5. A full-time senior manager for the IT function, referred to as CIO, should be appointed at senior management level.
6. The Member Organizations should:
   a. ensure the CIO is a Saudi national;
   b. ensure the CIO is sufficiently qualified; and
   c. obtain a written no objection letter from SAMA prior to assigning the CIO.
7. The Member Organizations should establish formal practices for IT-related financial activities covering budget, cost, and prioritization of spending aligned with IT strategic objectives.
8. The overall IT budget should be monitored, reviewed periodically and adjusted accordingly to meet the IT and business needs.
9. Member Organizations should define roles and responsibilities of senior management and IT staff using a responsibility assignment matrix, also known as RACI. The RACI matrix should outline who are responsible and accountable for the functions, as well as who should be consulted or informed.
10. Member organizations should define enterprise architecture reflecting fundamental components of the business processes and its supporting technology layers to ensure responsive and efficient delivery of strategic objectives.
11. Member Organizations should define enterprise application architect role within the IT function to identify the required changes to the portfolio of applications across the member organizations ecosystem.
12. Roles and responsibilities within IT function should be:
    a. documented and approved by the management; and
    b. segregated to avoid conflict of interest.

13. Member Organizations should develop formal IT succession plan in coordination with Human Resource (HR) Department taking into consideration the reliance on a key IT staff having critical roles and responsibilities.

3.1.2 Information Technology Strategy

Principle

An IT strategy should be defined in alignment with the Member Organization's strategic objectives and in compliance with legal and regulatory requirements.

Control Requirements

1. IT strategy should be defined, approved, maintained and executed.
2. IT strategic initiatives should be translated into defined roadmap considering the following:
   a. the initiatives should require closing the gaps between current and target environments;
   b. the initiatives should be integrated into a coherent IT strategy that aligns with the business strategy;
   c. the initiatives should address the external ecosystem (enterprise partners, suppliers, start-ups, etc.); and
   d. should include determining dependencies, overlaps, synergies and impacts among projects, and prioritization.
3. IT strategy should be aligned with:
   a. the Member Organization's overall business objectives; and
   b. legal and regulatory compliance requirements of the Member Organization.
4. IT strategy at minimum should address:
   a. the importance and benefits of IT for the Member Organization;
   b. the current business and IT environment, the future direction, and the initiatives required to migrate to the future state environment; and
   c. interdependencies of the critical information assets.
5. Member organization should identify IT strategic and emerging technology risks that may have impact on the achievement of overall organization wide strategic objectives.
6. Member organization should enhance skill sets and expertise (operational and technical) of the existing resources through providing periodic training on emerging technologies and if required to have the relevant resources on boarded in line with member organization direction towards digitalization.
7. IT strategy should be reviewed and updated periodically or upon material change in the Member Organizations operational environment, change in business strategy, objectives or amendment in laws & regulations.

3.1.3 Manage Enterprise Architecture

Principle

Enterprise architecture should be defined which outlines fundamental components of the business processes, data and supporting technology layers to ensure responsive and efficient delivery of Member organizations IT strategic objectives.

Control Requirements

1. The enterprise architecture should be defined, approved and implemented.
2. The compliance with the enterprise architecture should be monitored.
3. The enterprise architecture should address the following, but not limited to:
   a. a strategic outline of organizations technology capabilities;
   b. outline the gaps between baseline and target architectures, taking both business and technical perspectives; and
   c. agility to meet changing business needs in an effective and efficient manner.

3.1.4 Information Technology Policy and Procedures

Principle

IT policy and procedures should be defined, approved, communicated and implemented to set member organizations commitment and objectives to IT and communicated to the relevant stakeholders.

Control Requirements

1. IT policy and procedures should be defined, approved, communicated, and implemented.
2. IT policy and procedures should be reviewed periodically taking into consideration the evolving technology landscape.
3. IT Policy should be developed considering input from relevant member organizations policies (e.g. cyber security, finance, HR).
4. IT Policy should include:
    a. the Member Organization's overall IT objectives and scope;
    b. a statement of the board's intent, supporting the IT objectives;
    c. a definition of general and specific responsibilities for IT; and
    d. the reference to supporting IT (inter)national standards and process (where applicable).

3.1.5 Roles and Responsibilities

Principle

IT roles and responsibilities should be defined and all parties involved in the Member Organization's IT processes should have an adequate level of understanding of the expectations related to their role.

Control Requirements

1. The board should be accountable for:
    a. the ultimate responsibility for the establishment of IT governance practice;
    b. ensuring that robust IT risk management framework is established and maintained to manage IT risks;
    c. ensuring that sufficient budget for IT is allocated;
    d. approving the IT steering committee (ITSC) charter; and
    e. endorsing (after being approved by the ITSC):
        1. the governance and management practices roles and responsibilities;
        2. the IT strategy; and
        3. the IT policy.
2. ITSC, at a minimum, should be responsible for:
    a. monitoring, reviewing and communicating the Member Organization's IT risks periodically;
    b. approving, communicating, supporting and monitoring:
        1. IT strategy;
        2. IT policies;
        3. IT risk management processes; and
        4. key performance indicators (KPIs) and key risk indicators (KRIs) for IT.
3. The CIO, at minimum, should be accountable for:
    a. developing, implementing and maintaining:
        1. IT strategy;
        2. IT policy; and
        3. IT budget.
    b. ensuring that detailed IT standards and procedures are established, approved and implemented;
    c. delivering risk-based IT solutions that address people, process and technology;
    d. defining and maintaining specific key performance indicators (KPIs) and key risk indicators (KRIs) for IT processes;
    e. periodically inform ITSC on the latest developments on IT strategic initiatives and its implementation status;

f. implementing adequate technology to streamline all internal operations and help optimize their strategic benefits;
g. the IT activities across the Member Organization, including:
    1. monitoring of the IT operation;
    2. monitoring of compliance with IT regulations, policies, standards and procedures; and
    3. overseeing the investigation of IT related incidents.
h. analyzing IT costs, value and risks to advise COO/Managing director; and
i. defining IT training plan in coordination with HR.

4. The internal audit function should be responsible for:
    a. the identification of comprehensive set of auditable areas for IT risk and performance of effective IT risk assessment during audit planning; and
    b. performing IT audits.
5. The enterprise application architect, at minimum should be responsible for:
    a. developing of IT ecosystem application architecture models, processes and documentation;
    b. developing enterprise level application and custom integration solutions including major enhancements and interfaces, functions and features; and
    c. ensuring continuous improvement to transition between current and future states of the application architectures.
6. All Member Organization's staff should be responsible for complying with applicable IT policy, standards and procedures.

3.1.6 Regulatory Compliance

Principle

Relevant regulations including data privacy should be identified, communicated and complied which are affecting IT operations of the Member Organizations.

Control Requirements

1. Member Organizations should establish a process ensuring compliance with IT related regulatory requirements. The process of ensuring compliance should:
    a. be performed periodically or when new regulatory requirements become effective;
    b. involve representatives from key areas of the Member Organization;
    c. result in the update of IT policy, standards and procedures to accommodate any necessary changes (if applicable); and
    d. maintain an up-to-date log of all relevant legal, regulatory and contractual requirements; their impact and required actions.

3.1.7 Internal IT Audit

Principle

IT Audit should be conducted in accordance with generally accepted auditing standards and relevant SAMA framework (s) to verify that the IT control design is adequately implemented and operating as intended.

Control Requirements

1. IT audits should be performed independently and according to generally accepted auditing standards and relevant SAMA frameworks.
2. The Member Organizations should establish an audit cycle that determines the frequency of IT audits.
3. Member Organizations should develop formal IT audit plan addressing people, process and technology components.
4. IT audit plan should be approved by the Member Organization's audit committee.
5. The frequency of IT audit should be aligned with the criticality and risk of the IT system or process.
6. A follow-up process for IT audit observations should be established to track and monitor IT audit observations.

