Cyber Security Framework
Saudi Arabian Monetary Authority

Version 1.0

May 2017

مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Authority

Foreword

In view of the ever-growing seriousness of cyber-attacks, we are conscious of the need to stay one-step ahead. The issuance of a Cyber Security Framework ("Framework") seeks to support our regulated entities in their efforts to have an appropriate cyber security governance and to build a robust infrastructure along with the necessary detective and preventive controls. The Framework articulates appropriate controls and provide guidance on how to assess maturity level.

The adoption and implementation of the Framework is a vital step for ensuring that Saudi Arabian Banking, Insurance and Financing Companies sectors can manage and withstand cyber security threats. In designing the Framework, we have considered the ways that our regulated entities are leveraging technology and felt that each entity will be able to adopt a common approach for addressing cyber security. This will ensure cyber security risks are properly managed throughout the sectors

To achieve the above, the full support and oversight from the Board of Directors and Senior Management are required for its implementation.

The Information Technology Risk team within the Deputyship of Supervision is at your disposal for any clarifications and we remain committed to guiding our regulated entities in creating a safer cyber environment.

Ahmed Al Sheikh
Deputy Governor for Supervision

Contents

1 Introduction

1.1 Introduction to the Framework

The current digital society has high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data. Information assets and online services are now strategically important to all public and private organizations, as well as to broader society. These services are vital to the creation of a vibrant digital economy. They are also becoming systemically important to the economy and to broader national security. All of which underlines the need to safeguard sensitive data and transactions, and thereby ensure confidence in the overall Saudi Financial Sector.

The stakes are high when it comes to the confidentiality, integrity and availability of information assets, and applying new online services and new developments (e.g. Fintech, block chain); while improving resilience against cyber threats. Not only is the dependency on these services growing, but the threat landscape is rapidly changing. The Financial Sector recognizes the rate at which the cyber threats and risks are evolving, as well as the changing technology and business landscape.

SAMA established a Cyber Security Framework ("the Framework") to enable Financial Institutions regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

The objective of the Framework is as follows:

1. To create a common approach for addressing cyber security within the Member Organizations.
2. To achieve an appropriate maturity level of cyber security controls within the Member Organizations.
3. To ensure cyber security 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 cyber security controls at Member Organizations, and to compare these with other Member Organizations.

The Framework is based on the SAMA requirements and industry cyber security standards, such as NIST, ISF, ISO, BASEL and PCI.

The Framework supersedes all previous issued SAMA circulars with regard to cyber security. Please refer to 'Appendix A – Overview previous issued SAMA circulars' for more details.

1.2 Definition of Cyber Security

Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.

The general security objectives comprise the following:

- *Confidentiality* – Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data).
- *Integrity* – Information assets are accurate, complete and processed correctly (i.e., protected from unauthorized modification, *which may include authenticity and non-repudiation*).
- *Availability* – Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).

1.3 Scope

The Framework defines principles and objectives for initiating, implementing, maintaining, monitoring and improving cyber security controls in Member Organizations.

The Framework provides cyber security controls which are applicable to the information assets of the Member Organization, including:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment and communication networks (technical infrastructure).

The Framework provides direction for cyber security requirements for Member Organizations and its subsidiaries, staff, third parties and customers.

For business continuity related requirements please refer to the SAMA Business Continuity Minimum Requirements.

The Framework has an interrelationship with other corporate policies for related areas, such as physical security and fraud management. This framework does not address the non-cyber security requirements for those areas.

1.4 Applicability

The Framework is applicable to all Member Organizations regulated by SAMA, which include the following:

- All Banks operating in Saudi Arabia;
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia;
- All Financing Companies operating in Saudi Arabia;
- All Credit Bureaus operating In Saudi Arabia;
- The Financial Market Infrastructure

All domains are applicable for the banking sector. However, for other financial institutions the following exceptions apply:

- Sub-domain (3.1.2) the alignment with cyber security strategy of banking sector is mandatory when applicable.
- Exclude sub-domain (3.2.3). However, if the organization store, process or transmit cardholder data or deal with SWIFT services, then PCI standard and/or SWIFT Customer Security Controls Framework should be implemented.
- Exclude sub-domain (3.3.12).
- Exclude sub-domain (3.3.13). However, if the organization provides online services for customers, a Multi Factor Authentication capability should be implemented.

1.5 Responsibilities

The framework is mandated by SAMA. SAMA is the owner and is responsible for periodically updating the Framework.

The Member Organizations are responsible for adopting and implementing the Framework.

1.6 Interpretation

SAMA, as the owner of the Framework, is solely responsible for providing interpretations of the principles, objectives and control considerations, if required.

1.7 Target Audience

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

1.8 Review, Updates and Maintenance

The Framework will be reviewed and maintained by SAMA.

SAMA will review the Framework periodically to determine the Framework's effectiveness, including the effectiveness of the Framework to address emerging cyber security 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 approved, the Framework will be adjusted.

The Member Organization will remain responsible to be compliant with the Framework pending the requested update.

Please refer to 'Appendix B – 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 cyber security domains and subdomains, principles, objectives and control considerations.

2 Framework Structure and Features

2.1 Structure

The Framework is structured around four main domains, namely:

- Cyber Security Leadership and Governance.
- Cyber Security Risk Management and Compliance.
- Cyber Security Operations and Technology.
- Third Party Cyber Security.

For each domain, several subdomains are defined. A subdomain focusses on a specific cyber security topic. Per subdomain, the Framework states a principle, objective and control considerations.

- A **principle** summarizes the main set of required cyber security controls related to the subdomain.
- The **objective** describes the purpose of the principle and what the set of required cyber security controls are expected to achieve.
- The **control considerations** reflects the mandated cyber security controls that should be considered.

Control considerations have been uniquely numbered throughout the Framework. Where applicable, a control consideration can consist of up to 4 levels.

The control considerations are numbered according to the following numbering system:

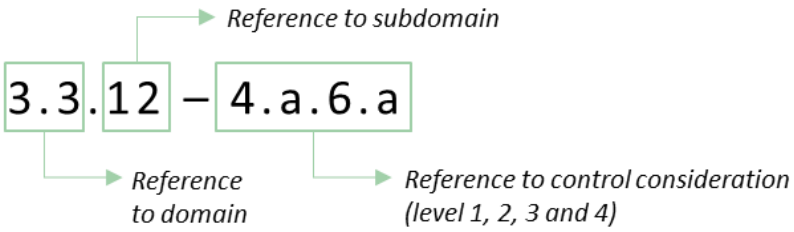


Figure 1 – Control consideration numbering system

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

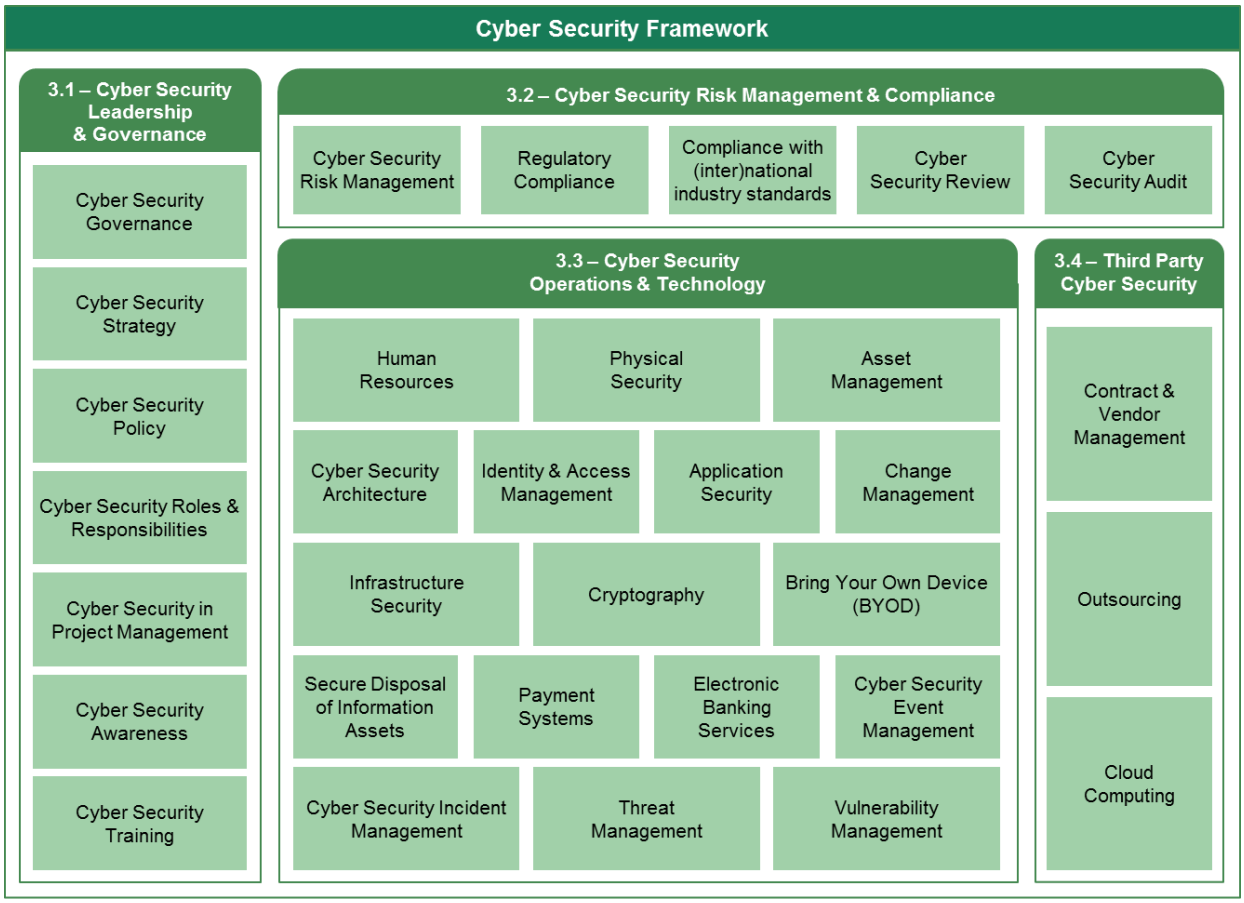


Figure 2 - Cyber Security Framework

2.2 Principle-based

The Framework is principle based, also referred to as risk based. This means that it prescribes key cyber security principles and objectives to be embedded and achieved by the Member Organization. The list of mandated control considerations provides additional direction and should be considered by the Member Organization in achieving the objectives. When a certain control consideration cannot be tailored or implemented, the Member Organization 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 Organization will be subject to a periodic self-assessment. The self-assessment will be performed by the Member Organization 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 cyber security maturity level of the Member Organization.

