Cyber Resilience Fundamental Requirements (CRFR)

January 2022

Version 1.0

البنك المركزي السعودي
SAMA
Saudi Central Bank

البنك المركزي السعودي
SAMA
Saudi Central Bank

Contents

1 Introduction

Modern society has high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data. Information assets and online financial services are now critically important to all public and private organizations and broader society. These services are fundamental to the global and national economy, vital to digital innovation and important to broader national security. This importance emphasizes the need to safeguard sensitive data, transactions and the availability of services, and thereby ensure confidence in the Saudi Financial Sector.

Not many industries have seen such a vivid increase in innovation like FinTech. Throughout the past decade, there has been an increase in the number of products and services that have reached the market which is already delivering significant benefits to consumers and financial institutions. However, the increasing use of emerging technologies also brings cyber resilience risks that may impact the financial stability of the financial sector ecosystem.

In November 2019, Saudi Central Bank (herein "SAMA") developed a regulatory sandbox framework1 in order to understand and assess the impact of new technologies in the KSA's FS market, as well as to help transforming the Saudi market into a smart financial centre. SAMA has designed a Regulatory Sandbox which welcomes local as well as international firms wishing to test new digital solutions in a 'live' environment with a view to deploy them in the KSA in the future.

SAMA developed the Cyber Resilience Fundamental Requirements (herein "Fundamental Requirements"), specifically intended for entities that are recently established and are in the early stages of their operations in the financial sector of the Kingdom of Saudi Arabia (herein "KSA").

1.1 Objective

Given the resource constraints these types of entities often face, the objective of the Fundamental Requirements is to help Entities in:

- **Managing** and **mitigating** a widened range of cyber security and resilience risks relevant to the KSA financial sector;
- **Focusing resources** on a fundamental set of controls aimed at an effective protection of information assets.

To achieve this objective, the fundamental requirements provides:

- a **prioritized** set of cyber security and resilience control requirements;
- a structure and a content that are **aligned** with other SAMA regulatory frameworks, such as the Cyber Security Framework (herein "CSF") and the Business Continuity Management Framework (herein "BCMF"), which will be applicable to organizations in the future.

1.2 Applicability

The framework "Fundamental Requirements" applies to entities intending to qualify for SAMA Regulatory Sandbox environment and/or entities seeking license to operate in the kingdom of Saudi Arabia. The "Fundamental Requirements" serves as a catalyst to enable entities to comply with minimum SAMA's cyber resilience licensing requirements. The "Fundamental Requirements" should not be treated as a replacement of SAMA's Cyber Security and Business Continuity Management regulatory frameworks where the entities are required to comply with other relevant SAMA regulatory requirements post licensing decision. Additionally, this framework should also be read in conjunction with the requirements mandated in SAMA's Regulatory Sandbox Framework.

1.3 Responsibilities

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

1 https://www.sama.gov.sa/en-US/Regulatory%20Sandbox/Documents/Regulatory_Sandbox_Framework_English_Nov4.pdf

Framework.

1.4 Compliance

In the event that an entity is not able to demonstrate compliance with the Fundamental Requirements, SAMA reserves the right to prohibit the sandboxing graduation/license request of the entity.

1.5 Interpretation

SAMA, as the owner of the Fundamental Requirements, is solely responsible for providing interpretations of the principles and control requirements, if required.

1.6 Target Audience

The Fundamental Requirements is intended for senior and executive management, business owners, owners of information assets, Heads of Cyber Security and those who are accountable for and involved in defining, implementing and reviewing cyber security and resilience controls within the Entities.

1.7 Review, Updates and Maintenance

SAMA will review the Fundamental Requirements periodically to evaluate its applicability to the context of the KSA financial sector and its intended Entities. If deemed necessary, SAMA will update the fundamental Requirements based on the outcome of the review.

SAMA will implement version control for maintaining the Fundamental Requirements. Whenever making any changes, SAMA will retire the preceding version, as well as release and communicate the new version to all Entities. For the convenience of the Entities, SAMA will clearly indicate any changes to the revised Fundamental Requirements.