7. Member Organizations should ensure that the IT auditors have the requisite level of competencies and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.
8. IT audit report, at a minimum, should:
    a. include the findings, recommendations, management's response with defined action plan, and responsible party and limitations in scope with respect to the IT audits;
    b. signed, dated and distributed according to the format defined; and
    c. submitted to the audit committee on periodical basis.

3.1.8 Staff Competence and Training

Principle

Staff of the Member Organizations should be equipped with the skills and required knowledge to operate the Member Organization's information assets in a controlled manner and provided with training regarding how to operate, address and apply IT relevant controls on Member Organization's information assets.

Control Requirements

1. Member Organizations should identify and define critical roles within IT department (e.g. DBA, sysadmin, etc.)
2. Member Organizations should ensure adequate staffing for critical IT roles, such that critical IT roles are not handled by only one staff.
3. Member Organizations should identify the professional certifications required for staff responsible for critical IT roles.
4. Member Organizations should evaluate staffing requirements on periodic basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources.
5. Annual IT training plan should be developed by the Member Organizations.
6. Formal training should be conducted, as a minimum for:
    a. IT staff (existing and new); and
    b. Contractors (where applicable).
7. IT training plan should be reviewed periodically.
8. Specialist training should be provided to staff in the Member Organization's relevant functional area categories in line with their job descriptions, including:
    a. staff involved in performing critical IT roles;
    b. staff involved in developing and (technically) maintaining information assets; and
    c. staff involved in risk assessments.

3.1.9 Performance Management

Principle

Efficiency and effectiveness of IT processes and services of the Member Organizations should be continuously measured through key performance indicators (KPIs).

Control Requirements

1. KPIs should be defined, approved and implemented to measure the execution of IT processes and system performance.
2. KPIs should be defined considering for the following, but not limited to:
    a. IT function and related processes;
    b. workforce competency and development; and
    c. compliance with regulatory regulations.
3. KPIs should be:
    a. communicated to the concerned IT Divisions/Units of the Member Organizations for implementation;
    b. supported by target value and thresholds;
    c. analyzed to identify the deviations against targets and initiate remedial actions;

d. analyzed to identify trends in performance and compliance and take appropriate action; and
e. monitored and periodically reported to the senior management and ITSC.

3.2 IT Risk Management

IT Risk Management is a continues process of identifying, analyzing, responding, monitoring, and reviewing risks related to IT from process, technology and people perspectives. In order to manage IT risks, Member Organizations should continually identify, assess and reduce IT risks within levels of tolerance set by the Member Organization's senior management.

3.2.1 Managing IT Risks

Principle

IT Risk Management process should be defined, approved, implemented, communicated and aligned to the Member Organization's Enterprise Risk Management process, including the identification, analysis, treatment, monitoring and review of IT risks at appropriate intervals.

Control Requirements

1. IT risk management process should be defined, approved, implemented and communicated.
2. The effectiveness of the IT risk management process should be measured and periodically evaluated.
3. IT risk management process should be aligned with the Member Organization's enterprise risk management process.
4. IT risk management process should clearly address the following sub processes, including but not limited to:
   a. risk identification, analysis and classification;
   b. risk treatment;
   c. risk reporting; and
   d. risk monitoring and profiling.
5. IT risk management process should address Member Organization's information assets, including but not limited to:
   a. business processes and related data;
   b. business applications;
   c. infrastructure components; and
   d. Third party relationships and associated risks.
6. IT risk management process should address Member Organization's people aspect (i.e. permanent staff, contractual employees, third party).
7. IT risk management process should be initiated at, but not limited to:
   a. an early stage of the program and project implementation;
   b. prior to initiate critical and major changes to the information assets;
   c. the time of outsourcing services; and
   d. prior to procuring of new systems, tools and emerging technologies (i.e. Distributed Ledger Technology (DTL), Robotic Process Assurance (RPA) etc.)
8. Existing information assets should be subject to periodic IT risk assessment based on their criticality such as:
   a. all mission critical and critical information assets should be assessed at least once a year; and
   b. non-critical information assets should be assessed based on their importance to the business.
9. IT risk management activities should involve the following stakeholders, but not limited to:
   a. business owners and users;
   b. IT departmental/functional heads;
   c. technical administrators; and
   d. cyber security specialists.

10. The Member Organization's should develop and implement IT risk response (i.e. avoid, mitigate, transfer and accept) and control strategies that are consistent with the value of the information assets and member organizations risk appetite.
11. IT key risk indicators (KRIs) should be defined, implemented and monitored.

3.2.2 Risk Identification and Analysis

Principle

Information assets should be identified, recorded and maintained to gather information about related threats, existing controls and associated risks should be analyzed based on their likelihood of occurrences and resulting impact.

Control Requirements

1. IT risk identification should be performed, documented and periodically updated in the formal centralized risk register.
2. IT risk register should be regularly updated.
3. IT risk analysis should address the following, but not limited to:
    a. information asset description and classification;
    b. potential threat(s) to the information asset;
    c. impact and likelihood;
    d. existing IT controls;
    e. risk owner (business or process owner);
    f. implementation owner (control owner); and
    g. inherent as well as residual risks related to the information assets.

3.2.3 Risk Treatment

Principle

IT risks associated with the Member Organization's information assets should be adequately treated based on the applicable criteria (i.e. accepted, avoided, transferred or mitigated).

Control Requirements

1. IT risk treatment plan should be defined, approved and communicated.
2. IT risk treatment plan should be implemented and periodically evaluated.
3. IT risks should be treated according to the Member Organization's risk appetite defined by the relevant governance function owner and approved by the ITSC.
4. IT risk treatment plan should include detail design and implementation of required controls to mitigate the identified risks.
5. IT risk treatment plan should ensure that the list of risk treatment options are formally documented (i.e. accepting, avoiding, transferring or mitigating risks by applying IT controls).
6. Risk acceptance should be least preferred over risk mitigation through implementation of primary controls.
7. Accepting IT risks should be formally documented, approved and signed-off by the business owner and reported to the risk committee, ensuring that:
    a. risk acceptance should be provided with detail justification including but not limited to the following:
        1. impact (i.e. operational, financial and reputational) of not implementing the primary control(s); and
        2. compensating control(s) in place of primary control(s) for risk mitigation.
    b. the accepted IT risk should be within the risk appetite of the Member Organization;
    c. the accepted IT risk should not contradict with the SAMA regulations;
    d. a separate exception should be documented for each unique risk;
    e. risk acceptance should be renewed periodically; and
    f. Risk acceptance should be presented and reported to the risk committee.
8. Avoiding IT risks should involve a decision by a business owner and risk committee to cancel or postpone a particular activity or project that introduces an unacceptable IT risk to the business.

9. Transferring or sharing the IT risks should:
    a. involve sharing the IT risks with relevant (internal or external) providers; and
    b. be accepted by the receiving (internal or external) provider(s).
10. Applying IT controls to mitigate IT risks should include:
    a. identifying appropriate IT controls;
    b. evaluating the strengths and weaknesses of the IT controls;
    c. selection of adequate IT controls; and
    d. documenting and obtaining sign-off for any residual risk by the business owner and risk committee.
11. IT risk treatment actions should be documented in a risk treatment plan.

3.2.4 Risk Reporting, Monitoring, and Profiling

Principle

IT risks should be treated according to the defined treatment plans and should be effectively reviewed, monitored and reported.

Control Requirements

1. IT risk assessment results should be formally documented and reported to the relevant business owners and senior management.
2. IT risk assessment results should include risks, impact, likelihood, mitigations, and remediation status.
3. IT risks should be monitored, including but not limited to:
    a. tracking progress in accordance to the risk treatment plan; and
    b. the selected and agreed IT controls are being implemented.
4. The design and operating effectiveness of the revised or newly implemented IT controls should be monitored and reviewed periodically.
5. The relevant business owners should accept the IT risk assessment results.
6. IT risk assessment results should be endorsed by the risk committee.
7. IT key risk indicators (KRIs) should be defined, implemented and monitored.
8. IT risk profile and related data should be provided as an input to operational risk department to formulate an organization level risk profile.
9. IT risk profile should be formulated and presented to the senior management, IT Steering Committee and board of directors on periodic basis.