Please refer to '2.4 Cyber Security Maturity Model' for more details about the cyber security maturity model.

2.4 Cyber Security Maturity Model

The cyber security maturity level will be measured with the help of a predefined cyber security maturity model. The cyber security 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, a Member Organization must 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 cyber security control.	• Cyber security controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such cyber security controls.
1 Ad-hoc	• Cyber security controls is not or partially defined. • Cyber security controls are performed in an inconsistent way. • Cyber security controls are not fully defined.	• Cyber security control design and execution varies by department or owner. • Cyber security control design may only partially mitigate the identified risk and execution may be inconsistent.
2 Repeatable but informal	• The execution of the cyber security control is • based on an informal and unwritten, though standardized, practice.	• Repeatable cyber security 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	• Cyber security controls are defined, approved and implemented in a structured and formalized way. • The implementation of cyber security controls can be demonstrated.	• Cyber security policies, standards and procedures are established. • Compliance with cyber security 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 cyber security controls are periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of cyber security controls are measured and periodically evaluated. • key risk indicators and trend reporting are used to determine the effectiveness of the cyber security controls. • Results of measurement and evaluation are used to identify opportunities for improvement of the cyber security controls.
5 Adaptive	• Cyber security controls are subject to a continuous improvement plan.	• The enterprise-wide cyber security program focuses on continuous compliance, effectiveness and improvement of the cyber security controls. • Cyber security controls are integrated with enterprise risk management framework and practices. • Performance of cyber security controls are evaluated using peer and sector data.

Table 1 - Cyber Security Maturity Model

The objective of the Framework is to create an effective approach for addressing cyber security and managing cyber security risks within the Financial Sector. To achieve an appropriate cyber security maturity level, the Member Organizations should at least operate at maturity level 3 or higher as explained below.

2.4.1 Maturity Level 3

To achieve level 3 maturity, a Member Organization should define, approve and implement cyber security controls. In addition, it should monitor compliance with the cyber security documentation .

The cyber security documentation should clearly indicate “why”, “what” and “how” cyber security controls should be implemented. The cyber security documentation consists of cyber security policies, cyber security standards and cyber security procedures.

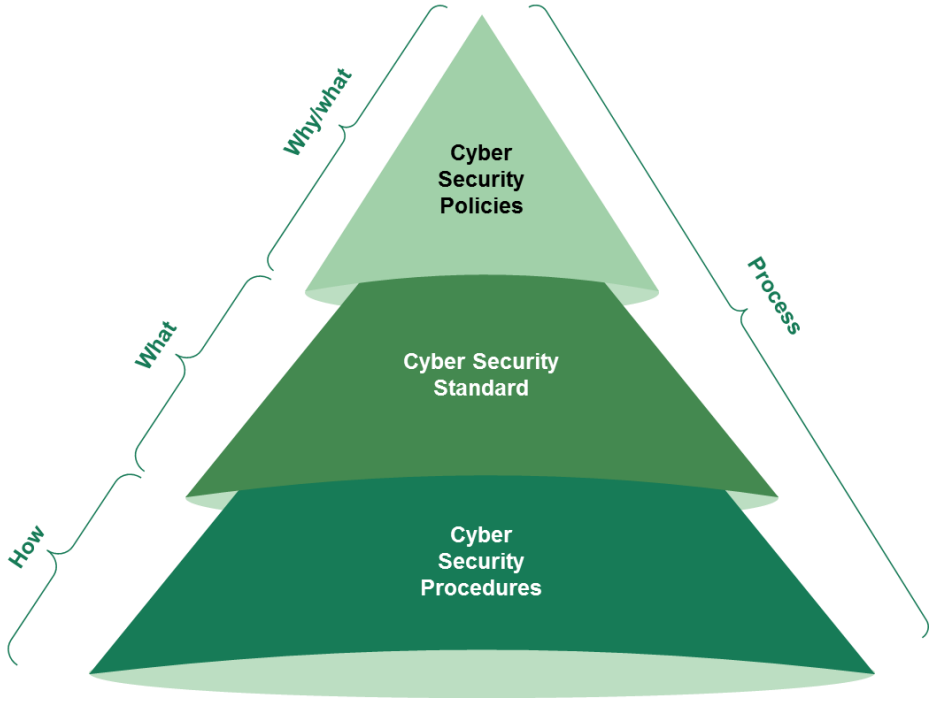


Figure 3 - Cyber Security Documentation Pyramid

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

Based on the cyber security policy, cyber security standards must be developed. These standards define "what" cyber security controls must be implemented, such as security and system parameters, segregation of duties, password rules, monitoring events and back-up and recovery rules. The standards support and reinforce the cyber security policy and are to be considered as cyber security baselines.

The step-by-step tasks and activities that should be performed by staff, third parties or customers of the Member Organization are detailed in the cyber security procedures. These procedures prescribe "how" the cyber security controls, tasks and activities have to be executed in the operating environment and support the safeguarding of the information assets of the Member Organization according to the cyber security policy and standards.

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 cyber security controls should be periodically monitored and evaluated using key performance indicators (KPIs).

2.4.2 Maturity Level 4

To achieve maturity level 4, the Member Organization should periodically measure and evaluate the effectiveness of implemented cyber security controls. In order to measure and evaluate whether the cyber security 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 cyber security controls. Continuous improvement is achieved through continuously analyzing the goals and achievements of cyber security and identifying structural improvements. Cyber security 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 cyber security controls, measuring the effectiveness of the cyber security controls and incorporating the cyber security controls within the enterprise risk management framework . Additionally, the performance of cyber security controls should be evaluated using peer and sector data.

3 Control domains

3.1 Cyber Security Leadership and Governance

The ultimate responsibility for cyber security rests with the board of the Member Organization. The board of the Member Organization can delegate its cyber security responsibilities to a cyber security committee (or a senior manager from a control function). The cyber security committee could be responsible for defining the cyber security governance and setting the Member Organization's cyber security strategy. The cyber security committee can also be responsible for defining a cyber security policy and ensuring the operational effectiveness of this cyber security policy.

To develop and maintain the cyber security policy and to execute the cyber security activities across the Member Organization, an independent cyber security function should be established.

3.1.1 Cyber Security Governance

Principle

A cyber security governance structure should be defined and implemented, and should be endorsed by the board.

Objective

To direct and control the overall approach to cyber security within the Member Organization.

Control considerations

1. A cyber security committee should be established and be mandated by the board.
2. The cyber security committee should be headed by an independent senior manager from a control function.
3. The following positions should be represented in the cyber security committee:
   a. senior managers from all relevant departments (e.g., COO, CIO, compliance officer, heads of relevant business departments);
   b. Chief information security officer (CISO);
   c. Internal audit may attend as an "observer.
4. A cyber security committee charter should be developed, approved and reflect:
   a. committee objectives;
   b. roles and responsibilities;
   c. minimum number of meeting participants;
   d. meeting frequency (minimum on quarterly basis).
5. A cyber security function should be established.
6. The cyber security function should be independent from the information technology function. To avoid any conflict of interest, the cyber security function and information technology function should have separate reporting lines, budgets and staff evaluations.
7. The cyber security function should report directly to the CEO/managing director of the Member Organization or general manager of a control function.
8. A full-time senior manager for the cyber security function, referred to as CISO, should be appointed at senior management level.
9. The Member Organization should :
   a. ensure the CISO has a Saudi nationality;
   b. ensure the CISO is sufficiently qualified;
   c. obtain no objection from SAMA to assign the CISO.
10. The board of the Member Organization should allocate sufficient budget to execute the required cyber security activities.

3.1.2 Cyber Security Strategy

Principle

A cyber security strategy should be defined and aligned with the Member Organization's strategic objectives, as well as with the Banking Sector's cyber security strategy.

Objective

To ensure that cyber security initiatives and projects within the Member Organization contribute to the Member Organization's strategic objectives and are aligned with the Banking Sector's cyber security strategy.

Control considerations

1. The cyber security strategy should be defined, approved, maintained and executed.
2. The cyber security strategy should be aligned with:
    a. the Member Organization's overall objectives;
    b. the legal and regulatory compliance requirements of the Member Organization;
    c. the Banking Sector's cyber security strategy.
3. The cyber security strategy should address:
    a. the importance and benefits of cyber security for the Member Organization;
    b. the anticipated future state of cyber security for the Member Organization to become and remain resilient to (emerging) cyber security threats;
    c. which and when cyber security initiatives and projects should be executed to achieve the anticipated future state.

3.1.3 Cyber Security Policy

Principle

A cyber security policy should be defined, approved and communicated.

Objective

To document the Member Organization's commitment and objectives of cyber security, and to communicate this to the relevant stakeholders.

Control considerations

1. The cyber security policy should be defined, approved and communicated.
2. The cyber security policy should be reviewed periodically according to a predefined and structured review process.
3. The cyber security policy should be:
    a. considered as input for other corporate policies of the Member Organization (e.g., HR policy, finance policy and IT policy);
    b. supported by detailed security standards (e.g., password standard, firewall standard) and procedures;
    c. based on best practices and (inter)national standards;
    d. communicated to relevant stakeholders.
4. The cyber security policy should include:
    a. a definition of cyber security;
    b. the Member Organization's overall cyber security objectives and scope;
    c. a statement of the board's intent, supporting the cyber security objectives;
    d. a definition of general and specific responsibilities for cyber security;
    e. the reference to supporting cyber security standards and procedures;
    f. cyber security requirements that ensure:
        1. information is classified in a way that indicates its importance to the Member Organization;

2. information is protected in terms of cyber security requirements, in line with the risk appetite;
3. owners are appointed for all information assets;
4. cyber security risk assessments are conducted for information assets;
5. relevant stakeholders are made aware of cyber security and their expected behavior (cyber security awareness program);
6. compliance with regulatory and contractual obligations are being met;
7. cyber security breaches and suspected cyber security weaknesses are reported;
8. cyber security is reflected in business continuity management.