1.8 Reading Guide

The Fundamental Requirements is structured as follows:

- **chapter 2** elaborates on the structure of the Fundamental Requirements and provides guidance on how to apply the Fundamental Requirements; and
- **chapter 3** presents the cyber security and resilience domains including control requirements.

2 Fundamental Requirements Structure and Features

2.1 Structure

The Fundamental Requirements is structured around four domains, including:

- Cyber Security Leadership and Governance;
- Cyber Security Operations and Technology; and
- Resilience.

Control requirements have been uniquely numbered throughout the Fundamental Requirements. The control requirements are numbered according to the following numbering system:

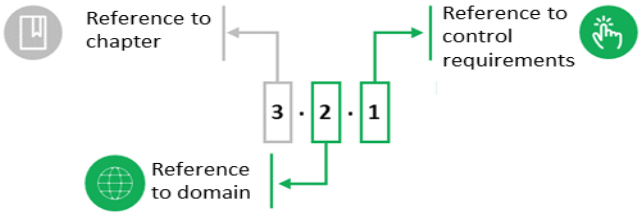

Figure 1. Control requirement numbering system

The figure below illustrates the overall structure of the Fundamental Requirements and indicates the cyber security and resilience domains:

Figure 3. Fundamental Requirements domains

2.2 Risk-Based Approach

The domains and control requirements included in the fundamental requirements are risk-based and intended to

provide participants with essential direction on how to mitigate the most common risks they face, without placing undue burden on them that could stifle innovation and business growth.

From this perspective, the fundamental requirements sets the essential cyber security and resilience mandatory requirements for entities that are within the scope of applicability. In addition, SAMA expects entities to conduct their own internal risk assessments to monitor the development of the cyber security and resilience threat landscape, to identify new and evolving risks, to evaluate the potential impact of these risks, and where deemed necessary to implement additional or enhanced security and resilience control requirements beyond the fundamental requirements to mitigate these risks in line with the entities risk appetite.

2.3 Entities Self-Assessment and SAMA Audit

The implementation of the fundamental requirements at the participants will be subject to periodic self-assessment. The self-assessment will be performed by the entities based on a questionnaire. The entities will send a copy of its self-assessment to SAMA, and SAMA reserves the right to review the self-assessment for demonstration of compliance with the fundamental requirements at its discretion. SAMA also reserves the right to audit the compliance with the fundamental requirements of the entities at any time.

3 Control Requirements

3.1 Cyber Security Leadership and Governance

Control ID	Control requirement description
3.1.1.	Entities should develop a robust Cyber Security Governance structure that is supported with appropriate resources to oversee and control overall approach to cyber security.
3.1.2.	Entities should define, approve, implement and communicate cyber security policies and procedures that is supported by detailed security standards (e.g. password standard, firewall standard).
3.1.3.	Entities should periodically review and update cyber security policies, procedures and standards taking into consideration the evolving cyber threat landscape.
3.1.4.	Entities should incorporate cyber security requirements in their new and/or existing business operating model, including at least: a. evaluation of cyber security and fraud risks that could target business operating model; and b. adoption and evaluation of cyber security measures for the protection against adversarial attacks (e.g. model stealing, malicious inputs, and poisoning attack).
3.1.5.	Entities should establish and implement strong password policy for users' access to its information assets, such as: a. change of password upon first logon, minimum password length and history and password complexity; b. revoking the access after the three successive incorrect passwords; and c. use non-caching techniques.
3.1.6.	Entities should execute comprehensive IT and cyber security risk assessments covering (infrastructure, network, applications, and systems) and the controls implemented to address the identified risks. The identified risks should be documented in a central register, and periodically monitored and reviewed.