3.3 Operations Management

IT Operations Management can be defined as the function responsible for continues management and maintenance of the Members Organization's IT applications and infrastructure to ensure delivery of the agreed level of IT services to the business. Thus, IT operations risk factors should be addressed by the Member Organizations through effective management and control.

3.3.1 Manage Assets

Principle

Asset Management process should be established to provide visibility of the Member Organization's information assets by maintaining an accurate and up-to-date inventory.

Control Requirements

1. The asset management process should be defined, approved, implemented and communicated.
2. The effectiveness of the asset management process should be monitored, measured and periodically evaluated.
3. The asset management process should include but not limited to:
    a. asset onboarding;
    b. asset identification, classification, labeling and handling;
    c. asset disposal; and

d. asset decommissioning.

4. Asset register should provide with the level of details, including (but not limited):
   a. asset name;
   b. asset owner;
   c. asset custodian; asset criticality;
   d. asset physical location;
   e. asset logical location (network zone);
   f. asset identified as direct in-scope of PCI;
   g. asset identified as indirect in-scope of PCI;
   h. availability or backup information;
   i. service contract or license information;
   j. technical contacts (OS, Application, Database and Network);
   k. primary and secondary processes supported by the asset;
   l. acceptable downtime aligned with BCM - Business Impact Analysis where applicable;
   m. financial impact per hour in the event of downtime;
   n. vendor engagement contract number;
   o. vendor point of contact details;
   p. vendor SLA details; and
   q. vendor classification details.
5. Asset register should be maintained and updated on yearly basis, or whenever any asset introduced or removed from inventory.
6. Member organizations should:
   a. define criteria for the identification of critical assets;
   b. identify, maintain and periodically update comprehensive list of critical assets;
   c. proactively monitor performance of critical assets; and
   d. ensure adequate resilience measures in place for critical assets to maintain availability of the required critical services.
7. Asset owner should be responsible for, but not limited to:
   a. classification and labeling of asset;
   b. defining and reviewing access rights, restrictions, and taking into account applicable access control policies of the Member Organizations;
   c. authorizing changes related to assets; and
   d. ensure alignment with cyber security controls.
8. Assets should be disposed of in a controlled and secure manner upon completion of its useful life and when other relevant obligations are met.

3.3.2 Interdependencies

Principle

Interdependencies for critical information assets should be identified and managed through governance model to ensure availability of business operations.

Control Requirements

1. Member Organizations should define and implement robust governance model in light of their interdependencies with relevant stakeholders (e.g. service providers, government institutions, etc.)
2. Member Organizations should identify its critical information assets interdependencies.
3. As part of the BCP testing, the Member Organizations should take into consideration the interdependencies of critical information assets scenarios within its infrastructure.

Note: For more Control Requirements to improve the overall resilience, please refer to the SAMA – BCM Framework.

3.3.3 Manage Service Level Agreements

Principle

Contractual terms and conditions governing the roles, relationships, obligations and responsibilities of internal stakeholder and third parties should be formally agreed, developed and adequately controlled.

Control Requirements

1. Internal IT Service Level Agreement (SLA) should be formally defined, approved, and communicated to the relevant business department of the Member Organizations.
2. The effectiveness of the internal IT SLA should be monitored, measured, and periodically evaluated.
3. Internal IT SLA should include the following, but not limited to:
   a. service level agreed between the business functions and the IT department;
   b. specific and measurable targets for IT services against the defined KPI's; and
   c. roles and responsibilities of the business and IT stakeholders.
4. The third party relationship process should be defined, approved, implemented, and communicated.
5. The effectiveness of the third party relationship process should be monitored, measured, and periodically evaluated.
6. Formal SLA should be defined and signed with the third party.
7. The third party relationship process should cover following requirements, but not limited to:
   a. outsourcing service providers should have adequate process in place to ensure availability, protection of data and applications outsourced;
   b. periodic reporting, reviewing and evaluating the contractually agreed requirements (in SLAs);
   c. changes to the provision of provided services;
   d. execution of a risk assessment as part of the procurement process;
   e. escalation process in case of SLA breached;
   f. administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of information;
   g. legal assurance from the third party to provide onsite support that mandates onsite presence of certified and experienced relevant support engineer within a defined timeline to support the Member Organizations in adverse situations;
   h. exiting, terminating, or renewing the contract (including escrow agreements if applicable);
   i. compliance with applicable frameworks including but not limited to SAMA Cyber Security, Business Continuity Management and IT Governance Frameworks-and applicable Laws and Regulations;
   j. right to audit (Member Organizations or independent party) ; and
   k. Non-Disclosure Agreement ('NDA').

3.3.4 IT Availability and Capacity Management

Principle

Service availability should be maintained to support member organizations business functions and to avoid disruption and slowness of systems performance through monitoring current system thresholds and prediction of future performance and capacity requirements.

Control Requirements

1. The IT availability and capacity management process should be defined, approved and implemented.
2. The effectiveness of the IT availability and capacity management process should be monitored, measured and periodically evaluated.
3. IT availability and capacity plan should be developed, approved and periodically evaluated.
4. IT availability and capacity plan should be defined to address the following, but not limited to:
   a. existing capacity of systems and resources;
   b. alignment with the current and future business needs;
   c. high availability requirements (including disruption and slowness for customer channels);
   d. roles and responsibilities to maintain the plan; and

e. identification of dependencies over service providers as part of capacity planning to address BCM requirements.

5. System performance thresholds should be defined and implemented.
6. System performance should be monitored considering the following, but not limited to:
   a. current and future business requirement;
   b. the agreed upon SLA with the business;
   c. critical IT infrastructures;
   d. disruption and slowness in the underlying system(s) supporting customer channels; and
   e. lessons learned from previous system performance issues.
7. Deviations from established capacity and performance baselines/thresholds should be identified, documented, followed-up, and reported to the management and ITSC.

3.3.5 Manage Data Center

Principle

Adequate physical controls are designed and implemented to protect IT facilities and equipment from damage and unauthorized access.

Control Requirements

1. Physical and environmental controls for managing the data center should be defined, approved and implemented.
2. Physical and environmental controls should be monitored and periodically evaluated.
3. Necessary physical and environmental controls should be implemented such as but not limited to:
   a. access to the data center should be strictly controlled and provided on need to know basis;
   b. visitors entry to data center should be logged and escorted by an authorized person;
   c. smoke detectors;
   d. fire alarms;
   e. fire extinguishers;
   f. humidity control;
   g. temperature monitoring; and
   h. CCTV.
4. The outsourcing of data center should comply with the requirements published in the SAMA circulars on the Rules of The Outsourcing and Cybersecurity Framework.
5. Member Organizations should ensure that appropriate control measures are built into contracts with the service providers to whom they plan to outsource data center such as but not limited to:
   a. have documented business case for outsourcing data center services; and
   b. nature and type of access to data center by the service provider.

3.3.6 Network Architecture and Monitoring

Principle

IT event management and network architecture controls should be designed and implemented to continuously monitor IT operations in order to protect member organizations network from unauthorized access.

Control Requirements

1. Member Organizations should define, approve and implement network architecture policy considering the following:
   a. organization's stance with respect to acceptable network usage;
   b. explicit rules for the secure use of specific network resources, services and applications;
   c. consequences of failure to comply with security rules;
   d. organization's attitude towards network abuse; and
   e. rationale(s) for the policy, and for any specific security rules.