3.1.4 Cyber Security Roles and Responsibilities

Principle

Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization. Additionally, all parties involved in cyber security should understand and take their role and responsibilities.

Objective

To ensure that relevant stakeholders are aware of the responsibilities with regard to cyber security and apply cyber security controls throughout the Member Organization.

Control considerations

1. The Board of Directors has the ultimate responsibility for cyber security, including:
   a. ensuring that sufficient budget for cyber security is allocated;
   b. approving the cyber security committee charter;
   c. endorsing (after being approved by the cyber security committee):
      1. the cyber security governance;
      2. the cyber security strategy;
      3. the cyber security policy.
2. The cyber security committee should be responsible for:
   a. monitoring, reviewing and communicating the Member Organization's cyber security risk appetite periodically or upon a material change in the risk appetite;
   b. reviewing the cyber security strategy to ensure that it supports the Member Organization objectives;
   c. approving, communicating, supporting and monitoring:
      1. the cyber security governance;
      2. the cyber security strategy;
      3. the cyber security policy;
      4. cyber security programs (e.g., awareness program, data classification program, data privacy, data leakage prevention, key cyber security improvements);
      5. cyber security risk management process;
      6. the key risk indicators (KRIs) and key performance indicators (KPIs) for cyber security.
3. The senior management should be responsible for:
   a. ensuring that standards, processes and procedures reflect security requirements (if applicable);
   b. ensuring that individuals accept and comply with the cyber security policy, supporting standards and procedures when they are issued and updated;
   c. ensuring that cyber security responsibilities are incorporated in the job descriptions of key positions and cyber security staff.
4. The CISO should be responsible for:
   a. developing and maintaining:
      1. cyber security strategy;
      2. cyber security policy;

3. cyber security architecture;
4. cyber security risk management process;

b. ensuring that detailed security standards and procedures are established, approved and implemented;
c. delivering risk-based cyber security solutions that address people, process and technology;
d. developing the cyber security staff to deliver cyber security solutions in a business context;
e. the cyber security activities across the Member Organization, including:
    1. monitoring of the cyber security activities (SOC monitoring);
    2. monitoring of compliance with cyber security regulations, policies, standards and procedures;
    3. overseeing the investigation of cyber security incidents;
    4. gathering and analyzing threat intelligence from internal and external sources;
    5. performing cyber security reviews;
f. conducting cyber security risk assessments on the Members Organization's information assets;
g. proactively supporting other functions on cyber security, including:
    1. performing information and system classifications;
    2. determining cyber security requirements for important projects;
    3. performing cyber security reviews.
h. defining and conducting the cyber security awareness programs;
i. measuring and reporting the KRIs and KPIs on:
    1. cyber security strategy;
    2. cyber security policy compliance;
    3. cyber security standards and procedures;
    4. cyber security programs (e.g., awareness program, data classification program, key cyber security improvements).

5. The internal audit function should be responsible for:
    a. performing cyber security audits.
6. All Member Organization's staff should be responsible for:
    a. complying with cyber security policy, standards and procedures.

3.1.5 Cyber Security in Project Management

Principle

Cyber security should be addressed in project management and project governance.

Objective

To ensure that the all the Member Organization's projects meet cyber security requirements.

Control considerations

1. Cyber security should be integrated into the Member Organization's project management methodology to ensure that cyber security risks are identified and addressed as part of a project.
2. The Member Organization's project management methodology should ensure that:
   a. cyber security objectives are included in project objectives;
   b. the cyber security function is part of all phases of the project;
   c. a risk assessment is performed at the start of the project to determine the cyber security risks and to ensure that cyber security requirements are addressed either by the existing cyber security controls (based on cyber security standards) or to be developed;
   d. cyber security risks are registered in the project-risk register and tracked;
   e. responsibilities for cyber security are defined and allocated;
   f. a cyber security review is performed by an independent internal or external party.

3.1.6 Cyber Security Awareness

Principle

A cyber security awareness program should be defined and conducted for staff, third parties and customers of the Member Organization.

Objective

To create a cyber security risk-aware culture where the Member Organization's staff, third parties and customers make effective risk-based decisions which protect the Member Organization's information.

Control considerations

1. The cyber security awareness programs should be defined, approved and conducted to promote cyber security awareness and to create a positive cyber security culture.
2. A cyber security awareness program should be defined and conducted for:
   a. staff of the Member Organization;
   b. third parties of the Member Organization;
   c. customers of the Member Organization.
3. The cyber security awareness program should target cyber security behaviors by tailoring the program to address the different target groups through multiple channels.
4. The activities of the cyber security awareness program should be conducted periodically and throughout the year.
5. The cyber security awareness program should at a minimum include:
   a. an explanation of cyber security measures provided;
   b. the roles and responsibilities regarding cyber security;
   c. information on relevant emerging cyber security events and cyber threats (e.g., spear-phishing, whaling).
6. The cyber security awareness program should be evaluated to:
   a. measure the effectiveness of the awareness activities;
   b. formulate recommendations to improve the cyber security awareness program.

7. Customer awareness should address for both retail and commercial customers and, at a minimum, include a listing of suggested cyber security mechanisms which customers may consider implementing to mitigate their own risk(s).

3.1.7 Cyber Security Training

Principle

Staff of the Member Organization should be provided with training regarding how to operate the Member Organization's systems securely and to address and apply cyber security controls.

Objective

To ensure that staff of the Member Organization are equipped with the skills and required knowledge to protect the Member Organization's information assets and to fulfil their cyber security responsibilities.

Control considerations

1. Specialist or security-related skills training should be provided to staff in the Member Organization's relevant functional area categories in line with their job descriptions, including:
   a. key roles within the organization;
   b. staff of the cyber security function;
   c. staff involved in developing and (technically) maintaining information assets;
   d. staff involved in risk assessments.
2. Education should be provided in order to equip staff with the skills and required knowledge to securely operate the Member Organization's information assets.

3.2 Cyber Security Risk Management and Compliance

Risk management is the ongoing process of identifying, analyzing, responding and monitoring and reviewing risks. The cyber security risk management process focusses specifically on managing risks related to cyber security. In order to manage cyber security risks, Member Organizations should:

- identify their cyber security risks – cyber security risk identification;
- determine the likelihood that cyber security risks will occur and the resulting impact – cyber security risk analysis;
- determine the appropriate response to cyber security risks and select relevant controls – cyber security risk response;
- monitor the cyber security risk treatment and review control effectiveness – cyber security risk monitoring and review.

The compliance with the cyber security controls should be subject to periodic review and audit.

3.2.1 Cyber Security Risk Management

Principle

A cyber security risk management process should be defined, approved and implemented, and should be aligned with the Member Organization's enterprise risk management process.

Objective

To ensure cyber security risks are properly managed to protect the confidentiality, integrity and availability of the Member Organization's information assets, and to ensure the cyber security risk management process is aligned with the Member Organization's enterprise risk management process.

Control considerations

1. The cyber security risk management process should be defined, approved and implemented.
2. The cyber security risk management process should focus on safeguarding the confidentiality, integrity and availability of information assets.
3. The cyber security risk management process should be aligned with the existing enterprise risk management process.
4. The cyber security risk management process should be documented and address:
   a. risk identification;
   b. risk analysis;
   c. risk response;
   d. risk monitoring and review.
5. The cyber security risk management process should address the Member Organization's information assets, including (but not limited to):
   a. business processes;
   b. business applications;
   c. infrastructure components.
6. The cyber security risk management process should be initiated:
   a. at an early stage of the project;
   b. prior to critical change;
   c. when outsourcing is being considered;
   d. when launching new products and technologies.
7. Existing information assets should be periodically subject to cyber security risk assessment based on their classification or risk profile.
8. The cyber security risk management activities should involve:
   a. business owners;

b. IT specialists;
c. cyber security specialists;
d. key user representatives.

9. The result of the risk assessment should be reported to the relevant business owner (i.e., risk owner) within the Member Organization;
10. The relevant business owner (i.e., risk owner) within the Member Organization should accept and endorse the risk assessment results.
11. The Member Organization's cyber security risk appetite and risk tolerance should be clearly defined and formally approved.

3.2.1.1 Cyber Security Risk Identification

Principle

Cyber security risk identification should be performed and should include the Member Organization's relevant assets, threats, existing controls and vulnerabilities.

Objective

To find, recognize and describe the Member Organization's cyber security risks.

Control considerations

1. Cyber security risk identification should be performed.
2. Identified cyber security risks should be documented (in a central register).
3. Cyber security risk identification should address relevant information assets, threats, vulnerabilities and the key existing cyber security controls.

3.2.1.2 Cyber Security Risk Analysis

Principle

A cyber security risk analysis should be conducted based on the likelihood that the identified cyber security risks will occur and their resulting impact.

Objective

To analyze and determine the nature and the level of the identified cyber security risks.

Control considerations

1. A cyber security risk analysis should be performed.
2. The cyber security risk analysis should address the level of potential business impact and likelihood of cyber security threat events materializing.

3.2.1.3 Cyber Security Risk Response

Principle

The cyber security risks of a Member Organization should be treated.

Objective

To ensure cyber security risks are treated (i.e., accepted, avoided, transferred or mitigated).

Control considerations

1. The relevant determined cyber security risks should be treated according to the Member Organization's risk appetite and cyber security requirements.
2. Cyber security risk response should ensure that the list of risk treatment options are documented (i.e., accepting, avoiding, transferring or mitigating risks by applying cyber security controls).