Ref. to other SAMA Framework(s)
Cyber Security Framework
- 3.1.1 Cyber Security Governance - 3.1.3 Cyber Security Policy - 3.2.1 Cyber Security Risk Management

3.2 Cyber Security Operations and Technology

Control ID	Control requirement description
3.2.1.	Entities should establish identity and access management process to govern the logical accesses to the information assets according to need-to-have and need-to-know principles.
3.2.2.	Entities should establish change management process to ensure that changes to the entities information assets are classified, tested and approved before their deployment into production environments. The change management process should also include cyber security requirements for controlling changes to information assets.
3.2.3.	Entities should establish and maintain a secure network architecture that address taking into consideration the following: a. segmentation of networks, according to the functionality of services and the adoption

	of network security systems (e.g. firewalls) to control the network traffic between segments; and b. availability.
3.2.4.	Entities should adopt secure and robust cryptography algorithms and ensure that the application and server communications are encrypted using secure protocols.
3.2.5.	Entities should periodically conduct comprehensive vulnerability assessment (VA) covering both the application and infrastructure layers of the Entities technology landscape.
3.2.6.	Entities should conduct penetration testing (PT) twice a year as a minimum or after major/ critical change to comprehensively evaluate its cyber security defense capability.
3.2.7.	Entities should ensure up-to-date and relevant patches are tested, applied and installed in a timely manner to avoid security breaches due to existing vulnerabilities in the applications and infrastructure.
3.2.8.	In addition to secure System Development Life Cycle (herein "Secure SDLC") process entities should implement shielding techniques (such as but not limited to code obfuscation, white box cryptography and anti-tampering) in the application design.
3.2.9.	Entities should implement effective brand protection controls to detect and defend against targeted attacks by continuously monitoring the online services such as apps, social media accounts and websites and proactively takedown malicious activities.
3.2.10.	Entities should ensure that endpoints (both personal, if allowed, and corporate) are secured through implementation of a minimum set of cyber security requirements such as the following, but not limited to: a. the real time protection for the endpoints (e.g. antivirus and antimalware); b. implementation of behavioural-based and/or signature-based solutions; c. ensuring anti-malware signatures are up-to-date and the systems are regularly scanned for malicious files or anomalous activities; and d. in case of mobile devices: i. separation and encryption of entities data; and ii. secure wiping of stored entities data in cases of device loss, theft or decommissioning in alignment with the Secure Information Asset Disposal process.
3.2.11.	Entities should establish and implement a process to collect, process, review and retain security logs to facilitate continuous security monitoring. These logs should provide sufficient details and should be retained securely for a period of one year as a minimum.
3.2.12.	Entities should ensure applications and infrastructure components are integrated with a security information and event management (SIEM) solution.
3.2.13.	Entities should ensure continuous security monitoring and analysis of cyber security events to promptly detect and respond to cyber security incidents.
3.2.14.	Entities should develop Cyber Security Incident Management process to timely identify, respond and contain cyber security incidents impacting the Entities information assets.
3.2.15.	Entities should implement session timeout configurations with reasonable timeframe; in-active sessions should not exceed 5 minutes for applications and underlying infrastructure.
3.2.16.	Entities should immediately inform SAMA (F.S.Cybersecurity@SAMA.GOV.SA) in case any of the following incidents classified as medium or above has occurred and identified for: a. Cyber security; b. Fraud; c. All disruptive incidents.

Ref. to other SAMA Framework(s)

Cyber Security Framework		
- 3.3.5 Identity and Access Management - 3.3.6 Application Security - 3.3.7 Change Management	- 3.3.8 Infrastructure Security - 3.3.9 Cryptography - 3.3.13 Electronic Banking Services	- 3.3.14 Cyber Security Event Management - 3.315 Cyber Security Incident Management - 3.3.17 Vulnerability Management

3.3 Resilience

Control ID	Control requirement description
3.3.1.	The Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) should be defined, approved, communicated, implemented and periodically reviewed to enable the entities to continue delivering its critical services, at an acceptable pre-defined level.
3.3.2.	Entities should define and implement its backup and restoration requirements considering the following, but not limited to: a. legal and regulatory requirements; b. Critical and customer data; c. business requirements; d. schedule of the backup (daily, weekly, monthly, etc.); e. protection of confidential data stored in back up media through applying encryption techniques; f. storage of backup media offline or at an offsite location; and g. secure destruction of backup data. h. restoration tests.

