الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

National Framework for Cybersecurity Risk Management

(NFCRM – 1:2025)

TLP: Clear

Document Classification: Public

Disclaimer: Please refer to the National Cybersecurity Authority's website (https://nca.gov.sa), to obtain the latest version of this document

In the Name of Allah,

The Most Gracious,

The Most Merciful

Disclaimer: This Framework shall be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia. The courts of the Kingdom of Saudi Arabia shall have exclusive jurisdiction over any disputes arising out of or in connection with this document. In the event of any ambiguity, conflict, or discrepancy between language versions, the Arabic version shall prevail and shall be deemed the sole authoritative text for purposes of interpretation and enforcement.

Traffic Light Protocol (TLP):

This protocol is widely used around the world and comprises four colors (light signals):

Red (Personal and Confidential- for the Intended Recipient Only)

The recipient is not authorized to share the red-classified material with any individual, whether inside or outside the entity; sharing is strictly prohibited beyond the defined scope of receipt.

Amber+ Strict (Internal Sharing within the Same Entity)

The recipient may share the information only with the intended recipients inside the entity.

Amber (Restricted Sharing)

The recipient may share the information only with the intended recipients inside the entity or with recipients who are required to take action related to the shared information.

Green (Sharing within the Same Community)

The recipient may share the information with others within the same entity or with entities that have a relevant relationship or operate within the same sector; however, it is not permitted to disseminate or publish the information via public channels.

Clear (No Restrictions)

Table of Contents

List of Figures and illustrations

List of Tables

1. Introduction

Pursuant to its statute issued by Royal Order No. (6801), dated 11/02/1439H (31/10/2017), the National Cybersecurity Authority (NCA) is the competent authority nationally in charge of cybersecurity in the Kingdom, and the national reference in its affairs. The NCA aims to improve the cybersecurity posture of the Kingdom in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities. The NCA powers and duties include, but not limited to, the development of cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines; their dissemination to the relevant entities; the monitoring of compliance therewith; and the continual updating thereof. The NCA is also responsible for establishing and updating cybersecurity risk management frameworks and monitoring compliance therewith.

Accordingly, the NCA has developed this Framework, which serves as a reference and methodology for managing cybersecurity risks in the Kingdom under the supervision of the NCA. This Framework provides a clear vision for managing cybersecurity risks both at the entity level and at the national level. It outlines, as a primary focus, the methodology for managing cybersecurity risks, as well as the related roles, responsibilities, and procedures that enhance cybersecurity risk management capabilities within the Kingdom.

2. Definitions

The terms used in this Framework shall have the same meanings assigned to them in the table below, unless the context requires otherwise:

Term	Definition
NCA	National Cybersecurity Authority (NCA).
Framework	The National Framework for Cybersecurity Risk Management, issued by NCA.
Critical National Infrastructure (CNI)	The essential elements of infrastructure (i.e. assets, facilities, systems, networks, processes, and key personnel who operate and manage them) whose loss or compromise may result in: ● A significant adverse impact on the availability, integration, or delivery of basic services, including services whose compromise may lead to major property damage, loss of life, and/or injury, taking into account national-level economic and/or social impact. ● A significant impact on national security, national defense, and/or the Kingdom's economy or sovereign capabilities.
Cybersecurity	The protection of networks, information technology systems, and operational technology systems, including hardware and software, services provided thereby, and data included therein, against hacking, disruption, modification, unauthorized access, and unlawful exploitation or use. Cybersecurity includes information security, electronic security, digital security, and the like.
Cybersecurity Risks	Risks that may impact the entity's operations (including its vision, mission, functions, image, reputation, or processes), or its assets, individuals, other entities, or the State, arising from the potential of hacking, disruption, modification, unauthorized access, and unlawful exploitation or use or disclosure, or unlawful destruction of networks, information technology systems, and operational technologies systems, including hardware and software, services provided thereby, and the data included therein.
Cybersecurity Vulnerabilities	Weaknesses—whether in assets, controls, or procedures—that may expose the entity to cybersecurity risks.