3. Accepting cyber security risks should include:
    a. the consideration of predefined limits for levels of cyber security risk;
    b. the approval and sign-off by the business owner, ensuring that:
        1. the accepted cyber security risk is within the risk appetite and is reported to the cyber security committee;
        2. the accepted cyber security risk does not contradict SAMA regulations.
4. Avoiding cyber security risks should involve a decision by a business owner to cancel or postpone a particular activity or project that introduces an unacceptable cyber security risk.
5. Transferring or sharing the cyber security risks should:
    a. involve sharing the cyber security risks with relevant (internal or external) providers;
    b. be accepted by the receiving (internal or external) provider(s);
    c. eventually lead to the actual transferring or sharing of the cyber security risk.
6. Applying cyber security controls to mitigate cyber security risks should include:
    a. identifying appropriate cyber security controls;
    b. evaluating the strengths and weaknesses of the cyber security controls;
        1. assessing the cost of implementing the cyber security controls;
        2. assessing the feasibility of implementing the cyber security controls;
        3. reviewing relevant compliance requirements for the cyber security controls;
    c. selecting cyber security controls;
    d. identifying, documenting and obtaining sign-off for any residual risk by the business owner.
7. Cyber security risk treatment actions should be documented in a risk treatment plan.

3.2.1.4 Cyber Risk Monitoring and Review

Principle

The progress cyber security risk treatment should be monitored and the effectiveness of revised or newly implemented cyber security controls should be reviewed.

Objective

To ensure that the cyber security risk treatment is performed according to the treatment plans. To ensure that the revised or newly implemented cyber security controls are effective.

Control considerations

1. The cyber security treatment should be monitored, including:
    a. tracking progress in accordance to treatment plan;
    b. the selected and agreed cyber security controls are being implemented.
2. The design and effectiveness of the revised or newly implemented cyber security controls should be reviewed.

3.2.2 Regulatory Compliance

Principle

A process should be established by the Member Organization to identify, communicate and comply with the cyber security implications of relevant regulations.

Objective

To comply with regulations affecting cyber security of the Member Organization.

Control considerations

1. A process should be established for ensuring compliance with relevant regulatory requirements affecting cyber security across the Member Organization. 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 cyber security policy, standards and procedures to accommodate any necessary changes (if applicable).

3.2.3 Compliance with (inter)national industry standards

Principle

The Member Organization should comply with mandatory (inter)national industry standards.

Objective

To comply with mandatory (inter)national industry standards.

Control considerations

1. The Member Organization should comply with:
   a. Payment Card Industry Data Security Standard (PCI-DSS);
   b. EMV (Europay, MasterCard and Visa) technical standard;
   c. SWIFT Customer Security Controls Framework – March 2017.

3.2.4 Cyber Security Review

Principle

The cyber security status of the Member Organization's information assets should be subject to periodic cyber security review.

Objective

To ascertain whether the cyber security controls are securely designed and implemented, and the effectiveness of these controls is being monitored.

Control considerations

1. Cyber security reviews should be periodically performed for critical information assets.
2. Customer and internet facing services should be subject to annual review and penetration tests.
3. Details of cyber security review performed should be recorded, including the results of review, issues identified and recommended actions.
4. The results of cyber security review should be reported to business owner.
5. Cyber security review should be subject to follow-up reviews to check that:
   a. all identified issues have been addressed;
   b. critical risks have been treated effectively;
   c. all agreed actions are being managed on an ongoing basis.

3.2.5 Cyber Security Audits

Principle

The cyber security status of the Member Organization's information assets should be subject to thorough, independent and regular cyber security audits performed in accordance with generally accepted auditing standards and SAMA cyber security framework.

Objective

To ascertain with reasonable assurance whether the cyber security controls are securely designed and implemented, and whether the effectiveness of these controls is being monitored.

Control considerations

1. Cyber security audits should be performed independently and according to generally accepted auditing standards and SAMA cyber security framework.
2. Cyber security audits should be performed according to the Member Organization's audit manual and audit plan.

3.3 Cyber Security Operations and Technology

In order to safeguard the protection of the operations and technology of the Member Organization's information assets and its staff, third parties and customers, the Member Organizations have to ensure that security requirements for their information assets and the supporting processes are defined, approved and implemented.

The compliance with these cyber security requirements should be monitored and the effectiveness of the cyber security controls should be periodically measured and evaluated in order to identify potential revisions of the controls or measurements.

3.3.1 Human Resources

Principle

The Member Organization should incorporate cyber security requirements into human resources processes.

Objective

To ensure that Member Organization staff's cyber security responsibilities are embedded in staff agreements and staff are being screened before and during their employment lifecycle.

Control considerations

1. The human resources process should define, approve and implement cyber security requirements.
2. The effectiveness of the human resources process should be monitored, measured and periodically evaluated.
3. The human resource process should include:
    a. cyber security responsibilities and non-disclosure clauses within staff agreements (during and after the employment);
    b. staff should receive cyber security awareness at the start and during their employment;
    c. when disciplinary actions will be applicable;
    d. screening and background check;
    e. post-employment cyber security activities, such as:
        1. revoking access rights;
        2. returning information assets assigned (e.g., access badge, tokens, mobile devices, all electronic and physical information).

3.3.2 Physical Security

Principle

The Member Organization should ensure all facilities which host information assets are physically protected against intentional and unintentional security events.

Objective

To prevent unauthorized physical access to the Member Organization information assets and to ensure its protection.

Control considerations

1. The physical security process should be defined, approved and implemented.
2. The effectiveness of the physical security process should be monitored, measured and periodically evaluated.
3. The physical security process should include (but not limited to):
    a. physical entry controls (including visitor security);
    b. monitoring and surveillance (e.g., CCTV, ATMs GPS tracking, sensitivity sensors);

c. protection of data centers and data rooms;
d. environmental protection;
e. protection of information assets during lifecycle (including transport and secure disposal, avoiding unauthorized access and (un)intended data leakage.

3.3.3 Asset Management

Principle

The Member Organization should define, approve, implement, communicate and monitor an asset management process, which supports an accurate, up-to-date and unified asset register.

Objective

To support the Member Organization in having an accurate and up-to-date inventory and central insight in the physical / logical location and relevant details of all available information assets, in order to support its processes, such as financial, procurement, IT and cyber security processes.

Control considerations

1. The asset management process should be defined, approved and implemented.
2. The effectiveness of the asset management process should be monitored, measured and periodically evaluated.
3. The asset management process should include:
   a. a unified register;
   b. ownership and custodianship of information assets;
   c. the reference to relevant other processes, depending on asset management;
   d. information asset classification, labeling and handling;
   e. the discovery of new information assets.

3.3.4 Cyber Security Architecture

Principle

The Member Organization should define, follow and review the cyber security architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities.

Objective

To support the Member Organization in achieving a strategic, consistent, cost effective and end-to-end cyber security architecture**.**

Control considerations

1. The cyber security architecture should be defined, approved and implemented.
2. The compliance with the cyber security architecture should be monitored.
3. The cyber security architecture should include:
   a. a strategic outline of cyber security capabilities and controls based on the business requirements;
   b. approval of the defined cyber security architecture;
   c. the requirement of having qualified cyber security architects;
   d. design principles for developing cyber security controls and applying cyber security requirements (i.e., the security-by-design principle);
   e. periodic review of the cyber security architecture.

3.3.5 Identity and Access Management

Principle

The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.

Objective
To ensure that the Member Organization only provides authorized and sufficient access privileges to approved users.

Control considerations
1. The identity and access management policy, including the responsibilities and accountabilities, should be defined, approved and implemented.
2. The compliance with the identity and access policy should be monitored.
3. The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.
4. The identity and access management policy should include:
    a. business requirements for access control (i.e., need-to-have and need-to-know);
    b. user access management (e.g., joiners, movers, leavers):
        1. all identified user types should be covered (i.e., internal staff, third parties);
        2. changes of job status or job positions for internal staff (e.g. joiner, mover and leaver) should be instigated by the human resources department;
        3. changes for external staff or third parties should be instigated by the appointed accountable party;
        4. user access requests are formally approved in accordance with business and compliance requirements (i.e., need-to-have and need-to-know to avoid unauthorized access and (un)intended data leakage));
        5. changes in access rights should be processed in a timely manner;
        6. periodically user access rights and profiles should be reviewed;
        7. an audit trail of submitted, approved and processed user access requests and revocation requests should be established;
    c. user access management should be supported by automation;
    d. centralization of the identity and access management function;
    e. multi-factor authentication for sensitive and critical systems and profiles;
    f. privileged and remote access management, which should address:
        1. the allocation and restricted use of privileged and remote access, specifying:
            a. multi-factor authentication should be used for all remote access;
            b. multi-factor authentication should be used for privilege access on critical systems based on a risk assessment;
        2. the periodic review of users with privileged and remote accounts;
        3. individual accountability;
        4. the use of non-personal privileged accounts, including:
            a. limitation and monitoring;
            b. confidentiality of passwords;
            c. changing passwords frequently and at the end of each session.

3.3.6 Application Security

Principle
The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated.

Objective

To ensure that sufficient cyber security controls are formally documented and implemented for all applications, and that the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.

Control considerations

1. The application cyber security standards should be defined, approved and implemented.
2. The compliance with the application security standards should be monitored.
3. The effectiveness of the application cyber security controls should be measured and periodically evaluated.
4. Application development should follow the approved secure system development life cycle methodology (SDLC).
5. The application security standard should include:
    a. secure coding standards;
    b. the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], identity and access management);
    c. the segregation of duties within the application (supported with a documented authorization matrix);
    d. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage);
    e. vulnerability and patch management;
    f. back-up and recovery procedures;
    g. periodic cyber security compliance review.

3.3.7 Change Management

Principle

The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated.

Objective

To ensure that all change in the information assets within the Member Organization follow a strict change control process.

Control considerations

1. The change management process should be defined, approved and implemented.
2. The compliance with the change management process should be monitored.
3. The effectiveness of the cyber security controls within the change management process should be measured and periodically evaluated.
4. The change management process should include:
    a. cyber security requirements for controlling changes to information assets, such as assessing the impact of requested changes, classification of changes and the review of changes;
    b. security testing, which should (if applicable) include:
        1. penetration testing;
        2. code review if applications are developed internally;
        3. code review of externally developed applications and if the source code is available
        4. a code review report (or equivalent, such as an independent assurance statement) in case the source code cannot be provided;
    c. approval of changes by the business owner;

d. approval from the cyber security function before submitting to Change Advisory Board (CAB);
e. approval by CAB;
f. post-implementation review of the related cyber security controls;
g. development, testing and implementation are segregated for both the (technical) environment and involved individuals;
h. the procedure for emergency changes and fixes;
i. fall-back and roll-back procedures.