Ref. to other SAMA Framework(s)
Business Continuity Management Framework
- 2.5 Business Continuity Plan - 2.6 Disaster Recovery Plan - 2.7 Cyber Resilience

4 Appendices

Appendix A: 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.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Availability	Ensuring timely and reliable access to and use of information. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Back-up	Files, devices, data and procedures available for use in case of a failure or loss, or in case of deletion or suspension of their original copies.
Business Continuity (BC)	The capability of an organization to continue delivery of IT and business services at acceptable predefined levels following a disruptive incident. *Source: ISO 22301:2012 Societal security -- Business continuity management systems*
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a Fundamental Requirements for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. *Source: ISO 22301:2012 - Business continuity management systems — Requirements*
Change management	The controlled identification and implementation of required changes within a business or information systems.
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. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Cyber risk	Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system *Source: NISTIR 7298r3 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 Entities information assets against internal and external threats.
Cyber Security event	Any observable occurrence in an information system or network that has, or may potentially result in, unauthorized access, processing, corruption, modification, transfer or disclosure of data and / or Information or (b) a violation of an explicit or implemented Organization security policy.

Term	Description
Cyber security governance	A set of responsibilities and practices exercised by the Board of Directors 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 (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Cyber security incident management	The monitoring and detection of security events on an information system and the execution of proper responses to those events.
Cyber security policy	A set of rules that governs all aspects of security-relevant system and system element behaviour. Note 1: System elements include technology, machine, and human, elements. Note 2: Rules can be stated at very high levels (e.g., an organizational policy defines acceptable behaviour of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behaviour of executing processes and use of resources by those processes) *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Cyber security risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Cyber security risk management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of 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 *Source: NISTIR 7298r3 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 (including mission, functions, image, or reputation), 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. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Disaster Recovery (DR)	Programs, activities and plans designed to restore the organizations critical business functions and services to an acceptable situation, following exposure to cyber and IT incidents or disruption of such services.

Term	Description
Head of Cyber Security	The Head of Cyber Security may refer to the Head of Information Security, the Chief Information Security Officer (CISO) or any other title given to the senior manager accountable for the cyber security function and processes.
Fall-back	Business procedures and measures, undertaken when events have triggered the execution of either a business continuity plan or a contingency plan.
Formally documented	Documentation that is written, approved by the senior leadership and disseminated to relevant parties.
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
Disaster Recovery Plan	Disaster Recovery is part of BCM which includes policies, standards, procedures and processes pertaining to resilience, recovery or continuation of technology infrastructure supporting critical business processes.
Major change	Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations. *Source: NISTIR 7298r2 Glossary of Key Information Security Terms* Critical changes are also included in the concept of major changes.
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Penetration testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Periodically	With this term, SAMA does not intend to define a default time interval. Each Entities has the responsibility to determine this interval based on its own risk-based approach. The same term adopted in different control requirements could be translated into different time intervals by the MO.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen or lost.
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. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*

Term	Description
Risk register	Risk register is a table used as a repository for all risks identified and includes additional information about each risk, e.g. risk category, risk owner, and mitigation actions taken.
Shielding technique	Shielding," a process that obfuscates an application's binary code, ostensibly making it harder for hackers to reverse-engineer
Strategy	Refer to “Cyber security strategy”.
SIEM	A security information and event management (SIEM) tool is Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
System Development Lifecycle (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. *Source: NISTIR 7298r3 Glossary of Key Information Security Terms*
Threat	Refer to “Cyber security threat”.
Threat landscape	A collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends. *Source: ENISA*
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source *Source: NISTIR 7298r3 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”.