Term	Definition
Cybersecurity Threats	Any circumstance or event that is likely to adversely impact the entity's operations (including its vision, mission, departments, image, reputation, or processes), its assets, individuals, other entities, or the State through exploiting cybersecurity vulnerabilities.
Cybersecurity Risk Scenarios	Detailed scenarios representing events or sequences of events that may lead to the exposure of the entity's assets to cybersecurity threats or cause such assets to be affected thereby.
Controls	Protective measures against cybersecurity threats, aligned with the Cybersecurity Controls issued by the NCA.
Cybersecurity Inherent Risks	The cybersecurity risks based on the cybersecurity risk scenario identified prior to the implementation of risk treatment plans and any controls included therein.
Cybersecurity Residual Risks	The cybersecurity risks that remain after considering risk treatment plans and any associated controls.
Assets	Tangible or intangible resources. Assets include various types such as data and information, technical infrastructure, software, applications, systems, technical devices, networks, databases, services, social media accounts, and others.
Internet-Facing Assets	Assets that have assigned Internet Protocol (IP) addresses and are generally accessible and routable over the public internet.
Likelihood	The Likelihood that a cybersecurity threat may materialize within a specified timeframe. This may be expressed quantitatively or qualitatively.
Impact	The consequences or outcomes resulting from the realization of a cybersecurity threat. This may be expressed quantitatively or qualitatively.
Acceptable Risk Level	The risk level that can be accepted by an authorized official.
Haseen	A comprehensive national cybersecurity ecosystem, through which the NCA provides centralized and non-centralized cybersecurity services and products to beneficiaries at the national level (government entities, CNIs, and private entities) in accordance with the NCA's mandate and its national cyber regulatory requirements.

TABLE 1: LIST OF DEFINITIONS

3. Framework Objectives

This Framework aims to effectively manage cybersecurity risk, as it forms the cornerstone of a unified, integrated, comprehensive, and interoperable ecosystem capable of identifying, assessing, treating, and following up with cybersecurity risks. The following factors contribute to the achievement of this objective:

- Identifying priority cybersecurity risks to treat.
- Enhancing national cybersecurity resilience through the implementation of necessary controls to reduce cybersecurity risks.
- Defining roles and responsibilities for cybersecurity risk management.
- Promoting a culture of cybersecurity risk management within entities.
- Managing cybersecurity risks effectively in a manner that enables entities to carry out their functions and fulfill their roles and responsibilities across various fields and sectors.

4. Framework Scope of Application

This Framework applies to government agencies in the Kingdom of Saudi Arabia (including ministries, authorities, institutions and others) and their affiliated companies and entities inside and outside the Kingdom, as well as all private sector entities that own, operate, or host Critical National Infrastructures (CNIs) (Hereinafter referred to collectively as the "entity"). The NCA strongly encourages all other entities in the Kingdom to leverage this Framework and apply best practices for cybersecurity risk management and to enhance and strengthen cybersecurity at the national level.

5. Responsibilities in Cybersecurity Risk Management at the National Level

Each entity falling within the scope of this Framework shall comply with the following:

5.1 Appoint a liaison officer responsible for cybersecurity risk management to coordinate with the NCA for the implementation of this Framework, its current and future requirements, and obligations.

5.2 Identify and classify the entity's assets, such as critical systems, facilities and operational technologies, social media accounts, and others, in accordance with what is issued by the NCA, and then review the classification periodically.

5.3 Identify Internet-facing assets of the entity.

5.4 Submit to the NCA a periodic report of the assets identified in paragraphs 5.2 and 5.3 in accordance with the specified period, and update them upon any change via Haseen or any other channel specified by the NCA.

5.5 Report to the NCA any cybersecurity risks at the entity classified as critical (Level 5) or high (Level 4) immediately upon identification, in accordance with the Cybersecurity Risk Assessment Matrix (Figure 2), and submit the entity's cybersecurity risk treatment plans periodically, upon updates, or in the event of any change, via Haseen or any other channel specified by the NCA.

5.6 Mitigate any cybersecurity risks, vulnerabilities, or observations issued by the NCA, provide a status update on the actions taken, and report the measures implemented periodically in accordance with the specified time period, including updates upon any changes, via Haseen or any other channel specified by the NCA.

6. Responsibilities for Cybersecurity Risk Management at the Entity Level

Each entity falling within the scope of this Framework shall comply with the Cybersecurity Risk Management Methodology and the Cybersecurity Risk Assessment Matrix as set forth in this section of the Framework.

Cybersecurity Risk Management Methodology

The Cybersecurity Risk Management Methodology is designed to identify inherent cybersecurity risks, evaluate their impact and likelihood, and determine appropriate risk treatment plans based on which risk treatment decisions are made. Within this methodology,

assets, cybersecurity vulnerabilities, cybersecurity threats, and controls are used as potential inputs to understand cybersecurity risks.