3.3.8 Infrastructure Security

Principle

The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated.

Objective

To support that all cyber security controls within the infrastructure are formally documented and the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.

Control considerations

1. The infrastructure security standards should be defined, approved and implemented.
2. The compliance with the infrastructure security standards should be monitored.
3. The effectiveness of the infrastructure cyber security controls should be measured and periodically evaluated.
4. The infrastructure security standards should cover all instances of infrastructure available in the main datacenter(s), the disaster recovery data site(s) and office spaces.
5. The infrastructure security standards should cover all instances of infrastructure (e.g., operating systems, servers, virtual machines, firewalls, network devices, IDS, IPS, wireless network, gateway servers, proxy servers, email gateways, external connections, databases, file-shares, workstations, laptops, tablets, mobile devices, PBX).
6. The infrastructure security standard should include:
    a. the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance);
    b. the segregation of duties within the infrastructure component (supported with a documented authorization matrix);
    c. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage);
    d. the use of approved software and secure protocols;
    e. segmentation of networks;
    f. malicious code/software and virus protection (and applying application whitelisting and APT protection);
    g. vulnerability and patch management;
    h. DDOS protection (where applicable); this should include:
        1. the use of scrubbing services;
        2. specification of the bandwidth agreed;
        3. 24x7 monitoring by Security Operating Center (SOC), Service Provider (SP) and scrubbing provider;
        4. testing of DDOS scrubbing (minimum twice a year);
        5. DDOS services should be implemented for the main datacenter(s) as well as the disaster recovery site(s);
    i. back-up and recovery procedures;

j. periodic cyber security compliance review.

3.3.9 Cryptography

Principle

The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented.

Objective

To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.

Control considerations

1. A cryptographic security standard should be defined, approved and implemented.
2. The compliance with the cryptographic security standard should be monitored.
3. The effectiveness of the cryptographic security controls should be measured and periodically evaluated.
4. The cryptographic security standard should include:
   a. an overview of the approved cryptographic solutions and relevant restrictions (e.g., technically, legally);
   b. the circumstances when the approved cryptographic solutions should be applied;
   c. the management of encryption keys, including lifecycle management, archiving and recovery.

3.3.10 Bring Your Own Device (BYOD)

Principle

When the Member Organization allows the use of personal devices (e.g., smartphones, tablets, laptops) for business purposes, the use should be supported by a defined, approved and implemented cyber security standard, additional staff agreements and a cyber security awareness training.

Objective

To ensure that business and sensitive information of the Member Organization is securely handled by staff and protected during transmission and storage, when using personal devices.

Control considerations

1. The BYOD cyber security standard should be defined, approved and implemented.
2. The compliance with the BYOD cyber security standard should be monitored.
3. The effectiveness of the BYOD cyber security controls should be measured and periodically evaluated.
4. The BYOD standard should include:
   a. responsibilities of the user (including awareness training);
   b. information regarding the restrictions and consequences for staff when the Member Organization implements cyber security controls on their personal devices; for example when using modified devices (jailbreaking), terminating the employment or in case of loss or theft of the personal device;
   c. the isolation of business information from personal information (e.g., containerization);
   d. the regulation of corporate mobile applications or approved "public" mobile applications;
   e. the use of mobile device management (MDM); applying access controls to the device and business container and encryption mechanisms on the personal device (to ensure secure transmission and storage).

3.3.11 Secure Disposal of Information Assets

Principle

The information assets of the Member Organization should be securely disposed when the information assets are no longer required.

Objective

To ensure that the Member Organization's business, customer and other sensitive information are protected from leakage or unauthorized disclosure when disposed.

Control considerations

1. The secure disposal standard and procedure should be defined, approved and implemented.
2. The compliance with the secure disposal standard and procedure should be monitored.
3. The effectiveness of the secure disposal cyber security controls should be measured and periodically evaluated.
4. Information assets should be disposed in accordance with legal and regulatory requirements, when no longer required (i.e. meeting data privacy regulations to avoid unauthorized access and avoid (un)intended data leakage).
5. Sensitive information should be destroyed using techniques to make the information non-retrievable (e.g., secure erase, secure wiping, incineration, double crosscut, shredding).
6. The Member Organization should ensure that third party service providers used for secure disposal, transport and storage comply with the secure disposal standard and procedure and the effectiveness is periodically measured and evaluated.

3.3.12 Payment Systems

Principle

The Member Organization should define, approve, implement and monitor a cyber security standard for payment systems. The effectiveness of this process should be measured and periodically evaluated.

Objective

To ensure the Member Organization safeguards the confidentiality and integrity of shared banking systems.

Control considerations

- For Saudi Arabian Riyal Interbank Express (SARIE) information, please refer to the SARIE Information Security Policy, Version Issue 1.0 - June 2016.
- For mada information, please refer to the following sections in the mada Rules and Standards Technical Book (see appendix A):
  - Part IIIa - Security Framework, Version Issue 6.0.0 - May 2016
  - Part IIIb - HSM Requirements, Version Issue 6.0.0 - May 2016
  - SAMA CA IPK Certificate Procedures, Version Issue 6.0.1 – October 2016

3.3.13 Electronic Banking Services

Principle

The Member Organization should define, approve, implement and monitor a cyber security standard for electronic banking services. The effectiveness of this standard should be measured and periodically evaluated.

Objective

To ensure the Member Organization safeguards the confidentiality and integrity of the customer information and transactions.

Control Considerations

1. The cyber security standards for electronic banking services should be defined, approved and implemented.
2. The compliance with cyber security standards for electronic banking services should be monitored.
3. The effectiveness of the cyber security standard for electronic banking services should be measured and periodically evaluated.
4. Electronic banking services security standard should cover:
   a. use of brand protection measures to protect online services including social media.
   b. online, mobile and phone banking:
      1. use of official application stores and websites (applicable for online and mobile banking);
      2. use of detection measures and take-down of malicious apps and websites (applicable for online and mobile banking);
      3. use of sandboxing (applicable for online and mobile banking);
      4. use of non-caching techniques (applicable for online and mobile banking);
      5. use of communication techniques to avoid ‘man-in-the-middle’-attacks (applicable for online and mobile banking);
      6. use of multi-factor authentication mechanisms:
         a. multi-factor authentication should be used during the registration process for the customer in order to use of electronic banking services;
         b. multi-factor authentication should be implemented for all electronic banking services available to customers;
         c. the use of hard and soft tokens should be password protected;

d. revoking the access of customers after 3 successive incorrect passwords or invalid PINs;
e. the process for changing the customer mobile number should only be done from either a branch or ATM;
f. the processes for requesting and activating of the multi-factor authentication should be done through different delivery channels;
g. multi-factor authentication should be implemented for the following processes:
    1. sign-on;
    2. adding or modifying beneficiaries;
    3. adding utility and government payment services;
    4. high-risk transactions (when it exceeds predefined limits);
    5. password reset;

7. the processes for adding and activating beneficiaries should be done through different delivery channels (applicable for mobile and online banking);
8. high availability of the electronic banking services should be ensured;
9. scheduled downtime of the electronic banking services should be timely communicated to SAMA and customers;
10. contractual agreements between the Member Organization and the customer addressing the roles, responsibilities and liabilities for both the Member Organization and the customers;
11. obtaining approval of SAMA before launching a new electronic banking service.

c. ATMs and POSs:
    1. prevention and detection of exploiting the ATM/POS application and infrastructure vulnerabilities (e.g., cables, (USB)-ports, rebooting);
    2. cyber security measures, such as hardening of operating systems, malware protection, privacy screens, masking of passwords or account numbers (e.g., screen and receipt), geo-blocking (e.g., disable cards per default for outside GCC countries, disable magnetic strip transactions), video monitoring (CCTV), revoking cards after 3 successive invalid PINs, anti-skimming solutions (hardware/software), and PIN-pad protection;
    3. remote stopping of ATMs in case of malicious activities.
d. SMS instant notification services:
    1. SMS messages should not contain sensitive data (e.g., account balance - except for credit cards);
    2. SMS alert should be sent to both mobile numbers (old and new) when the customer's mobile number has been changed;
    3. SMS notification should be sent to the customer's mobile number when requesting a new multi-factor authentication mechanism.
    4. SMS notification should be sent to the customer's mobile number for all retail and personal financial transactions.
    5. SMS notification should be sent to the customer's mobile number when beneficiaries are added, modified and activated.

3.3.14 Cyber Security Event Management

Principle

The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated.

Objective

To ensure timely identification and response to anomalies or suspicious events within regard to information assets.

Control considerations

1. The security event management process should be defined, approved and implemented.
2. The effectiveness of the cyber security controls within the security event management process should be measured and periodically evaluated.
3. To support this process a security event monitoring standard should be defined, approved and implemented.
   a. the standard should address for all information assets the mandatory events which should be monitored, based on the classification or risk profile of the information asset.
4. The security event management process should include requirements for:
   a. the establishment of a designated team responsible for security monitoring (i.e., Security Operations Center (SOC));
   b. skilled and (continuously) trained staff;
   c. a restricted area to facilitate SOC activities and workspaces;
   d. resources required continuous security event monitoring activities (24x7);
   e. detection and handling of malicious code and software;
   f. detection and handling of security or suspicious events and anomalies;
   g. deployment of security network packet analysis solution;
   h. adequately protected logs;
   i. periodic compliance monitoring of applications and infrastructure cyber security standards
   j. automated and centralized analysis of security loggings and correlation of event or patterns (i.e., Security Information and Event Management (SIEM));
   k. reporting of cyber security incidents;
   l. independent periodic testing of the effectiveness of the security operations center (e.g., red-teaming).

3.3.15 Cyber Security Incident Management

Principle

The Member Organization should define, approve and implement a cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated.

Objective

To ensure timely identification and handling of cyber security incidents in order to reduce the (potential) business impact for the Member Organization.

Control considerations

1. The cyber security incident management process should be defined, approved, implemented and aligned with the enterprise incident management process.
2. The effectiveness of the cyber security controls within the cyber security incident management process should be measured and periodically evaluated.
3. The standard should address the mandatory and suspicious security events which should be responded to.
4. The security incident management process should include requirements for:
   a. the establishment of a designated team responsible for security incident management;
   b. skilled and (continuously) trained staff;
   c. sufficient capacity available of certified forensic staff for handling major incidents (e.g., internal staff or contracting an external forensic team);
   d. a restricted area to facilitate the computer emergency response team (CERT) workspaces;
   e. the classification of cyber security incidents;
   f. the timely handling of cyber security incidents, recording and monitoring progress;

g. the protection of relevant evidence and loggings;
h. post-incident activities, such as forensics, root-cause analysis of the incidents;
i. reporting of suggested improvements to the CISO and the Committee;
j. establish a cyber security incident repository.

5. The Member Organization should inform 'SAMA IT Risk Supervision' immediately when a medium or high classified security incident has occurred and identified.
6. The Member Organization should obtain 'no objection' from 'SAMA IT Risk Supervision' before any media interaction related to the incident.
7. The Member Organization should submit a formal incident report 'SAMA IT Risk Supervision' after resuming operations, including the following incident details:
   a. title of incident;
   b. classification of the incident (medium or high);
   c. date and time of incident occurred;
   d. date and time of incident detected;
   e. information assets involved;
   f. (technical) details of the incident;
   g. root-cause analysis;
   h. corrective activities performed and planned;
   i. description of impact (e.g., loss of data, disruption of services, unauthorized modification of data, (un)intended data leakage, number of customers impacted);
   j. total estimated cost of incident;
   k. estimated cost of corrective actions.

3.3.16 Threat Management

Principle

The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated.

Objective

To obtain an adequate understanding of the Member Organization's emerging threat posture.

Control considerations

1. The threat intelligence management process should be defined, approved and implemented.
2. The effectiveness of the threat intelligence management process should be measured and periodically evaluated.
3. The threat intelligence management process should include:
   a. the use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tooling, Security Information and Event Monitoring (SIEM), support functions (e.g., Legal, Audit, IT Helpdesk, Forensics, Fraud Management, Risk Management, Compliance);
   b. the use of reliable and relevant external sources, such as SAMA, government agencies, security forums, (security) vendors, security organizations and specialist notification services;
   c. a defined methodology to analyze the threat information periodically;
   d. the relevant details on identified or collected threats, such as modus operandi, actors, motivation and type of threats;
   e. the relevance of the derived intelligence and the action-ability for follow-up (for e.g., SOC, Risk Management);
   f. sharing the relevant intelligence with the relevant stakeholders (e.g., SAMA, BCIS members).

3.3.17 Vulnerability Management

Principle

The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated**.**

Objective

To ensure timely identification and effective mitigation of application and infrastructure vulnerabilities in order to reduce the likelihood and business impact for the Member Organization.

Control considerations

1. The vulnerability management process should be defined, approved and implemented.
2. The effectiveness of the vulnerability management process should be measured and periodically evaluated.
3. The vulnerability management process should include:
    a. all information assets;
    b. frequency of performing the vulnerability scan (risk-based);
    c. classification of vulnerabilities;
    d. defined timelines to mitigate (per classification);
    e. prioritization for classified information assets;
    f. patch management and method of deployment.

3.4 Third Party Cyber Security

When Member Organizations do rely on, or have to deal with third party services, it is key to ensure the same level of cyber security protection is implemented at the third party, as within the Member Organization.

This paragraph describes how the cyber security requirements between the Member Organization and Third Parties should be organized, implemented and monitored. Third Parties in this Framework are defined as, information services providers, outsourcing providers, cloud computing providers, vendors, suppliers, governmental agencies, etc.

3.4.1 Contract and Vendor Management

Principle

The Member Organization should define, approve, implement and monitor the required cyber security controls within the contract and vendor management processes.

Objective

To ensure that the Member Organization's approved cyber security requirements are appropriately addressed before signing the contract, and the compliance with the cyber security requirements is being monitored and evaluated during the contract life-cycle.

Control Considerations

1. The cyber security requirements should be defined, approved, implemented and communicated within the contract and vendor management processes.
2. The compliance with contract and vendor management process should be monitored.
3. The effectiveness of the cyber security controls within the contract and vendor management process should be measured and periodically evaluated.
4. These contract and vendor management processes should cover:
   a. whether the involvement of the cyber security function is actively required (e.g., in case of due diligence);
   b. the baseline cyber security requirements which should be applied in all cases;
   c. the right to periodically perform cyber security reviews and audits.
5. The contract management process should cover requirements for:
   a. executing a cyber security risk assessment as part of the procurement process;
   b. defining the specific cyber security requirements as part of the tender process;
   c. evaluating the replies of potential vendors on the defined cyber security requirements;
   d. testing of the agreed cyber security requirements (risk-based);
   e. defining the communication or escalation process in case of cyber security incidents;
   f. ensuring cyber security requirements are defined for exiting, terminating or renewing the contract (including escrow agreements if applicable);
   g. defining a mutual confidentiality agreement.
6. The vendor management process (i.e., service level management) should cover requirements for:
   a. periodic reporting, reviewing and evaluating the contractually agreed cyber security requirements (in SLAs).

3.4.2 Outsourcing

Principle

The Member Organization should define, implement and monitor the required cyber security controls within outsourcing policy and outsourcing process. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.

Objective

To ensure that the Member Organization's cyber security requirements are appropriately addressed before, during and while exiting outsourcing contracts.

Control Considerations

1. The cyber security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within Member Organization.
2. The cyber security requirements regarding the outsourcing policy and process should be measured and periodically evaluated.
3. The outsourcing process should include:
   a. the approval from SAMA prior to material outsourcing;
   b. the involvement of the cyber security function;
   c. compliance with the SAMA circular on outsourcing.

3.4.3 Cloud Computing

Principle

The Member Organization should define, implement and monitor the required cyber security controls within the cloud computing policy and process for hybrid and public cloud services. The effectiveness of the defined cyber security controls should periodically be measured and evaluated.

Please note that this requirement is not applicable to private cloud services (= internal cloud).

Objective

To ensure that all functions and staff within the Member Organization are aware of the agreed direction and position on hybrid and public cloud services, the required process to apply for hybrid and public cloud services, the risk appetite on hybrid and public cloud services and the specific cyber security requirements for hybrid and public cloud services.

Control Considerations

1. The cyber security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and implemented and communicated within Member Organization.
2. The compliance with the cloud computing policy should be monitored.
3. The cyber security controls regarding the cloud computing policy and process for hybrid and public cloud services should be periodically measured and evaluated.
4. The cloud computing policy for hybrid and public cloud services should address requirements for:
   a. the process for adopting cloud services, including that:
      1. a cyber security risk assessment and due diligence on the cloud service provider and its cloud services should be performed;
      2. the Member Organization should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider;
      3. a contract should be in place, including the cyber security requirements, before using cloud services;
   b. data location, including that:

1. in principle only cloud services should be used that are located in Saudi Arabia, or when cloud services are to be used outside Saudi Arabia that the Member Organization should obtain explicit approval from SAMA;

c. data use limitations, including that:
   1. the cloud service provider should not use the Member Organization's data for secondary purposes;
d. security, including that:
   1. the cloud service provider should implement and monitor the cyber security controls as determined in the risk assessment for protecting the confidentiality, integrity and availability of the Member Organization's data;
e. data segregation, including that:
   1. the Member Organization's data is logically segregated from other data held by the cloud service provider, including that the cloud service provider should be able to identify the Member Organization's data and at all times should be able to distinguish it from other data.
f. business continuity, including that:
   1. business continuity requirements are met in accordance with the Member Organization's business continuity policy;
g. audit, review and monitoring, including that:
   1. the Member Organization has the right to perform a cyber security review at the cloud service provider;
   2. the Member Organization has the right to perform a cyber security audit at the cloud service provider;
   3. the Member Organization has the right to perform a cyber security examination at the cloud service provider;
h. exit, including that:
   1. the Member Organization has termination rights;
   2. the cloud service provider has to return the Member Organization's data on termination;
   3. the cloud service provider has to irreversibly delete the Member Organization's data on termination.

Appendices

Appendix A - Overview previous issued SAMA circulars

The Framework Supersedes the following previously issued SAMA circulars:

- Assessment of protection and information security systems for all banks, 25514-MAT-53331, 25/10/2012;
- Enhance monitoring controls over ATMs, 49616-MAT-24388, 8/9/2012;
- Requirements to reduce DoS/DDoS attacks, 361000033746, 24/12/2014;
- Cards Cloning, 361000078157, 19/3/2015;
- Independency of Information Security, 361000036797, 30/12/2014;
- Caution from electronic fraud, 17722-MAT, 29/6/2011;
- Confidentiality of banking information, 341000065707, 6/4/2013;
- SAMA regulation about mobile banking, 341000096665, 16/6/2013;
- Using forged ATM cards to withdrawals from client accounts, 644/MAT/33043, 24/6/2009;
- Token service, 341000071570, 18/4/2013;
- E-Banking Rules, 11231-MAG-23612, 9/4/2010;
- Multi-factor authentication, 789/MAT/40690, 6/8/2009.