2. Member Organizations should ensure the implementation of following network architecture controls, but not limited to:
   a. network diagram showing the complete current infrastructure;
   b. segmentation of network into multiple separate network domains based on the required trust levels (e.g. public domain, desktop domain, server domain) and in line with relevant architectural principles;
   c. perimeter of each network domain should be well protected by a security gateway (e.g. firewall, filtering router). For each security gateway a separate service access (security) rules should be developed and implemented to ensure that only the authorized traffic is allowed to pass;
   d. all internal traffic (head office users, branch users, third party users, etc.) passing to DMZ or internal servers should pass via a security gateway (firewall);
   e. all outbound internet access from internal networks are routed via proxy server such that access is allowed only to approved authenticated users;
   f. visitor network (wired/wireless network) should be isolated and segregated from the internal network;
   g. the perimeter firewall to the DMZ should raise an alert and block active scanning;
   h. web application firewall (WAF) should be implemented against customer facing applications;
   i. ensure non-existence of single node of failure that affects the critical service availability;
   j. centralized authentication server (AAA, TACACS or RADIUS, etc.) should be deployed for managing authentication and authorization of network devices;
   k. centralized log server (e.g. syslog server) should be deployed to collect and store logs from all network devices;
   l. retention period for logs should be 12 months minimum;
   m. all network devices should synchronize their clock timings from a centralized NTP server;
   n. all network communication over extranet (WLAN) and internet should be through an encrypted channel;
   o. remote access should be restricted only to certain group of IP addresses;
   p. remote administration should be over an encrypted channel (like SSL VPN, SSH);
   q. remote administration access for vendors should be time-bound and granted on a need basis with approval;
   r. scan for Member Organization's devices before accessing the network to ensure enforcement of security policies on devices before they access organization's network; and
   s. segregation of duties within the infrastructure component (supported with a documented authorization profile matrix).
3. Member Organizations should ensure that network monitoring is performed considering the following, but not limited to:
   a. administrative trails including login and activity trails (like configuration change, rule change, etc.);
   b. resource utilization (processor and memory); and
   c. network connectivity to all branches and ATMs.

3.3.7 Batch Processing

Principle

Batch management process should be defined, approved and implemented in order to manage the bulk processing of automated tasks in an efficient and controlled manner.

Control Requirements

1. Batch management process should be defined, approved, implemented and communicated.
2. The effectiveness of the Batch management process should be measured and periodically evaluated.
3. Batch Management process should include the following, but not limited to:
   a. start and end of day schedules;
   b. roles and responsibilities;
   c. monitoring of batches; and
   d. error or exception handling.

4. Changes in the batch schedules should be approved by the relevant stakeholder(s).
5. Member organizations should maintain log containing information about start and end of the day batch operations along with its status e.g. (successful or unsuccessful).

3.3.8 IT Incident Management

Principle

IT incident Management process should be established to timely identify, respond and handle IT incidents impacting the Member Organization's information assets and to report relevant incidents to SAMA, according to a defined communication protocol.

Control Requirements

1. IT incident management process should be defined, approved, implemented and communicated.
2. The effectiveness of the IT incident management process should be measured and periodically evaluated.
3. IT incident management process should include the following requirements, but not limited to:
   a. the establishment of a designated team responsible for incident management;
   b. communication plan;
   c. details of key staff who need to be notified;
   d. skilled and (continuously) trained staff;
   e. the prioritization and classification of incidents;
   f. the timely handling of incidents, recording and monitoring progress;
   g. the protection of relevant evidence and loggings;
   h. post-incident activities such as root-cause analysis of the incidents; and
   i. lessons learned.
4. IT incident management process should be automated such as through IT service desk.
5. A process should be established for documenting the details of incident, steps taken which were successful and which were not successful, should be communicated to the relevant IT staff for hands on experience and also for future reference to enhance efficiency.
6. All user requests and IT incident should be logged with the following information but not limited to:
   a. unique reference number;
   b. date and time;
   c. name of the impacted services and systems;
   d. update the relevant owner; and
   e. categorization and prioritization based on the urgency and impact.
7. All IT incident should be tracked and resolved as per agreed service level.
8. Member organizations relevant teams should be involved (when applicable) to ensure adequate handling of the incident.
9. The Member Organizations should inform 'General Department of Cyber Risk Control' immediately upon identification of 'Medium' or above classified incident that have impact on customers, as per SAMA BCM Framework.
10. The Member Organizations should inform 'General Department of Cyber Risk Control' immediately upon identification of disruption and slowness in the critical and/or application(s) impacting customer.
11. Member Organizations should notify 'General Department of Cyber Risk Control' before disclosing any information about the incident to the media.
12. The Member Organizations should submit a detail incident report within five (5) days to 'General Department of Cyber Risk Control', including the following details as a minimum:
    a. title of the incident;
    b. identification, classification and prioritization of incident;
    c. logging and monitoring of incident;
    d. resolution and closure of incident;

e. impact assessment such as financial, data, customer and/or reputational;
f. date and time of the incident;
g. name of the impacted services and systems;
h. root-cause analysis; and
i. corrective actions with target dates.

3.3.9 Problem Management

Principle

Criteria and procedures to report problems should be defined to limit recurring incidents and to minimize the impact of incidents on the Member Organizations.

Control Requirements

1. The problem management process should be defined, approved, implemented and communicated.
2. The effectiveness of the problem management process should be measured and periodically evaluated.
3. The problem management process should include the following requirements but not limited to:
   a. identification, classification and prioritization of problem;
   b. logging and monitoring of problem;
   c. resolution and closure of problem;
   d. the protection of relevant evidence and loggings;
   e. impact assessment such as financial, data, customer and/or reputational;
   f. date and time of the problem;
   g. name of the impacted services and systems;
   h. root-cause analysis; and
   i. corrective actions.
4. The Member Organizations should maintain a database for known error records.

3.3.10 Data Backup and Recoverability

Principle

Data backup management strategy along with backup and restoration procedures should be defined, approved and implemented to ensure reliability, availability, and recoverability of data of the Member Organizations.

Control Requirements

1. Data backup management strategy should be defined, approved and implemented.
2. The data backup management policy should consider the following, but not limited to:
   a. alignment with SAMA Business Continuity Management Framework;
   b. implementation of replication, backup and recovery capabilities;
   c. data storage;
   d. data retrieval; and
   e. data retention as per the legal, regulatory and business requirements.
3. Backup and restoration procedures should be defined, approved and implemented.
4. The effectiveness of the backup and restoration procedure should be measured and periodically evaluated.
5. Member Organizations should define its backup and restoration requirements considering the following, but not limited to:
   a. legal and regulatory requirements;
   b. business requirements in line with agreed RPO (Recover Point Objective);
   c. type of backups (offline, online, full, incremental, etc.); and
   d. schedule of the backup (daily, weekly, monthly, etc.).
6. Member Organizations should ensure the following information are backed up at minimum:
   a. applications;
   b. operating systems software;

c. databases; and
d. device configurations.

7. In case of replication of data between primary and disaster recovery site, Member Organizations should ensure that all replication issues are timely resolved such that data at the disaster recovery site are in sync with the primary site as per the agreed recovery point objective (RPO) and recovery time objective (RTO).
8. Member Organizations should ensure that RTOs for critical services such as payment systems, customer related services, etc. are adequately defined considering the high availability of the supporting operations and minimum disruption in the event of disaster.
9. Member Organization should ensure sufficient investment are made from people, process and technology perspective to achieve the targeted RTOs.
10. Member Organizations should implement alternate mechanism for backup redundancy (e.g. transaction dumps in addition to full database backup).
11. Member Organizations should conduct periodic testing and validation of the recovery capability of backup media.
12. Backup media should be appropriately labelled.
13. Backup media including USB disks, containing sensitive or confidential information should be encrypted before transportation to offsite for storage.

3.3.11 Virtualization

Principle

Formal process for creation, distribution, storage, use and retirement of virtualized images, snapshots or containerization should be defined and managed in a controlled and secured manner.