The phases illustrated in Figure (1) below constitute the primary phases of the Cybersecurity Risk Management Methodology. Each phase includes a set of tasks aimed at enhancing visibility, understanding, and execution within the context of cybersecurity risk management.

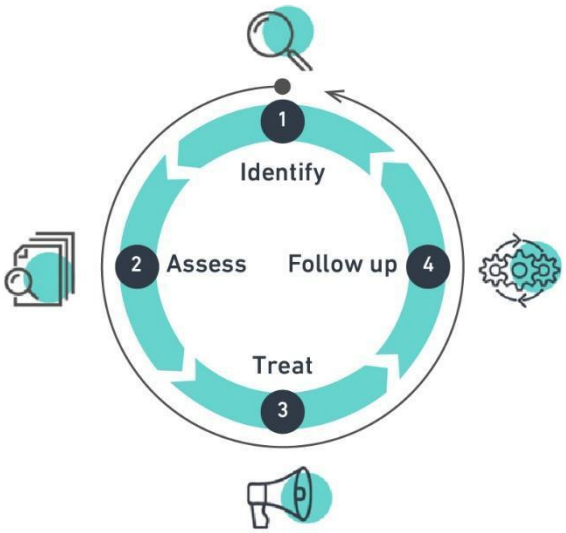

FIGURE 1: KEY PHASES OF CYBERSECURITY RISK MANAGEMENT METHODOLOGY

To ensure the sustainable application of this Methodology, the following actions shall be undertaken:

6.1 Develop and operate a continuous program for implementing the Cybersecurity Risk Management Methodology, with the allocation of the necessary resources.

6.2 Engage relevant stakeholders at various phases, including the cybersecurity steering committee and the information technology department.

Identification Phase

In this phase, the entity's assets are identified and classified. Expected cybersecurity risk scenarios are developed based on potential cybersecurity threats and identified vulnerabilities, with the objective of determining inherent cybersecurity risks. This phase consists of the following steps:

6.3 Identify and classify the entity's assets.

6.4 Identify cybersecurity vulnerabilities.

6.5 Identify potential cybersecurity threats.

6.6 Develop expected cybersecurity risk scenarios based on potential cybersecurity threats and identified vulnerabilities.

6.7 Identify currently implemented controls to address the expected cybersecurity risk scenarios.

6.8 Determine the entity's acceptable level of cybersecurity risk.

Assessment Phase

In this phase, cybersecurity risks are assessed based on the expected cybersecurity risk scenarios by evaluating both likelihood and impact. This phase consists of the following steps:

6.9 Conduct an analysis of inherent cybersecurity risks for all expected cybersecurity risk scenarios and the currently implemented controls, and assess the likelihood and impact in accordance with the Cybersecurity Risk Assessment Matrix illustrated in Figure (2).

6.10 Document the results of analysis and assessment in the cybersecurity risk register.

Treatment Phase

In this phase, a decision is made on how to treat cybersecurity risks—whether by accepting, sharing, mitigating, or avoiding such risks—and corresponding risk treatment plans are then defined and implemented. This phase consists of the following steps:

6.11 Identify and develop cybersecurity risk treatment plans.

6.12 Assess the expected residual cybersecurity risks following the implementation of the risk treatment plans to ensure that an acceptable level of risk is reached.

6.13 Make a decision on the treatment approach for cybersecurity risks and determine the corresponding risk treatment plans.

6.14 Develop risk treatment plans based on priority.

6.15 Implement the risk treatment plans.

6.16 Update the cybersecurity risk register to include treatment plans and residual cybersecurity risks.

Follow-up Phase

In this phase, the cybersecurity risk management activities of the entity are followed up, monitored, and assessed through the Cybersecurity Risk Management Methodology, in order to update the cybersecurity risk register periodically or upon any change in assets, cybersecurity threats, or the controls implemented. This phase consists of the following steps:

6.17 Develop cybersecurity risk management reports.

6.18 Establish criteria for collecting statistical data related to cybersecurity risk monitoring.

6.19 Monitor the implementation of cybersecurity risk treatment plans on a periodic basis and issue related reports and data.

6.20 Execute the phases of the Cybersecurity Risk Management Methodology periodically, or as instructed by the NCA, or upon any update in any of the following:

- Cybersecurity risk treatment plans.
- Potential cybersecurity threats.
- Expected cybersecurity risk scenarios.
- The status of controls implementation.
- Changes in the digital infrastructure.