The framework refers to the following SAMA circulars or documents with regard to Payment Systems:

- For Saudi Arabian Riyal Interbank Express (SARIE) information, please refer to the SARIE Information Security Policy, Version Issue 1.0 - June 2016.
- For mada information, please refer to the following sections in the mada Rules and Standards Technical Book (see appendix A):
  - Part IIIa - Security Framework, Version Issue 6.0.0 - May 2016
  - Part IIIb - HSM Requirements, Version Issue 6.0.0 - May 2016
  - SAMA CA IPK Certificate Procedures, Version Issue 6.0.1 – October 2016

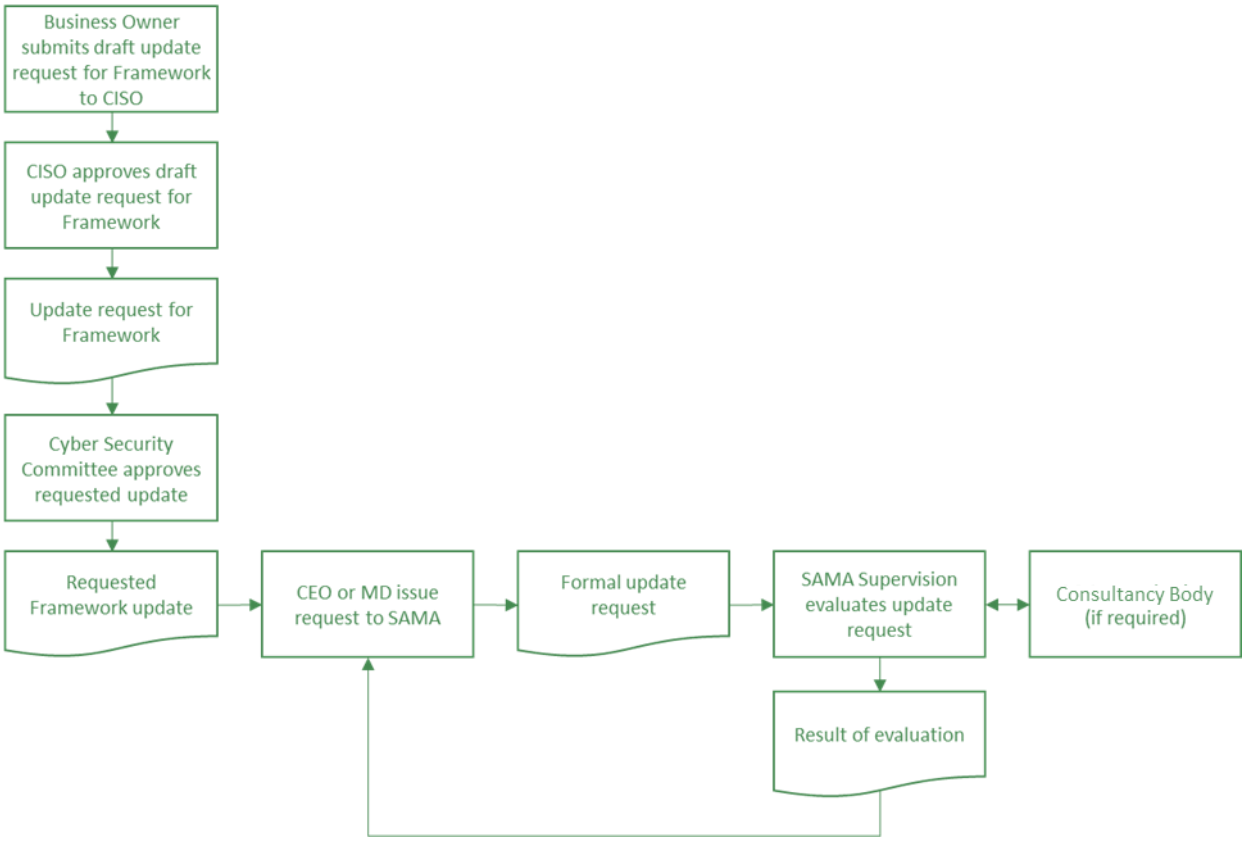
The framework refers to the following SAMA circulars or documents with regard to outsourcing and business continuity management:

- Rules on outsourcing, 424-BCS-34720, 20/7/2008;
- Business Continuity Framework, 381000058504, 01/06/1438H

Appendix B - 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 CISO before submitting to cyber security committee.
- The request should be approved by Member Organization's cyber steering committee.
- The request should be sent formally in writing to SAMA via the Member Organization's CEO or managing director to the deputy governor of Supervision.
- 'SAMA IT Risk Supervision' 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 C – Framework Update request form

Request to Update the SAMA Cyber Security Framework

A submission to the deputy governor of SAMA IT Risk Supervision

The Saudi Arabian Monetary Authority (SAMA) will consider requests from a member organization (MO) to update its Cyber Security 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

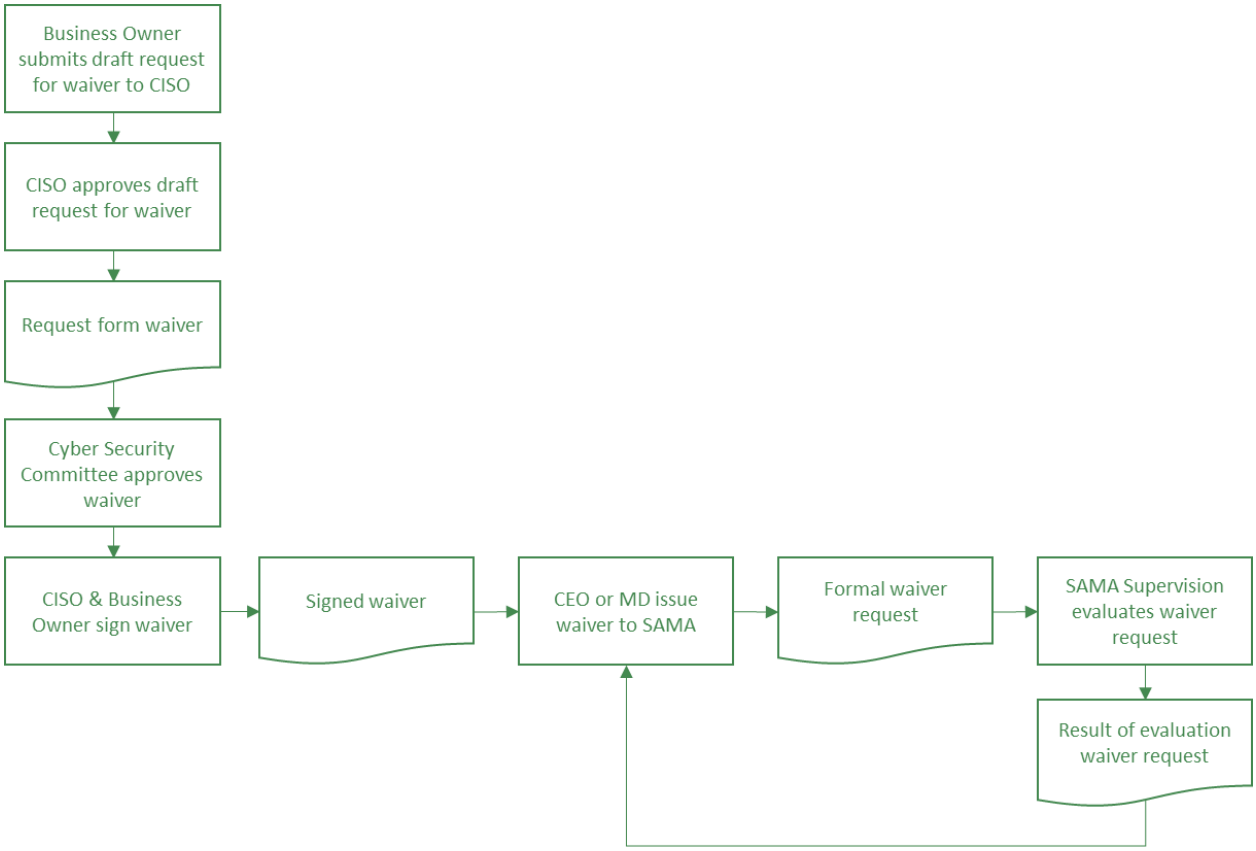
1. MO's CISO APPROVAL*	DATE*	
2. MO'S CYBER SECURITY COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*

* Denotes required fields

Appendix D - 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 bank could not meet the required control.
- Details description about the available or suggested compensating controls.
- The waiver request should first be approved by CISO before submitting to cyber security committee.
- The waiver request should approved by the members of Member Organization's cyber security committee.
- The waiver request should be signed by the CISO and relevant (business) owner.
- The waiver request should be formally issued in writing to SAMA via the Member Organization's CEO or managing director to the deputy governor of Supervision.
- 'SAMA IT Risk Supervision' 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 E – Framework Waiver request form

Request for Waiver from the SAMA Cyber Security Framework

A submission to the deputy governor of SAMA IT Risk Supervision

The Saudi Arabian Monetary Authority (SAMA) will consider requests for waiver from a member organization (MO) from its Cyber Security 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 CISO APPROVAL*	DATE*	
2. MO'S CYBER SECURITY COMMITTEE APPROVAL*	APPROVER'S POSITION*	DATE*

* Denotes required fields

Appendix F - Glossary

Term	Description
Access management	Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users.
Anti-skimming solution	A solution that monitors an ATM or POS environment for illegally mounted intrusion mechanisms (both hard- and software).
Application whitelisting	A list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which use blacklists to block known bad activity and permit all other, application whitelisting technologies are designed to permit known activity and block all other. (NIST SP 800-167 Guide to Application Whitelisting)
APT	An advanced persistent threat (APT) is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Asset management	The systematic process of deploying, operating, maintaining, upgrading, and disposing of assets in a safe, secure and cost effective manner.
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Audit trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Authorization matrix	A matrix that defines the rights and permissions a specific role needs for information. The matrix lists each user, the business process tasks he or she performs, and the affected systems.
Availability	Ensuring timely and reliable access to and use of information. (NISTIR 7298r2 Glossary of Key Information Security Terms)

Business applications	Any software or set of computer programs that are used by business users to perform various business functions.
Business continuity	The capability of an organization to continue delivery of IT and business services at acceptable predefined levels following a disruptive incident. (ISO 22301:2012 Societal security -- Business continuity management systems)
BYOD	Bring your own device (BYOD) refers to personally owned devices (laptops, tablets, and smart phones) that employees and contractors are permitted to use to carry out business functions.
CCTV	Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
CEO	The Chief Executive Officer (CEO) is the executive with the chief decision-making authority in an organization.
CERT	A computer emergency response team (CERT) is a group of experts that handle computer security incidents.
Change management	The controlled identification and implementation of required changes within a business or information systems.
CIO	Chief information officer (CIO). A senior-level executive responsible for the information technology and computer systems that support enterprise goals.
CISO	Chief information security officer (CISO). A senior-level executive responsible for establishing and maintaining the enterprise cyber security vision, strategy, and program to ensure information assets and technologies are adequately protected.
Classification scheme	Refer to 'Data classification'.
Cloud computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models: (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). (NISTIR 7298r2 Glossary of Key Information Security Terms)
Compensating Security Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in place of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NISTIR 7298r2 Glossary of Key Information Security Terms)

Containerization	A virtualization method for deploying and running distributed applications without launching a virtual machine for each application. Instead, multiple isolated systems run on a single control host and access a single kernel.
Control effectiveness	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance. (NISTIR 7298r2 Glossary of Key Information Security Terms)
COO	Chief Operating Officer. A senior-level executive responsible for the daily operation of the organization.
Cryptographic solutions	Solutions pertaining to cryptography. Refer to 'Cryptography'.
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Custodianship	Responsibility for controlling the access to and the accounting, safeguarding, and destruction of information according to an organization's security policy .
Cyber risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security	Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.
Cyber security architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for the enterprise’s security processes, cyber security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security audit	Independent review and examination of security-related records and activities to provide reasonable assurance that system controls are adequate and that established policies and operational procedures are compliant. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security awareness	Activities which seek to focus an individual’s attention on a cyber security issues. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security awareness program	A program that explains proper rules of behavior for the safe and secure use of IT systems and information. The program communicates cyber security policies and procedures that need to be followed.
Cyber security control	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (NISTIR 7298r2 Glossary of Key Information Security Terms)

Cyber security examination	A review of security-related records and activities of records and activities to assess the adequacy of system controls and to ensure compliance with established policies and operational procedures. An examination does not provide assurance.
Cyber security function	A function, independent from the information technology function, that is headed by a CISO and that reports directly to the CEO/managing director of the Member Organization or general manager of a control function. The information security function is responsible for: – supporting information security policies, defining information security roles and responsibilities, and setting information security goals for implementation; – providing information security and information risk management frameworks; – identifying known and emerging information security issues; – identifying shifts in the organization's implicit information risk appetite; – assisting management in developing information security processes and controls to manage information security risks and information security issues; – providing guidance and training on information security and information risk management processes; – facilitating and monitoring implementation of effective information security and information risk management practices by operational management; – alerting operational management to emerging information security issues and changing regulatory and information risk scenarios; – monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations in connection with information security , and timely remediation of deficiencies.
Cyber security governance	A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction for cyber security, ensuring that cyber security objectives are achieved, ascertaining that cyber risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
Cyber security 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. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security incident management	The monitoring and detection of security events on an information systems and the execution of proper responses to those events.
Cyber security policy	A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security program	Top-down management structure and mechanism for coordinating security activities throughout the organization.

Cyber security review	Independent review and examination of security-related records and activities to provide limited assurance that system controls are adequate and that established policies and operational procedures are compliant. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security risk assessment	The process of identifying risks to organizational operations, organizational assets, individuals, other organizations, and the nation, arising through the operation of an information system. A part of risk management, it incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security risk management	The process of managing risks to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and consists of (i) a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Cyber security strategy	A high-level plan, consisting of projects and initiatives, to mitigate cyber security risks while complying with legal, statutory, contractual, and internally prescribed requirements.
Cyber security threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Data classification	The conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of business assets.
Double crosscut	A technique using saws or blades to cut media into confetti-sized bits.
Enterprise architecture	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. (NISTIR 7298r2 Glossary of Key Information Security Terms)

Enterprise risk management	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Fall-back	Business procedures and measures, undertaken when events have triggered the execution of either a business continuity plan or a contingency plan.
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Formally documented	Documentation that is written, approved by the senior leadership and disseminated to relevant parties.
Gateway server	Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. It directs, but does not filter, connections between networks. See also 'Proxy server'.
GCC countries	Members of the Gulf Cooperation Council (GCC), a political and economic alliance of the Kingdom of Bahrain, the State of Kuwait, the Sultanate of Oman, the State of Qatar, the Kingdom of Saudi Arabia and the United Arab Emirates.
Geo-blocking	A form of internet censorship where access to content is restricted based upon the user's geographical location.
Hard token	A hard token (a.k.a. an 'authentication token') is a hardware security device that is used to authorize a user to a system. Some hard tokens are used in combination with other security measures to further enhance security (known as multi-factor authentication). See also 'Soft token'.
Hybrid cloud services	A cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. (Gartner)
Identity management	The process of controlling information about users on computers, including how they authenticate and what systems they are authorized to access and/or what actions they are authorized to perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified. Managed entities typically include users, hardware and network resources and even applications.
IDS	An intrusion detection system (IDS) is a hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). (NISTIR 7298r2 Glossary of Key Information Security Terms)
Incident management	Refer to 'Cyber security incident management'.

Incident management plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system(s). Also Refer to 'Cyber security incident management'. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Incineration	A method of media and device destruction using high heat.
Indicator of compromise	A forensic artifact or remnant of an intrusion that can be identified on a host or network. (RSA)
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (NISTIR 7298r2 Glossary of Key Information Security Terms)
IPS	An intrusion prevention system (IPS) can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Irreversibly delete	See 'Secure erase'
Jailbreaking	A form of privilege escalation that removes software restrictions imposed by the software manufacturer and often results in unlimited privileges on the device.
Key performance indicator	A type of performance measurement that evaluate the success of an organization or of a particular activity in which it engages. Numerical threshold(s) are typically used to categorize performance.
Key risk indicator	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.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NISTIR 7298r2 Glossary of Key Information Security Terms)
MDM	Mobile device management (MDM) is an industry term for the administration of mobile devices.
Member organization	Organizations affiliated with SAMA.
Mobile device	Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards or drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (NISTIR 7298r2 Glossary of Key Information Security Terms)
Multi-factor authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). (NISTIR 7298r2 Glossary of Key Information Security Terms)

NIST	The (U.S.) National Institute of Standards and Technology (www.nist.gov)
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. (NISTIR 7298r2 Glossary of Key Information Security Terms)
PBX	A private branch exchange (PBX) is a telephone exchange or switching system that serves a private organization and performs concentration of central office lines and provides intercommunication between a large number of telephone stations within the organization.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary cyber security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.
Penetration testing	A test methodology in which assessors, working under specific constraints and optionally using all available documentation (e.g., system design, source code, manuals), attempt to circumvent the security features of an information system. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Personal devices	Devices, like a smart phone, that are not owned or issued by the organization.
Physical security	The physical protection of facilities that host information assets against intentional and unintentional security events.
PIN	A password consisting only of decimal digits. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Privileged account / access	An information system account with approved authorizations to perform security-relevant functions that ordinary users are not authorized to perform. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Proxy server	A server that services the requests of its clients by forwarding those requests to other servers. It directs and filters connections between networks. See also 'Gateway server'.
Public cloud service	Services that are rendered over a network that is open to the public. Public cloud providers own and operate the infrastructure at their data center and access is generally via the Internet.
Red-teaming	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

Resilience	The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
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. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Risk appetite	The amount and type of risk that an organization is willing to take in order to meet their strategic objectives. Also refer to 'Risk tolerance'. (ISO/Guide 73:2009 Risk management — Vocabulary)
Risk profile	A description of any set of risks that relate to the whole organization, part of the organization, or as otherwise defined. The risk profile will outline the number of risks, type of risk and potential effects of risks. (ISO/Guide 73:2009 Risk management — Vocabulary)
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'. (COSO Internal Control — Integrated Framework)
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. (ISO/Guide 73:2009 Risk management — Vocabulary)
Risk-aware culture	The shared values, beliefs, knowledge, attitudes and understanding about risk within an organization. In a strong risk culture people proactively identify, discuss and take responsibility for risks. (Institute of Risk Management)
Root-cause analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Sandboxing	A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Scrubbing services	A service that analyzes an organization's network traffic and removes malicious traffic (DDoS, known vulnerabilities and exploits).

SDLC	A system development lifecycle (SDLC) describes the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Secure coding standard	A document that describes a uniform set of rules and guidelines for developing computer software that protects against the accidental introduction of security vulnerabilities. Examples includes OWASP's Secure Coding Practices and the Software Engineering Institute's Secure Coding Standards.
Secure disposal	The disposing of equipment and media that minimizes the risk of unwanted disclosure. See also 'Secure erase', 'Secure wiping', 'Incineration', and 'Double crosscut'.
Secure erase	An overwrite technology using a firmware-based process to overwrite a hard drive. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Secure wiping	Refer to 'Secure erase'.
Security architecture	Refer to 'Cyber security architecture'.
Security control	Refer to 'Cyber security control'
Security testing	Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Sensitive information	Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the organizational affairs, or the privacy to which individuals are entitled. Additionally, sensitive information is the information deemed sensitive according to the organizational data classification policy (see 'Data classification'). (NISTIR 7298r2 Glossary of Key Information Security Terms)
SIEM	A security information and event management (SIEM) tool is a system that provides the ability to gather security data from information system components and presents that data as actionable information via a single interface. (NISTIR 7298r2 Glossary of Key Information Security Terms)
SLA	A service level agreement (SLA) defines the specific responsibilities of the service provider and sets the customer expectations. (NISTIR 7298r2 Glossary of Key Information Security Terms)
SOC	A security operations center (SOC) is a specialized location (and team) where security-related data from enterprise information systems (e.g., web sites, applications, databases, servers, networks, desktops and other devices) is monitored, assessed and actioned. The SOC is often dedicated to the detection, investigation and potential response to indicators of compromise. The SOC works closely with, and disseminates, collated security-related information to other areas of the organization (e.g., the cyber security function, incident management team and IT service owners).

Soft token	A soft token (a.k.a. a virtual token) is a software version of a hard token. Soft tokens are typically generated by a central server that runs security software and sent to users' devices. Some hard tokens are used in combination with other security measures to further enhance security (known as multi-factor authentication). See also 'Hard token'.
Strategy	Refer to 'Cyber security strategy'.
Threat	Refer to 'Cyber security threat'
Threat intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. (Gartner)
Threat landscape	1. An overview of threats, together with current and emerging trends. 2. A collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends. (ENISA)
Token	Something that the user possesses and controls (typically a key or password) that is used to authenticate the user's identity. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Vendor management	The practice of ensuring that third-party service providers adhere to the same information security standards that an organization must comply with and includes periodic security assessments.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Vulnerability management	Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. Also refer to 'Vulnerability'.

P.O. Box 12531 Riyadh 11483,
Kingdom of Saudi Arabia
Tel.: +966 11 221 1000,
www.sama.gov.sa