Control Requirements

1. A process should be defined, approved, implemented and communicated by the Member Organizations to setup, deploy and configure a virtual environment.
2. The process should be governed with well-defined policies, procedures and standards.
3. The effectiveness of the virtualization or containerization process should be measured and periodically evaluated.
4. All virtual components deployed in the Member Organizations should be provided with the same level of security as of non-virtualized environment.
5. All virtual components should be adequately configured using defined and approved minimum baseline security standards (MBSS) specific to virtualization or containerization.
6. Strong authentication mechanism should be implemented and access should be granted on need to know or least privileged basis for all virtual environments including host operating system, hypervisor, guest operating systems and any other related components.
7. The creation, distribution, storage, use, retirement and destruction of the virtual images and snapshots should be handle in a controlled and secured manner.
8. The following should be considered as part of virtualization/containerization but not limited to:
   a. administrative access should be tightly controlled where access via local admin should be restricted;
   b. management of hypervisors should be restricted to administrators only;
   c. virtual test environment should be physically and/or logically segregated from the production environment and even should not operate on the same host;
   d. unnecessary program and services should be disabled on virtual machines unless authorized by the business;
   e. audit logging should be enabled and monitored for all virtual machines that should include but not limited to:
      1. creation, deployment and removal;
      2. root and administrative activities; and

3. creation, modification and deletion of system level objects.

f. appropriate controls should be in place to protect sensitive and critical data being used and managed through virtual images or snapshots; and
g. all virtual drives used by the guest operating systems should be backed-up and tested on regular basis, using the same policy for backup management as is used for non-virtualized systems.

3.4 System Change Management

System change management is a process of defining, designing, testing and implementing changes related to information assets including but not limited to application, software, device and data. Thus, risks factors related to system change management should be addressed by the Member Organizations through adequate implementation of required IT controls.

3.4.1 System Change Governance

Principle

A Change Management process should be established to ensure that changes to the Member Organization's information assets are classified, tested and approved before their deployment into production environments

Control Requirements

1. System change management process should be defined, approved, implemented and communicated within the Member Organizations.
2. The effectiveness of the system change management process should be measured and periodically evaluated.
3. System change management process should be governed by the change management policy and procedure that should be approved, monitored, reviewed and updated on periodic basis and/or whenever significant changes occurs in the IT environment or changes in laws and regulatory requirements.
4. System change management process should address the following, but not limited to:
   a. change requirement definition and approval;
   b. change severity and priority;
   c. change risk and impact assessment;
   d. change development;
   e. change testing;
   f. change roll-out and roll-back;
   g. change roles and responsibilities;
   h. change documentation;
   i. change awareness and/or training for users; and
   j. change advisory board (CAB) input, if applicable.
5. A workflow system should be implemented to automate the change management process by the Member Organizations to the maximum extent possible.
6. Any changes in the information assets should be logged, monitored and documented.
7. System environments (i.e. development, testing, production, etc.) should be technically and logically segregated.
8. Access to different system environments should be strictly controlled and monitored. In order to do so, segregation of duties ('SoD') should be ensured so that no individual have two conflicting responsibilities such as (develop, compile, test, migrate and deploy) at the same time.
9. Emergency changes in the information assets should be performed in a strictly controlled manner and should consider the following:
   a. the number of emergency changes should be least preferred over planned changes in order to keep such changes as minimum as possible;
   b. emergency changes should be assessed for their impact on the systems;
   c. emergency changes should be approved by the Emergency Change Advisory Board ('ECAB');

d. minimum level of testing should be acceptable to implement the emergency changes;
e. formal documentation of emergency changes should be completed post implementation;
f. post implementation review should be conducted for all emergency changes; and
g. root cause analysis should be conducted to determine the cause due to which emergency change was required, as well as maintaining a register to reflect lesson learned and report to all concerned staff, management and ITSC.

10. Sufficient auditing should be enabled to log emergency changes related to information assets for future reference or investigation purposes.

3.4.2 Change Requirement Definition and Approval

Principle

Changes to information assets should be formally defined, documented and approved by relevant asset owner prior to implementing the change in the information assets.

Control Requirements

1. Change requirements should be formally initiated by the requestor of the change.
2. Change requirements should specify both functional and non-functional requirements, where applicable.
3. Change requirements should be formally reviewed and approved by the concern asset owner.
4. Any changes in the information assets should be assessed for their impact on the systems prior to implement the change.
5. Any change in the information assets should be endorsed by the Change Advisory Board ('CAB') prior deploying to the production environment.
6. Any changes in the information assets should be reviewed and approved by the cyber security function before submitting to 'CAB' *(required as per the SAMA Cyber Security Framework, 3.3.7 Change Management, Control Requirements, 4 – d).*

3.4.3 System Acquisition

Principle

System acquisition process should be established to ensure risks associated with the system acquisition and related vendor service level are adequately assessed and mitigated prior acquiring system.

Control Requirements

1. System acquisition process should be defined, approved, implemented and communicated by the Member Organizations.
2. The effectiveness of the system acquisition process should be measured and periodically evaluated.
3. System requirements (i.e. functional and non-functional) should be formally defined and approved as part of system acquisition.
4. A feasibility study should be conducted to assess functional and non-functional requirements of the new system particularly in conformance with the SAMA regulatory requirements, and other applicable regulatory requirements.
5. Vendor evaluation should be incorporated in the system acquisition process to assess vendor for their offering and capabilities to support system during and post implementation.
6. The system acquisition should be supported with a detail implementation plan describing the following, but not limited to:
   a. system implementation milestones (including requirement gathering, development or customization, testing, go-live etc.);
   b. timeline for each milestone and their dependencies; and
   c. resources assigned to milestones.
7. The off-the-shelf system or package should be evaluated based on the following, but not limited to:
   a. system conformance with the requirements of the Member Organization;

b. system creditability and market presence, if required; and
c. vendor evaluation and service level.

3.4.4 System Development

Principle

System development methodology should be documented, approved and implemented to ensure that the development of Member Organization's system is performed in a strictly controlled manner.

Control Requirements

1. The system development methodology should be defined, approved, implemented and communicated.
2. The effectiveness of the system development methodology should be monitored and periodically evaluated.
3. The system development methodology should address the following, but not limited to:
   a. system development approach such as agile, waterfall, etc.;
   b. secure coding standards;
   c. testing types and approaches such as unit testing, regression testing, stress testing, etc.;
   d. version controlling;
   e. quality control;
   f. data migration;
   g. documentation; and
   h. end user training.
4. The system design document should be defined, documented and approved.
5. The system design document should address the low level design requirements for the intended system, which includes but not limited to following:
   a. configurations requirements;
   b. integration requirements;
   c. performance requirements;
   d. cyber security requirements; and
   e. data definition requirements.
6. Member organizations relevant IT function or development team should conduct secure code review for:
   a. applications developed internally; and
   b. externally developed applications if the source code is available.
7. Member Organizations should ensure that the secure code review report (or equivalent, such as an independent assurance statement) is formulated in case the source code is not available with the member organization.
8. Cyber security controls should be embedded in the system development process in line with SAMA Cyber Security Framework.
9. Version control system should be utilized to keep track of source code or build versions between various system environments (i.e. development, test, production, etc.).

3.4.5 Testing

Principle

All changes to information systems should be comprehensively tested on the test environment based on the defined and approved test cases to ensure that changes meets the business requirements as well as to identify defects or vulnerabilities before releasing changes to the production environment.

Control Requirements

1. Test plan should be formally defined, approved and documented for the changes.
2. Test case should be defined, approved and documented for the changes. In addition, test case should address the following, but not limited to:

a. test case name and unique ID;
b. test case designed by and tested by;
c. test case description with clear identification of negative and positive test cases;
d. test priority;
e. date of the test execution;
f. data use to test the cases;
g. status of the test case (i.e. pass or fail);
h. expected outcome of the test case; and
i. third party testing certification requirement, if applicable. i.e. MADA, Tanfeeth, etc.

3. At a minimum, the following types of testing should be considered as part of system change management.
   a. unit testing;
   b. system integration testing (SIT);
   c. stress testing (if applicable);
   d. security testing; and
   e. user acceptance testing (UAT).
4. All changes to information system should be thoroughly tested on a separate test environment in accordance with the approved test cases.
5. All changes should be formally tested and accepted by the concern business users.
6. Testing should include positive and negative test cases scenarios.
7. The results of UAT should be documented and maintained for future reference purposes.
8. The production data should not be utilized for system testing in the test environment. Only sanitized data should be used for testing purposes.

3.4.6 Change Security Requirements

Principle

Cyber security requirements should be defined and thoroughly tested for all changes in the information system in a testing environment in order to identify and mitigate security vulnerabilities therein prior introducing them into the production environment.

Control Requirements

1. System change management process should consider SAMA Cyber Security Framework for defining, testing and implementing security requirements for any changes in the information assets.

3.4.7 Change Release Management

Principle

Change release management process should be defined to ensure that system changes are adequately planned and released to the production environment in a strictly controlled manner.

Control Requirements

1. The release management process should be defined, approved, implemented and communicated.
2. The release management process should be monitored and periodically evaluated.
3. The release management process should address the following, but not limited to:
   a. change release strategy and approach;
   b. roles and responsibilities to carry out change releases;
   c. change release schedule and logistics;
   d. change roll-out and roll-back procedures; and
   e. data migration, where applicable.
4. The changes should be released in the corresponding system in disaster recovery site upon successful implementation of changes in the production environment at main site.

5. Change should be introduced as part of an agreed change window, exceptions has to have their own approval process and seldom allowed without compelling reasons.

3.4.8 System Configuration Management

Principle

System Configuration Management Process should be defined, approved, communicated and implemented to maintain a reliable and accurate information about configuration items ('CIs') for Member Organization's information assets.

Control Requirements

1. The configuration management process should be defined, approved, implemented and communicated by the Member Organizations.
2. The configuration management process should be monitored and periodically evaluated.
3. The configuration management process should address the following, but not limited to:
   a. roles and responsibilities for carrying out configuration management;
   b. identification and recording of configuration items and their criticality with respect to its supporting business processes;
   c. interrelationships between configuration items among various information assets; and
   d. periodic verification of configuration items.
4. Member Organizations should implement configuration management database ('CMDB') to identify, maintain, and verify information related to Member Organization's Information assets.

3.4.9 Patch Management

Principle

Patch management process should be defined and implemented to ensure up-to-date with latest applicable and relevant patches (i.e. functional or non-functional) are installed in a timely manner to avoid technical issues including security breaches due to existing vulnerabilities in the system.

Control Requirements

1. The patch management process should be defined, approved, implemented and communicated by the Member Organizations.
2. The effectiveness of the patch management process should be monitored, measured and periodically evaluated.
3. All patches should be thoroughly assessed for impact by relevant stakeholders including cyber security before being implemented into the production environment.
4. All systems should be periodically scanned or inspected to identify any outdated patches and vulnerabilities in the systems.
5. Deployment of patches should follow a formal change management process.
6. All patches should be thoroughly tested in a separate test environment prior introducing to the production environment to avoid any compatibility issue with the system and related components.
7. Patches should be rolled out to systems and related components systematically.
8. Following deployment of patches to the production environment, systems should be monitored for any abnormal behavior and, if such behavior identified should be thoroughly investigated to identify the root cause and fix them properly.
9. Patch deployment window (i.e. schedule) should be communicated to business and relevant stakeholders in advance and preferable should be done during non-peak hours and non-freezing periods to avoid any business disruption.
10. The external feeds from software vendors or other acknowledged sources should be monitored to identify any new vulnerabilities in the system and to be patched accordingly.

3.4.10 IT Project Management

Principle

Formal process should be defined, approved and implemented to effectively manage IT project and related risks throughout the lifecycle of the project.

Control Requirements

1. The IT project management process should be defined and approved by the Member Organizations.
2. The IT project management process should be governed with a formally defined and approved IT project management framework, policy and procedure to manage IT project lifecycle from initiation till closure.
3. The effectiveness of the IT project management process should be monitored, measured and periodically evaluated.
4. All IT projects should be provided with detail project plan, which include the following, but not limited to:
    a. detail scope of work including activities for a project or each phase of the project;
    b. priorities, milestones and timelines associated with project or each phase of the project;
    c. deliverables;
    d. roles and responsibilities; and
    e. risks associated with any IT projects.
5. Necessary documentations for the IT project should be defined, approved and maintained for future reference purposes including but not limited to following:
    a. project charter;
    b. requirement analysis, business information flow and technical information flow;
    c. feasibility as well as cost-benefit analysis; and
    d. detail project plan.
6. IT project steering committee should be established having representation from relevant business and technical teams to oversee plan, progress and risks associated with the IT projects.
7. All IT projects should be assessed for the risks that could impact the scope, timeline and quality of the projects. Any identified risks should be mitigated and monitored throughout the project lifecycle.
8. Any significant risks associated with the IT project should be reported to IT project steering committee and to senior management or board of directors of the member organization in a timely manner.
9. All project deliverables should be reviewed by an independent quality assurance function or an independent person provided with such responsibly prior commencing project to the production environment.
10. Post-implementation reviews should be planned and executed to determine whether IT projects delivered the expected benefits, met business/user requirements, and complied with the IT project management framework.
11. The Member Organizations should inform ‘General Department of Cyber Risk Control’ for any major IT transformation projects, such as core system implementation, after the approval from the senior management.
12. Cyber security should be involved during various phases of the IT project management lifecycle in line to the control considerations provided in the SAMA Cyber Security Framework.

3.4.11 Quality Assurance

Principle

The quality assurance process should be defined, approved, communicated and implemented to independently ascertain quality of the changes or development in the information assets in line with the business/user requirements prior moving them to the production environment.

Control Requirements

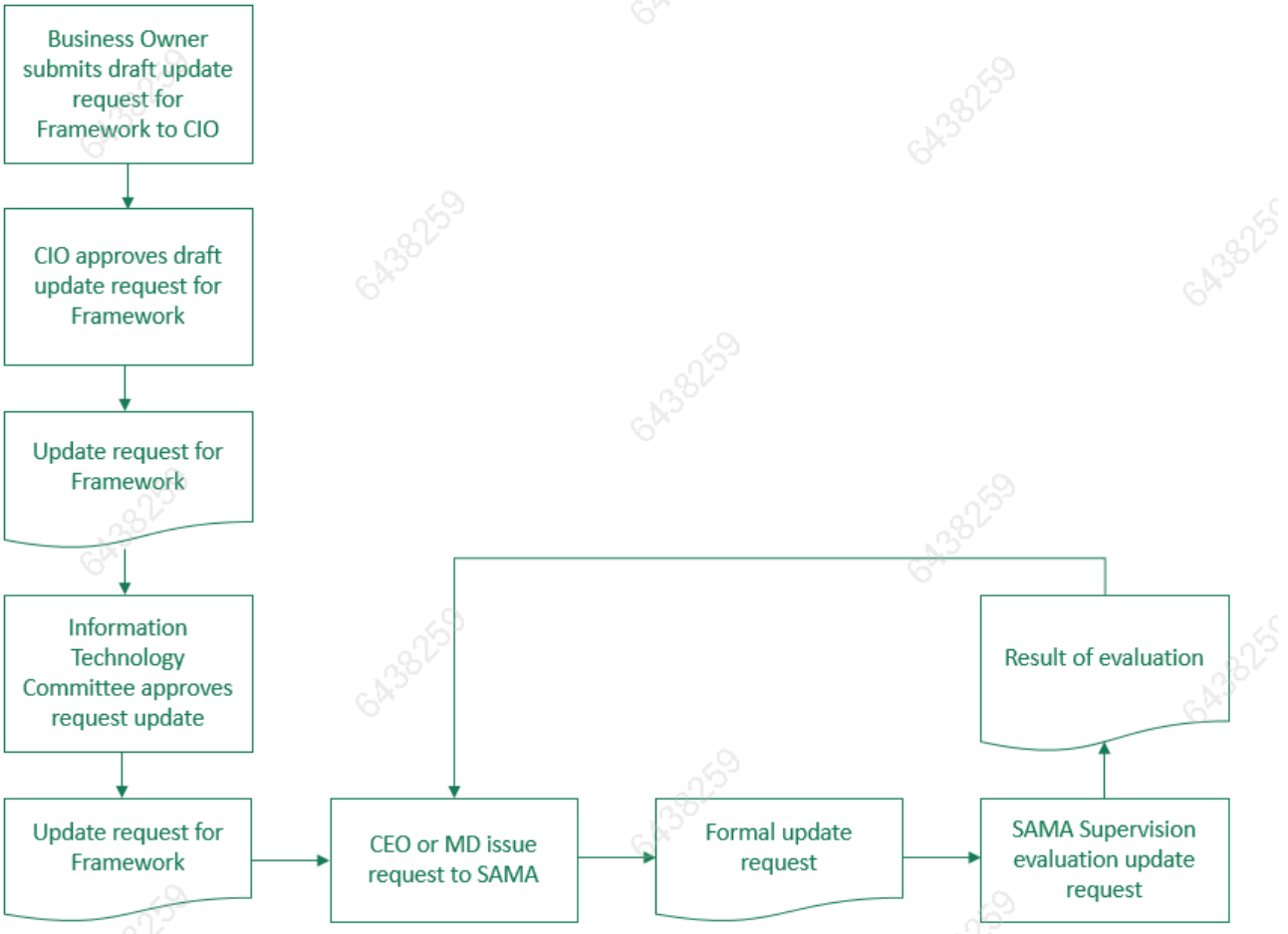
1. The quality assurance process should be defined, approved, implemented and communicated by the Member Organizations.
2. The quality assurance process should be monitored and periodically evaluated.
3. The quality assurance process should address the following, but not limited to:
   a. clear roles and responsibilities for personnel carrying out quality assurance activities;
   b. minimum quality requirements sets by the Member Organizations including business and any other applicable regulatory requirements; and
   c. process for identification, maintenance and retirement of quality related records.
4. The quality assurance function/department should have independent existence and reporting with authority to provide objective evaluation.
5. All changes or development to information system should be assessed by the quality assurance team prior releasing to the production environment.
6. The quality assurance function should report the reviewed results to the relevant stakeholder(s) within the Member Organizations and initiate improvements where appropriate.

Appendices

Appendix A - How to request an Update to the Framework

Below the illustration of the process for requesting an update to the Framework.

- Detail information supported by pros and cons about the suggested update.
- The request should first be approved by CIO before submitting to IT steering committee.
- The request should be approved by Member Organization's IT steering committee.
- The request should be sent formally in writing to the manager 'General Department of Cyber Risk Control' via the Member Organization's CEO or managing director.
- 'General Department of Cyber Risk Control' will evaluate the request and informs the Member Organization.
- The current Framework remains applicable while the requested update is being considered, processed and if applicable is approved and processed.



Appendix B – Framework Update request form

Request to Update the IT Governance Framework

A submission to the manager of SAMA General Department of Cyber Risk Control.

The Saudi Central Bank (SAMA) will consider requests from a member organization (MO) to update its IT Governance Framework based on the information submitted using the form below. A separate form must be completed for each requested update. Please note that all required fields must be properly filled in before SAMA will begin the review process

Requestor Information

REQUESTOR'S SIGNATURE* x	REQUESTOR'S POSITION*	DATE*
REQUESTOR'S NAME*	MEMBER ORGANIZATION OF REQUESTOR*	

FRAMEWORK SECTION*:
PURPOSE OF REQUESTED UPDATE (including detailed information on its pros and cons)*:
PROPOSAL*:

Approvals

1. MO's CIO APPROVAL*	DATE*	
2. MO'S IT STEERING COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*
3. SAMA DECISION	SAMA APPROVAL	DATE

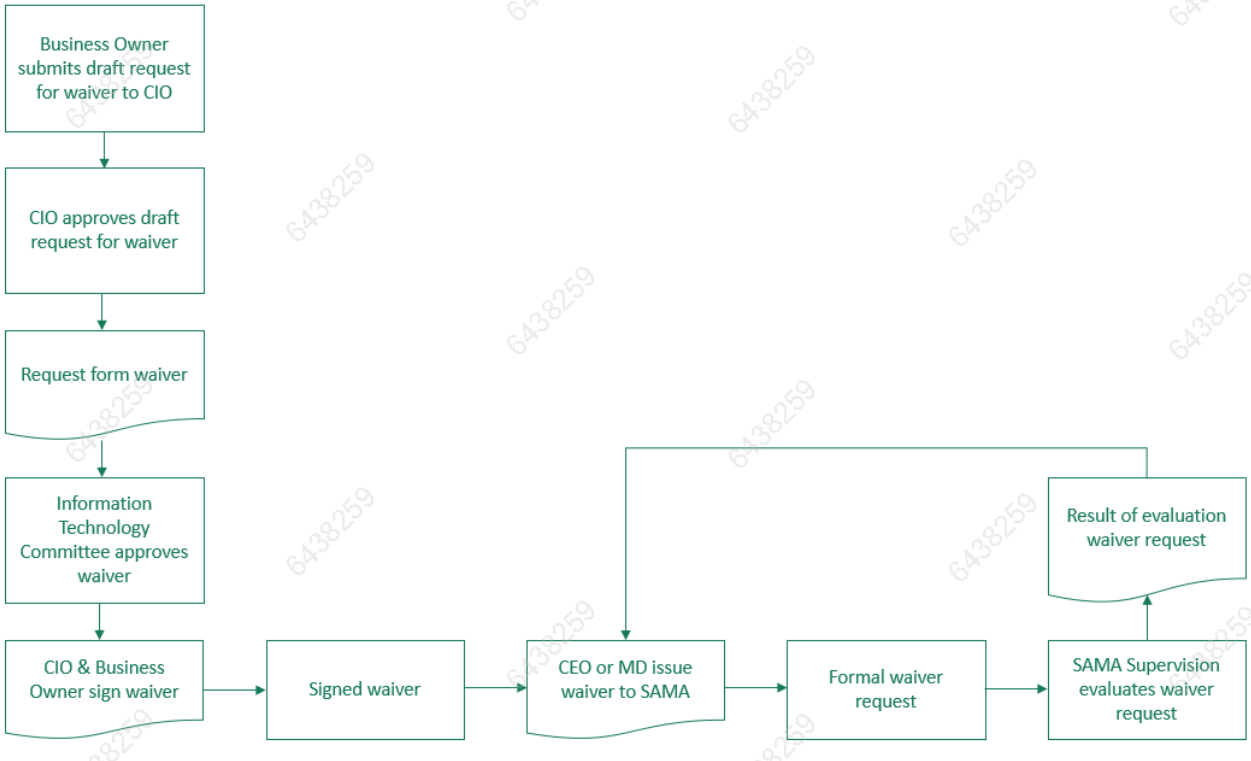
* Denotes required fields

Appendix C - How to request a Waiver from the Framework

Below the illustration of the process for requesting a waiver from the Framework.

- Detail description about the reasons that the member organization could not meet the required control.
- Details description about the available or suggested compensating controls.
- The waiver request should first be approved by CIO before submitting to IT steering committee.
- The waiver request should approved by the members of Member Organization's IT steering committee.
- The waiver request should be signed by the CIO and relevant (business) owner.
- The waiver request should be formally issued in writing to the manager of 'General Department of Cyber Risk Control' via the Member Organization's CEO or managing director.
- 'General Department of Cyber Risk Control' will evaluate the waiver request and informs the Member Organization.

The current Framework remains applicable while the requested waiver is being evaluated and processed, until the moment of granting the waiver.



Appendix D – Framework Waiver request form

Request for Waiver from the SAMA IT Governance Framework

A submission to the manager of 'General Department of Cyber Risk Control'

The Saudi Central Bank (SAMA) will consider requests for waiver from a member organization (MO) from its IT Governance Framework based on the information submitted using the form below. A separate form must be completed for each requested waiver. Please note that all required fields must be properly filled in before SAMA will begin the review process.

Requestor Information

REQUESTOR'S SIGNATURE* X	REQUESTOR'S POSITION*	DATE*
REQUESTOR'S NAME*	MEMBER ORGANIZATION OF REQUESTOR*	

FRAMEWORK CONTROL*:
DETAILED DESCRIPTION OF WHY CONTROL CANNOT BE IMPLEMENTED*:
DETAILED DESCRIPTION OF AVAILABLE OR SUGGESTED COMPENSATING CONTROLS*:

Approvals

1. MO's CIO APPROVAL*	DATE*	
2. MO'S IT STEERING COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*
3. SAMA DECISION	SAMA APPROVAL	DATE

* Denotes required fields

** The validity of this waiver is one year. It is the Member Organizations responsibility to ensure renewal of this waiver.

Appendix E – Glossary

Term	Description
Access Control	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Application Architects	Application Architects identify needed changes to the portfolio of applications across the ecosystem. They develop and administer application-specific standards such as user interface design, globalization, Web services, portal application programming interfaces, XML, and content. They provide design recommendations based on long-term development organization strategy and develop enterprise level application and custom integration solutions including major enhancements and interfaces, functions and features.
Asset Management	The systematic process of deploying, operating, maintaining, upgrading, and disposing of assets in a safe, secure and cost effective manner
Asset Owner	The term Asset owner identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use of the information assets.
Authorization Matrix	A matrix that defines the rights and permissions for a specific role needs for information. The matrix lists each user, the business process tasks he or she performs, and the affected systems.
Audit	Independent review and examination of records and activities to assess the effectiveness of IT governance controls and to ensure compliance with established policies, operational procedures and relevant standard, legal and regulatory requirements.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite in order to allow access to resources in a system.
Backup	Files, devices, data and procedures available for use in case of a failure or loss, or in case of deletion or suspension of their original copies.
Business Application	Any software or set of computer programs that are used by business users to perform various business functions.
Batch Processing	Batch processing is the processing of the transactions in a group or batch with no or minimal human interaction.
Configuration Item (CI)	Component of an infrastructure-or an item, such as a request for change, associated with an infrastructure-which is (or is to be) under the control of configuration management
Change Management	The controlled identification and implementation of required changes within a business or information systems.
Chief Information Officer (CIO)	A senior-level executive referred as *Chief Information Officer (CIO),* Chief Technology Officer (CTO) / Head of IT or relevant stakeholder who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources.
Classification	Setting the sensitivity level2 of data and information that results in security controls for each level of classification. Data and information sensitivity levels are set according to predefined categories where data and information is created, modified, improved, stored or transmitted. The classification level is an indication of the value or importance of the data and information of the organization.

Term	Description
Chief Operating Officer (COO)	A senior-level executive responsible for the daily operation of the organization.
Critical IT infrastructures	These are the information assets (i.e., facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property, alongside observance of significant economic and/or social impacts.
Compensating Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in place of a recommended control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
Containerization	Unit of software that packages up code and all its dependencies.
Data Masking	A computerized technique of blocking out the display of sensitive information or PII.
Database Administrator	Database administrator, frequently known just by the acronym DBA, is a role usually within the Information Technology department, charged with the creation, maintenance, backups, querying, tuning, user rights assignment and security of an organization's database.
Disaster Recovery	Programs, activities and plans designed to restore the organizations critical business functions and services to an acceptable situation, following exposure to cyber and IT incidents or disruption of such services.
Enterprise Architect	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the enterprise’s objectives.
Feasibility study	A phase of a system development life cycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need.
Formally documented	Documentation that is written, approved by the senior leadership and disseminated to relevant parties.
Freezing period	e.g. Salaries deposit days, public or national holidays.
Hypervisor	A hypervisor allows one host computer to support multiple guest Virtual Machines (VMs) by virtually sharing its resources, like memory and processing.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Management	The monitoring and detection of events on an information systems and the execution of proper responses to those events.
Information Asset	A piece of information, stored in any manner, which is recognized as 'valuable' to the organization.
Interdependencies	Set of interaction with dependence of information assets on each another in order to deliver set of works or tasks.

Term	Description
IT Change and Release Management	A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change
IT facilities	The physical environment where the IT infrastructure is located.
IT risk	The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
IT Steering committee	An executive-management-level committee that assists in the delivery of the IT strategy oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects.
Key Performance Indicator (KPI)	KPI is a type of performance measurement that evaluates the success of an organization or of a particular activity in which it engages to achieve particular objectives and goals.
Key Risk Indicator (KRI)	KRI is a measure used to indicate the probability an activity or organization will exceed its defined risk appetite. KRIs are used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.
Likelihood	A weighted factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability.
Member Organization	Organizations affiliated with SAMA.
Need-to-know	The restriction of data, which is considered sensitive unless one has a specific need to know; for official business duties.
Off-the-shelf system	Software that already exists and is available from commercial sources.
Outsourcing	Obtaining goods or services by contracting with a supplier or service provider.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen or lost.
Recovery Point Objective (RPO)	The point in time to which data must be recovered after an outage. RPO is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
Recovery Time Objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Regression Testing	Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made.
Residual risks	The remaining risk after management has implemented a risk response.
Retention	The length of time that information, data, event logs or backups must be retained, regardless of the form (i.e., paper and electronic).
Risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Term	Description
Risk register	Risk register is a table used as a repository for all risks identified and includes additional information about each risk, e.g. risk category, risk owner, and mitigation actions taken.
Risk Tolerance	The acceptable variation relative to performance to the achievement of objectives. Also refer to 'Risk appetite'.
Risk Treatment	A process to modify risk that can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the risk source; changing the likelihood; changing the consequences; sharing the risk with another party or parties; and retaining the risk by informed decision. Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Risk treatments can create new risks or modify existing risks.
Root-cause analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
RACI Chart	Illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework.
Security Testing	A process intended to ensure that modified or new systems and applications include appropriate security controls and protection and do not introduce any security holes or vulnerabilities that might compromise other systems or applications or misuses of the system, application or its information, and to maintain functionality as intended.
Security-by Design	A methodology to systems and software development and networks design that seeks to make systems, software and networks free from cybersecurity vulnerabilities/weaknesses and impervious to cyber-attack as much as possible through measures such as: continuous testing, authentication safeguards and adherence to best programming and design practices.
Segregation of Duties	Key principle that aims at minimizing errors and fraud when processing specific tasks. It is accomplished through having several people with different privileges, required to complete a task.
Service level agreement (SLA)	Defines the specific responsibilities of the service provider and sets the customer expectations.
Stress Testing	A type of performance testing conducted to evaluate a system or component at or beyond the limits of its anticipated or specified workloads, or with reduced availability of resources such as access to memory or servers.
System Acquisition	Procedures established to purchase application software, or an upgrade, including evaluation of the supplier's financial stability, track record, resources and references from existing customers
System Configuration Management	The control of changes to a set of configuration items over a system life cycle.
Third-Party	Any organization acting as a party in a contractual relationship to provide goods or services (this includes suppliers and service providers).
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or

Term	Description
	reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Unit Testing	A testing technique that is used to test program logic within a particular program or module.
User Acceptance Testing (UAT)	Taking use cases or procedures for how the system was designed to perform and ensuring that someone who follows the procedure gets the intended result.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Owner	Individual or group that holds or possesses the rights of and the responsibilities for an enterprise, entity or asset.