Cybersecurity Risk Assessment Matrix

The Cybersecurity Risk Assessment Matrix provides a methodology for determining cybersecurity risk levels. The matrix takes into account the likelihood of occurrence of cybersecurity risk scenarios and the potential impact resulting therefrom. Figure (2) illustrates the Cybersecurity Risk Assessment Matrix.

Risk Level = Impact x Likelihood

Likelihood						
5	Almost Certain	Low	Medium	High	Critical	Critical
4	Probable	Low	Medium	Medium	High	Critical
3	Improbable	Low	Low	Medium	Medium	High
2	Rare	Very Low	Low	Low	Medium	Medium
1	Very Rare	Very Low	Very Low	Low	Low	Low
		Very Low	Low	Medium	High	Critical
		1	2	3	4	5
		Impact				

FIGURE 2: CYBERSECURITY RISK ASSESSMENT MATRIX

Figure (3) below presents a description of the cybersecurity risk levels, where the risk is classified using the following formula: (Impact × likelihood), based on the Cybersecurity Risk Assessment Matrix.

Risk Level

Very Low	Low	Medium	High	Critical
1-2	3-7	8-14	15-19	20-25

FIGURE 3: CYBERSECURITY RISK LEVELS

Description of Impact Levels

Figure (4) below provides a description of the impact levels, where the level of impact is classified in the event of a breach of one or more of the cybersecurity elements: confidentiality, integrity, or availability.

	(1) Very Low	(2) Low	(3) Medium	(4) High	(5) Critical
Confidentiality	Disclosure or leakage of non-sensitive data or information, with no impact on the entity.	Disclosure or leakage of sensitive data or information, with a minor impact on the entity.	Disclosure or leakage of sensitive data or information, with a tangible impact on the entity.	Disclosure or leakage of sensitive data or information, with a significant impact on the entity.	Disclosure or leakage of sensitive data or information, resulting in a significant impact on the entity that is intolerable, or having an impact at the national level.
Integrity	A change to the entity's assets that has no impact on the entity.	A change to the entity's assets that has a minor impact on the entity.	A change to the entity's assets that has a tangible impact on the entity.	A change to the entity's assets that has a significant impact on the entity.	A change to the entity's assets, resulting in a significant impact on the entity that is intolerable, or having an impact at the national level.
Availability	Disruption of the entity's assets with no impact on the entity.	Disruption of the entity's assets, resulting in a minor impact on the entity.	Disruption of the entity's assets, resulting in a tangible impact on the entity.	Disruption of the entity's assets, resulting in a significant impact on the entity.	Disruption of the entity's assets, resulting in a significant impact on the entity that is intolerable, or having an impact at the national level.

FIGURE 4: DESCRIPTION OF IMPACT LEVELS

Description of Likelihood Levels

Figure (5) below provides a description of the likelihood levels, where each level is classified based on the time frame or the ease of exploitation:

Assessment	Value	Likelihood	
		Time Frame	Exploitability
Almost Certain	5	Expected to recur in most cases, possibly multiple times per month or several times per year.	**Or** a cybersecurity vulnerability can be exploited by an unskilled attacker (e.g., script-kiddie), using readily available exploit code.
Probable	4	Commonly occurs in most cases with a frequency of once per year.	**Or** the cybersecurity vulnerability can be exploited by an advanced attacker through a sophisticated attack using custom tools or methods.
Improbable	3	May occur at some point, approximately once every 2 to 3 years.	**Or** the cybersecurity vulnerability is exploitable by an advanced attacker, but only under specific conditions (e.g., precisely crafted exploit or deep knowledge of the internal network).
Rare	2	May occur approximately once every 3 to 10 years.	**Or** the cybersecurity vulnerability is not directly exploitable, but may be exploitable in the future.
Very Rare	1	Occurs only under exceptional circumstances, estimated at less than once every 10 to 20 years.	**Or** the cybersecurity vulnerability is not currently considered exploitable.

FIGURE 5: DESCRIPTION OF LIKELIHOOD LEVELS

7. Obligations and Provisions

General Obligations

All entities falling within the scope of application of this Framework shall comply with the National Cybersecurity Risk Management Framework issued by the NCA. Entities shall also comply with all relevant regulatory requirements issued by the NCA, including policies, frameworks, controls, guidelines, and standards.

General Provisions

The NCA may review and update this Framework in accordance with cybersecurity risk management requirements. Accordingly, all entities must adhere to any updates as approved and issued by the NCA.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority