Hay'adda Isgaarsiinta Qaranka
الـهيئـة الوطنيـة للإتـصالات
National Communications Authority

NATIONAL CYBERSECURITY RISK MANAGEMENT FRAMEWORK

JUNE 2026

H.E. Mr. Mohamed Adam Moalim (Soomaali)

Minister,

Ministry of Communication and Technology (MoCT)

Federal Republic of Somalia

FOREWORD BY THE MINISTER

The rapid expansion of Somalia's digital ecosystem has made cybersecurity and cyber risk management critical national priorities. As digital technologies continue to advance across government institutions, critical infrastructure, telecommunications, financial services, and public service delivery, opportunities for economic growth and innovation continue to grow. At the same time, these developments increase exposure to cyber threats, operational disruptions, and risks to national security and public trust.

The Federal Government of Somalia recognizes cybersecurity as a strategic pillar for protecting critical information infrastructure, safeguarding national interests, and strengthening national resilience. In this regard, I reaffirm the commitment of the Ministry of Communications and Technology (MoCT) to advancing national cybersecurity governance through strategic policy leadership.

This National Cybersecurity Risk Management Framework establishes a coordinated national approach to identifying, assessing, managing, and mitigating cyber risks in alignment with national priorities and international best practices. The framework establishes baseline cybersecurity requirements, governance principles, and risk management controls aimed at strengthening resilience, protecting critical infrastructure, and ensuring the continuity of essential digital services.

Cybersecurity is a shared national responsibility that requires strong leadership, collaboration, and sustained commitment from all stakeholders. I believe this framework will strengthen national cybersecurity preparedness, reinforce national security, enhance trust in the digital ecosystem, and contribute to a secure and resilient digital future for Somalia.

Mr. Mustafa

Yasin Sheikh

Director General

National Communications Authority

FOREWORD BY DIRECTOR GENERAL

As the Federal Republic of Somalia continues to advance its digital transformation across government institutions, critical infrastructure, businesses, and public services, cybersecurity risk management has become a national priority. The increasing reliance on digital technologies and interconnected systems continues to create opportunities for innovation and economic growth, while also exposing institutions to evolving cyber threats and operational risks. Strengthening cyber resilience is therefore essential to protecting national digital assets, safeguarding critical infrastructure, ensuring service continuity, and enhancing national security and public trust in the digital ecosystem.

The National Communications Authority (NCA), as the leading institution for cybersecurity in Somalia, remains committed to strengthening national cyber resilience through effective governance, regulatory oversight, and risk-based cybersecurity practices based on the policy direction of the Ministry of Communications and Technology (MoCT).

The National Cybersecurity Risk Management Framework provides organizations with a practical and structured approach to identifying, assessing, managing, and mitigating cyber risks in alignment with international standards and Somalia's operational environment. The framework establishes cybersecurity requirements, governance principles, and control measures to strengthen institutional resilience, improve cyber preparedness, and support informed risk-based decision-making. It also promotes collaboration, accountability, continuous improvement, and shared responsibility among government institutions, service providers, academia, and the private sector.

The NCA is confident that the implementation of this framework will enhance regulatory oversight, strengthen institutional resilience, improve national cyber preparedness, and contribute to a secure, resilient, and trusted digital future for Somalia.

Table Of Contents

List Of Tables

List of Figures

1 Risk Assessment Overview

1.1 Introduction

This Framework presents the official Federal Government of Somalia approach for understanding the nature and estimating the level of security risks affecting Critical Information Infrastructure (CII). All public and private sector organizations that own and/or operate CII must use this Framework to identify, quantify or qualitatively describe and prioritize risks against risk evaluation criteria and objectives relevant to them.

1.2 Aims of the Framework

This Framework guides the cybersecurity risk management process. It presents a systematic approach for identifying and evaluating the risks of deliberate and accidental disclosure, interception and modification of information held, stored and processed by a CII. The framework aims to help public and private sector organizations to:

- Understand risk and its potential impact upon business objectives;
- Offer Boards and other decision-makers information about the main security risks affecting vital business assets;
- Understand risks better and assist in the selection of treatment options;
- Identify major causes of risks and weak links in systems and organizations;
- Compare risks in alternative systems, technologies or approaches;
- Communicate risks and uncertainties;
- Establish priorities;
- Improve incident prevention based upon post-incident investigation;
- Select different forms of risk treatment;
- Meet mandated regulatory obligations;
- Obtain information to help assist in evaluating whether a security risk should be accepted when compared with pre-defined criteria; and
- Assess risks for end-of-life disposal.

1.3 Applicability of the Framework

All public and private sector organizations that own and/or operate CII shall implement this Framework to guide their technical risk assessment and treatment activities. It addresses risks to the confidentiality, integrity and availability of information that CII hold, store and process. The Somalia Cybersecurity Act requires that CII operators must conduct regular and systematic cybersecurity risk assessments.

1.4 Authority

The duties and responsibilities of the National Communications Authority, established under Article 5 of the National Communications Act, 2017, were expanded by the Somalia Cybersecurity Act, and the governance and management of the country's cybersecurity is placed under the National Communications Authority. Based on this, all-designated Critical Infrastructure Operators shall implement this framework and submit annual risk assessment report to the Authority.

2 Risk Management Concepts

This Framework adopts ISO/IEC terms and definitions for concepts that appear throughout this framework. The framework cites the appropriate ISO/IEC standards from which it derives the definitions.

2.1 Accountability

This framework adopts the ISO/IEC 27000 definition of accountability as the property that enables the unambiguous tying of an action to an entity such as a user, process, system and information asset.

2.2 Asset

In accordance with ISO/IEC 27005, an asset is anything that has value to an organization and which, therefore requires protection.

2.3 Authenticity

This framework adopts the ISO/IEC 27000 definition of authenticity as the property that ensures that the identity of a subject or resource (i.e. entities such as users, processes, systems and information) is the one claimed.

2.4 Availability

In accordance with ISO/IEC 27000, availability is the property of being accessible and usable upon demand by an authorized entity.

2.5 Baseline Controls

Baseline controls refer to the minimum set of security controls or safeguards established for a system or organization to achieve an acceptable level of security. This Standard uses the term “baseline controls” interchangeably with “minimum security requirements.”

2.6 Confidentiality

In accordance with ISO/IEC 27000, Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

2.7 Critical Information Infrastructure

The Somalia Cybersecurity Act (2026) defines Critical Information Infrastructure (CII) as tangible and intangible digital assets, networks and information systems determined by the National Communications Authority to be essential to national security, economic welfare, public safety, or the public interest.

2.8 Integrity

In accordance with ISO/IEC 27000, Integrity is the property of safeguarding the accuracy and completeness of information and information assets.

2.9 Internal Context

In accordance with ISO/IEC 27000 and ISO/IEC 27005, internal context refers to the internal environment in which an organization seeks to achieve its objectives. The internal context can influence information security risk management activities and includes:

- Governance, organizational structure, roles, and accountabilities.
- Policies, objectives, and strategies established to achieve organizational goals.
- Capabilities in terms of resources and knowledge, including capital, time, people, processes, systems, and technologies.
- nformation systems, information flows, and decision-making processes, both formal and informal.
- Relationships with, and perceptions and values of, internal stakeholders. Organizational culture.

- Standards, guidelines, and models adopted by the organization.
- The form and extent of contractual relationships.

2.0 Level of Risk

In accordance with ISO Guide 73:2009, the level of risk describes the magnitude of risk as expressed in terms of the combination of impacts and their likelihood.

2.11 Likelihood

In accordance with ISO Guide 31073:2009, likelihood describes the chance of something happening. Similarly, ISO/IEC 27005 states that in risk management terminology, the word "likelihood" refers "to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period)." This Standard uses the term "likelihood" as a synonym of "probability".

2.2 Residual Risk

In accordance with ISO Guide 31073:2009, residual risk refers to the risk remaining after risk treatment. Residual risk may include unidentified risks; therefore, risk assessment should be a continuous process.

2.3 Risk

In accordance with ISO/IEC 27005, risk is the effect of uncertainty on objectives and is commonly expressed as a combination of the consequences of an event and the associated likelihood of occurrence.

The Somalia Cybersecurity Act based on principles requires operators to address information risk in the same way as other risks such as legal, financial, operational, compliance, reputational, health and safety. The operator's articulated information Risk Appetite forms the basis for the handling of information risk at project, product and process levels.

2.14 Risk Analysis

In line with ISO Guide 31073:2022, this framework regards risk analysis as a process aimed at understanding the nature and level of risk. ISO/IEC 27005 notes that risk analysis provides the basis for risk evaluation and decisions about risk treatment. Furthermore, risk analysis includes risk estimation.

2.15 Risk Appetite

A statement of information security risk appetite defines the level and type of information security risk that an organization is willing to accept, tolerate, or retain in pursuit of its strategic goals.

2.16 Risk Assessment

In accordance with ISO Guide 31073:2022, the risk assessment process comprising of risk identification, analysis and evaluation activities.

2.17 Risk Communication and Consultation

In accordance with ISO Guide 31073:2022, risk communication and consultation are iterative processes that help organizations provide, share or obtain information, and engage stakeholders on risk management activities. ISO/IEC 27005 notes that the information exchanged can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.

2.18 Risk Criteria

In accordance with ISO Guide 31073:2022, this framework regards risk criteria as the basis for evaluating risk. The ISO/IEC 27005 international standard notes that organizations can base risk criteria on their goals, external and internal context. Aspects of the external context might include standards and legislation.

2.19 Risk Identification

In accordance with ISO Guide 31073:2022, this framework regards risk identification as the process of finding, recognizing and describing risks. ISO/IEC 27005 notes that the process involves the identification of risk sources, events, their causes and their potential consequences. The risk identification approaches can encompass the use of historical data, theoretical analysis, informed and expert opinions, and the elicitation of stakeholder needs.

2.20 Risk Evaluation

In accordance with ISO Guide 31073:2022, this framework regards risk evaluation as the process for comparing the result of risk analysis with the agreed risk criteria to determine the acceptability of the risk and/or its magnitude.

2.21 Risk Management

In accordance with ISO Guide 31073:2022, risk management refers to coordinated activities to direct and control an organization regarding the risk.

2.22 Risk Treatment

The Somalia Cybersecurity Act requires owners and/or operators of CII to adopt a formal, consistent and policy-guide approach to risk management activities including treatment. In accordance with ISO Guide 31073:2022, this framework regards risk treatment as about modifying risk. ISO/IEC 27005 notes that risk treatment can involve:

- Avoidance i.e. deciding not to start or continue with the activity that gives rise to the risk.
- Taking or increasing risk to pursue an opportunity.
- Removing the risk source.
- Changing the likelihood.
- Changing the consequences.
- Sharing the risk with another party or parties including through contracts and insurance; and
- Retaining the risk by informed choice.

2.23 Security Domain

In this Framework, a Security Domain (SD) refers to a group of assets that are subject to common risk identification, assessment, and treatment activities. Security domains may include groups of IT assets supporting an end-to-end business service, such as remote access services. A security domain may also refer to network segments, environments, services, or organizational units governed by a common security policy. Security domains help standardize approaches to risk identification, assessment, and treatment.

2.24 Threat

In accordance with ISO/IEC 27000, a threat is a potential cause of an unwanted incident that may result in harm to a system or organization. This Standard adopts examples of typical threats identified in Annex A of ISO/IEC 27005.

2.25 Threat Actor

A threat actor is an individual, group, organization, or entity that exploits vulnerabilities or conducts malicious activities against systems, networks, or organizations, either independently or on behalf of another entity.

2.26 Threat Source

A threat source is any intent and method targeted at the intentional exploitation of a vulnerability or any situation and method that may accidentally trigger a vulnerability. Threat sources may include individuals, groups, organizations, natural events, or technical failures.

2.27 Vulnerability

In accordance with ISO/IEC 27000, a vulnerability is a weakness of an asset, control, or system that can be exploited by one or more threats.

3 Scoping Risk Assessments

As outlined in the introduction, risk assessment comprises three core activities: risk identification, risk analysis, and risk evaluation. Risk identification seeks to determine what events could occur, how and why they could occur, and where they may originate in ways that could result in potential loss or harm. Risk analysis aims to understand the nature of risk and determine its level by assessing the likelihood and potential impact of identified risks. Risk evaluation uses established risk criteria to determine the significance, acceptability, and priority of risks.

3.1 Risk Assessment Perspectives

A risk assessment is most effective when conducted within a clearly defined scope and boundary. Organizations may define the scope of a risk assessment in different ways depending on the purpose and context of the assessment. For example, the assessment may cover the entire organization, a specific department, a business process, an ICT system, system components, or individual services. To promote consistency and comprehensive risk management, organizations implementing this Standard shall consider risk assessment from at least three perspectives: external, internal, and project perspectives, as illustrated in the Figure below.

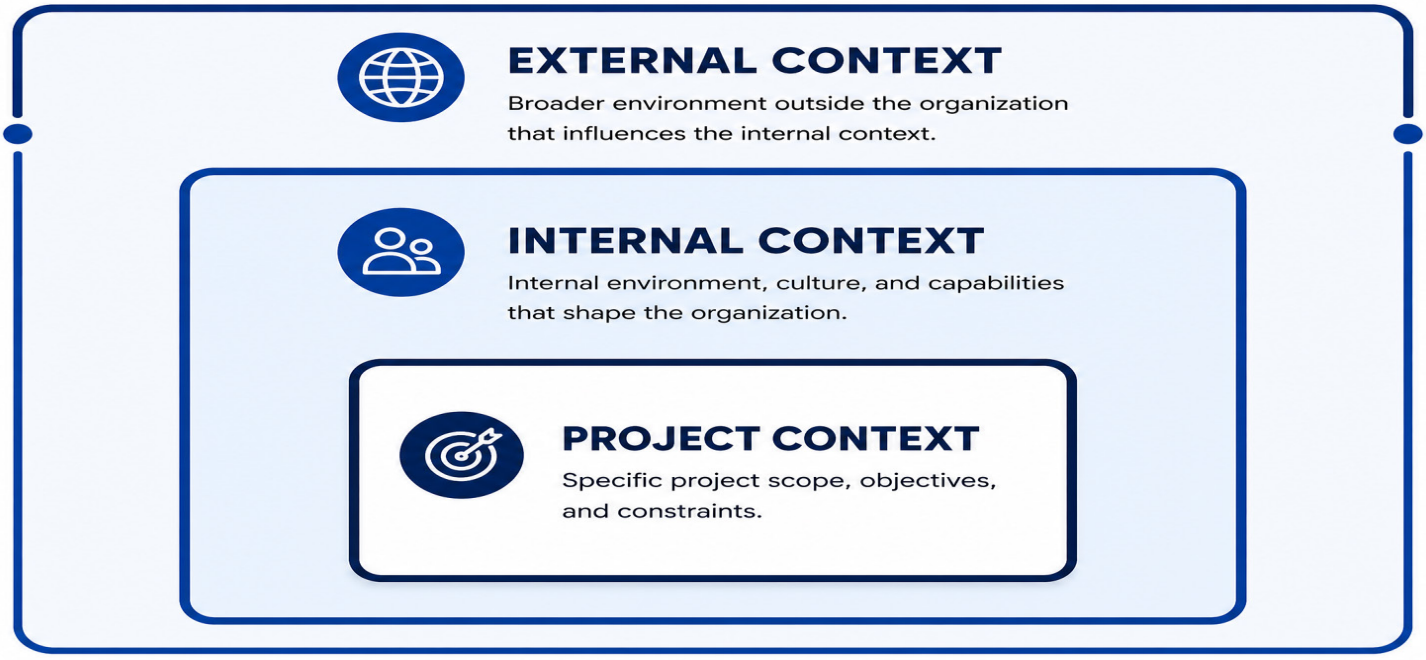

Figure 1: Risk Assessment Perspectives

3.1.1 External Context

Organizations applying this Standard shall identify and document sufficient information relating to the external environment within which the organization and Critical Information Infrastructure (CII) operate. In accordance with ISO 31000 and ISO/IEC 27005, the analysis of the external context should include:

- Applicable laws, regulations, and legal instruments, including the Somalia Cybersecurity Act.
- Factors affecting the organization's financial, economic, political, regulatory, and competitive environment at international, national, regional, or local levels.
- Relevant external drivers, trends, and emerging threats that may influence organizational objectives and cybersecurity risk exposure.
- Applicable industry standards, good practices, and cybersecurity guidance.
- Relationships with and expectations of external stakeholders, including regulators, partners, suppliers, service providers, and donors.

3.1.2 Internal Context

The internal context constitutes elements outside the project scope that have an impact on its accreditation. Whilst the CII project team rarely controls this wider internal organizational context, it relies upon it to secure the ICT system. Within the context of this framework, elements that CII projects depend upon but are outside their control include corporate-level risk management and physical security. Therefore, the CII project team must identify and evaluate the risks the internal context poses to security accreditation. Projects must capture the following information about the organizational environment in which the CII must operate:

3.1.2.1 Internal Constraints

Table 1 above illustrates that the internal context is a subset of the external context. Consequently, the description of the internal context must recognize the impact of external factors. For example, the internal context must reflect impact of mandated Somalia Cybersecurity Act requirements on corporate-level security. In line with ISO/IEC 27005, organizations applying this framework must capture the following details:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- The capabilities, understood in terms of resources and knowledge e.g. capital, time, people, processes, systems and technologies;
- Perceptions and values of internal stakeholders;
- Information systems, information flows and decision-making processes i.e. both formal and informal;
- Relationships with, and perceptions and values of, internal stakeholders;
- Organizational culture;
- Standards, guidelines and models adopted by the organization; and
- Form and extent of contractual relationships.

3.1.2.2 Risk Criteria Definition

All parties applying this framework shall adopt recognizable criteria for identifying, analysis and evaluating risks. As part of a broader risk management process, and in line with IEC/ISO 31010, the risk criteria definition process shall capture:

- How to measure the nature, types of (business) impacts of risk;
- Approach for determining risk levels;
- Criteria for determining when a risk needs treatment; and
- Criteria for deciding when a risk is acceptable and/or tolerable.

The Business Impact Tables contain the official Government risk criteria. However, each organization has a duty to decide its own acceptable and/or tolerable risk levels.

3.1.3 Project Context

Given that, the Government and private sector

organizations usually deliver CII through projects, parties applying this Framework must conduct risk assessments on all project elements within the scope of accreditation. Risk assessment is a primary feature of the accreditation process because it helps generate evidence to show that all system development phases have identified, analyzed and evaluated risks to a CII. As illustrated in Table 1 above, the project context is a subset of the internal context. Therefore, project risk assessments must accommodate the requirements and/or constraints from external and internal context reviews. It is recommended that risk management activities must follow project management best practices sot that results are consistent and repeatable as well as standardized. In particular, the risk assessments must occur at these stages:

3.1.3.1 Project Initiation and Planning

Boards and Management will require the senior officials with delegated responsibility for risk management to provide evidence that they have addressed information risk issues in all phases. Cyber security milestones shall run in parallel with the normal project plan. Failure to identify and address cyber security requirements sufficiently early in the lifecycle could have devastating impacts on milestones, scope and budgets.

3.1.3.1.1 Risk Assessment at Project Initiation and Planning

Parties applying this framework must assess the cyber security risks of a CII project including national security implications during the initiation and planning phases. Whilst not exhaustive, the assessment of the risk potential of the project in the early phase positions security as a vital feature of the delivery methodology. Guided by information from the external and internal contexts, the project should seek to identify the following details:

» The Somalia Cybersecurity Act
» Mandatory information, personnel and physical security requirements;
» Interconnections, flows and relationships with other assets;
» Relevant stakeholders;
» Required skills; and
» Relevant organization risk policies and standards.

3.1.3.2 Project Risk Assessment Scope

This stage builds on the outputs of the security activities in the initiation and planning phase(s) to create a formal scope for the cyber security assessment for the CII project. This activity shall involve detailed review of:

» Business options and preferences;
» Security information obtained in the initiation and planning phase(s);
» The impact of security on the business requirements; and
» Dependencies and applicable legislation.

3.1.3.3 Security Requirements Definition

Building on the previous two activities, this activity:

» Reviews and revised list of security risks identified earlier; and
» Initiates work on the information risk management plan.

3.1.3.4 Review and Selection of Solutions

In accordance with supply chain security requirements, this activity helps the organization select the appropriate technical solution(s). The activities during this phase include:

» Ensuring that supplier contracts contain clear security deliverables;
» Validation of the existence of security deliverables in supply contracts; and
» Revision and approval of the draft information risk management plan.

4 Identify the Assets

As defined under "Risk Management Concepts", an asset is anything that has value to the organization and which, therefore requires protection. The "Scoping Risk Assessments" section requires the CII team to ensure that the activity only encompasses assets in the agreed scope of the risk assessment.

4.1 Objectives of Asset Identification

This activity aims to catalogue of assets. In particular, the CII team shall:

- Identify business/information assets, their locations, functions;
- Information exchange requirements of the information assets;
- Other systems that support the information assets i.e. directly or indirectly.

The result would be a catalogue with the following fields as a minimum.

4.1.1 Description of the Assets

Government and private sector organizations operating CII must obtain sufficient details about the assets to facilitate the risk assessment exercise. The level of detail gathered would depend on the requirements of the project. The organization may also obtain more information about the assets during further iterations of the risk assessment exercises.

4.1.2 Asset Owners

The Somalia Cybersecurity Act by design requires Government and private sector organizations operating CII to appoint heads of division or department as owners of named information assets. The asset owner shall:

- Know the information the assets under their responsibility hold;
- Know who accesses the assets under their responsibility and why, and;
- Help identifying risks to the assets under their responsibility; Information from the asset owner enables the determination of asset value.

4.2 Asset Identification Activities

ISO/IEC 27005 outlines the asset identification approach. The framework recommends the categorization of assets into primary and secondary.

4.2.1 Primary Assets

In line with ISO/IEC 27005, organizations should assemble teams of managers, information systems specialists and users to identify assets essential for the performance of the activity in the scope. Primary assets are of two types:

4.2.1.1 Business processes (or sub-processes) and activities

ICT systems are a means to an end. The end is always to support business processes. Consequently, risk assessment activities must identify the business processes whose interruption could hamper the organization's ability to achieve its mission(s). These include:

- Processes whose loss or degradation make it impossible to carry out the mission of the organization;
- Processes that contain secret processes or processes involving proprietary technology;
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission; and
- Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

4.2.1.2 Information

Primary information mainly comprises:

» Information vital for the exercise of the organization's mission or business;

» Personal information, as defined in national laws regarding privacy;

» Information required to achieve strategic objectives; and

» Information whose gathering, storage, processing and transmission require a long time and/or involve a high cost.

The organization should regard processes and information that do not fall into the categories above as non-essential. The organization can classify as non- essential, a business process or information, if it is able to continue specified operations after the compromise of such a process and/or information.

4.2.2 Secondary Assets

Organizations should also identify and describe secondary assets. The exploitation of vulnerabilities in secondary assets could affect in-scope primary assets. Secondary assets include the following:

4.2.2.1 Hardware

Organizations should identify and record all hardware components including:

» Active data processing equipment i.e. equipment for information processing;

» Passive data medium i.e. for storing data or functions;

» Portable and removable media e.g. laptop computers, tablet computers, smartphones, etc.;

» Fixed computer equipment used at the organization's premises e.g. servers, workstations;

» Electronic medium that can be connected to a computer or computer network for data storage e.g. back-up tapes, removable hard discs, memory keys, tapes; and

» Other media i.e. static, non-electronic media containing data including paper, slides, transparencies, documentation, faxes etc.

4.2.2.2 Software

Organizations should identify and record all software components that contribute to the operation of a data processing set including:

» Operating systems in particular equipment management services (CPU, memory, disc, and network interfaces), task or process management services and user rights management services;

» Service, maintenance or administration software i.e. not directly accessible by users or applications but crucial or even indispensable for CII operations;

» Package software or standard software e.g. database management software, electronic messaging, groupware, directory, web server software, etc; and

» Business applications e.g. account software, machine tool control software, customer care software, HR & administrative software, etc.

4.2.2.3 Network

Organizations should identify and record all telecommunications devices that interconnect several physically remote computers or ICT elements including:

» Medium and supports e.g. Public Switching Telephone Network (PSTN), Ethernet, Gigabit Ethernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications;

» Passive or active relay e.g. bridge, router, hub, switch, etc; and

» Communication interface e.g. Ethernet adaptor.

4.2.2.4 Site

Organizations must identify and record information about the assets linked to the locations, sites and facilities required to host and operate CII including:

» External or exposed environments outside the physical security perimeter

1/1. homes of the personnel, premises of another organization, environment outside the site (urban area, hazard area);

» Information processing premises e.g. data center establishment, buildings;

» Internal information processing premise zones e.g. offices, reserved access zone, secure zone;

» Essential services required for the organization's equipment to operate;

» Telecommunications services and equipment required to operate CII

» and peripherals e.g. low voltage power supply, inverter, electrical circuit head-end; and

» Services and means (equipment, control) for cooling and purifying the air e.g. chilled water pipes, air-conditioners.

5 Defining Security Domains

Applying stringent controls on an asset only improves security if the defenses protecting other assets in its operational environment are equally good. If not, threat actors will identify the weakest link to circumvent the more rigorous defenses. Therefore, after organizations catalogue all assets, the next step is to group the identified assets into security domains.

5.1 Purpose of Security Domains

As defined earlier, a security domain (SD) is a group of assets that are the focus of risk identification (i.e. finding, recognizing and describing) and evaluation activities. This framework requires organizations to group IT assets into security domains for risk assessment purposes. Therefore, security domains aim to:

» Standardize risk identification, analysis and evaluation activities;

» Reduce the difficulty of conducting risk assessments across large, complex and interdependent system boundaries;

» Reduce the effort of conducting risk assessments on individual assets;

» Add context to risk assessment exercises by requiring analysts to consider cyber attacks on other assets supporting the same function, or have similar characteristics and/or reside in the same operating environment;

» Ensuring end-to-end security for assets sharing common threat actors; and

» Enabling the consistent assessment of risks to assets with similar sensitivity.

Organizations shall record the reasons for allocating assets to security domains.

5.2 Modelling a Security Domain

Organizations shall use modelling techniques to represent security domains and their relationships. This framework does not specify a preferred modelling technique. Thus, organizations can choose any technique as long as it presents the information in the format that makes it easy to explain, share and compare. Whatever modelling technique chosen, it must be able to:

- Identify the information assets requiring protection;
- Identify actors and sources threatening to compromise the system's security;
- Express the system's purpose and information exchange requirements;
- Show direct or third parties and relationships with other systems; and
- Show relationships within and between security domains.

5.3 Potential Security Domains

The list below shows the security domains within which organizations usually group assets. They are usual domains because they in effect represent business processes from the external context (Internet) into the project scope. CII teams usually create descriptions of each security domain in different environments such as production, pre-production and disaster recovery. The domains are:

- Internet-facing systems including interfaces with external systems;
- Core access zones organized on criteria such as classification levels;
- Management networks;
- Evidential components of CII with a need to safeguard the chain of evidence to maintain the legal weight and ensure admissibility of electronic records;
- Internal support functions e.g. helpdesks, IT operations and test services;
- Operational sites and facilities;
- Data backup and restore services;
- Third party and other externally managed infrastructure support functions;
- Connections to the CII via (virtual) private connections e.g. remote access;
- Connections to secure external networks for information exchange; and
- Internet and public connected networks to commercial organizations.

5.4 Asset Catalogue

Government and private sector organizations that operate and/or own CII shall use the Asset Catalogue Form below to capture facts about information assets.

SD [Number]	[Name of Security Domain e.g. Backup Environment]				
Asset Identifier	Description	Asset Owner C	Impact Levels		
			I	A	
A1 (A = Asset)	Data backups		4	4	3

Table 1: Asset Catalogue Form

6 Valuing Assets

Asset valuation follows the identification activity. This process is about assigning the asset a widely understood value to enable its secure handling across the organization. In this framework, asset valuation focuses on the business impact of the breach of the asset's confidentiality, integrity and availability rather that its monetary value. Thus, this framework takes a qualitative rather than a quantitative view of asset valuation. Next, this framework presents a scale that organizations shall use to assess and assign business impact values to assets.

6.1 Business Impact Levels

ISO/IEC 27005 states that the creation of unequivocal criteria for assigning asset value is often one of the most difficult aspects of asset valuation. This is because some asset value determinations require subjective judgments yet the activity involves many different stakeholders. Some asset valuation approaches consider the asset's original cost, its replacement or re-creation costs. As noted above, this framework focuses on the business impact of a security incident. The approach in this framework is broader because adverse business consequences resulting from security incidents cover the financial cost of replacing the asset and the information therein and costs to reputation, lost business productivity, sector-wide and national security impacts.

6.2 Business Impact Tables

This framework contains four tables to allow Government and private sector organizations to assess the business impact level of a breach of confidentiality, integrity and availability. This framework organizes the tables as noted below:

- Table 1 – Security, Defense and International Relations;
- Table 2 – Law Enforcement, Public Safety and Public Order;
- Table 3 – Public Services, Public utilities and other Critical Infrastructure; and
- Table 4 – Banking, finance and public finance

6.2.1 Purpose of Business Impact Tables

The business impacts of breaches of confidentiality, integrity and availability differ across sectors. For example, while the disclosure of an individual's banking details could cause distress, a similar disclosure within the defense and security sector could put the life of the individual and others at risk. Therefore, given that organizations in the same sector handle similar information assets and usually face similar threats, consistent business impact assessment improves collective security. This framework uses a business impact level scale from 0 (trivial) to 5 (catastrophic). The scale helps compare business impacts across sectors.

6.2.2 Business Area Sub-Categories

The business impact tables contain sub-categories to help organizations choose the most relevant category for the asset or group of assets under consideration.

6.2.3 Classification and Business Impact Levels Relationship

For confidentially, business impact levels relate directly to classification levels as outlined in the table below.

Classification Level	Impact Level	Business Impact
UNCLASSIFIED	0	Trivial
UNCLASSIFIED-PERSONAL[1]	1	Low
OFFICIAL	2	High
SECRET	3	Extreme
TOP SECRET	4	Catastrophic

Table 2: Relationship between Classification and Business Impact Levels

This Standard requires organizations to assume that security attacks would inflict the maximum possible impact on availability and integrity.

6.2.4 Security, Defense and International Relations

The table provides organizations in the security, defense and diplomacy a consistent approach for assessing business impact of cyber-attacks that could disrupt and/or destroy military, intelligence and other related CII.

Sub Category	IL0	IL1	IL2	IL3	IL4
Life and safety	A security compromise could cause an individual nuisance or anxiety	Disclosure of private information could threaten an individual's personal safety or liberty	A breach of security around certain official records could threaten the security or liberty of a group of people	A security compromise could then threaten life directly leading to limited loss of life	A compromise of security could cause widespread loss of life
Intelligence operations	None	A compromise of security could make it difficult to conduct low level intelligence operations	A compromise of security could hamper intelligence operations in support of public order and public safety	A compromise of security could hamper and damage capacity to conduct intelligence operations aimed to avert severe risks to national security	A compromise of security could hamper and damage capacity to conduct intelligence operations aimed to avert catastrophic risks to national security
Military operations	A security breach could have a minor impact on supply services	A security compromise could moderately reduce operational effectiveness or security of Somali and allied forces	A security compromise could significant damage to the operational effectiveness or security of Somali and allied forces	A security compromise could cause extreme damage to the operational effectiveness or security of a large group of Somali and allied forces in theatre	A security compromise could cause catastrophic damage to the operational effectiveness or security of an extremely large group of Somali and allied forces in theatre
International relations	None	A security compromise could cause low-level embarrassment in international relations	A security compromise could cause embarrassment in international relations e.g. leading formal protest or sanctions	A security compromise could cause extreme tension and serious damage to relations with friendly countries	A security compromise could cause a catastrophic damage to relations potentially provoking war and at best gravely damaging friendly relations
International trade negotiations	None	A security compromise could low-level damage to the prospects of a major Somali company	A security compromise could significantly damage to the prospects of several major companies	A security compromise could cause extreme damage to Somalia's position in bi- lateral international negotiations	A security compromise could cause catastrophic damage to Somalia's position in major multi-lateral international negotiations

Table 3: Security, Defense and International Relations

6.2.5 Law Enforcement, Public Safety and Public Order

The table below aims to provide parties involved in maintaining social order, protecting life and property of the citizens of Somalia a consistent approach for assessing the business impact of cyber-attacks that could disrupt and/or destroy their CII.

Sub Category	IL0	IL1	IL2	IL3	IL4
Life and safety	A security compromise could cause an individual nuisance or anxiety	Disclosure of private information could threaten an individual's personal safety or liberty	A breach of security around certain official records could threaten the security or liberty of a group of people	A security compromise could then threaten life directly leading to limited loss of life	A compromise of security could cause widespread loss of life
Existence or identity of confidential source	A security compromise could lead to disclosure of existence of a confidential source beyond those with a Need-to-Know	A security compromise could lead to disclosure of identity of confidential source beyond those with a Need-to-Know	Disclosure of the identities of a small group of confidential sources identify could increase their vulnerability to attack	A security compromise significantly undermines the witness protection scheme leading to limited loss of life	A security compromise causes a catastrophic failure of the entire witness protection scheme nationwide leading directly to loss widespread loss of life
Police services	None	A security breach leads to minor disruption of police services for an individual	A security compromise leads to substantial disruption of police services to a small group of individuals	A security breach leads to an extremely serious disruption of police services to a large area threatening safety and/or leading to limited loss of life	A security breach leads to a catastrophic disruption of police services directly leading to widespread loss of life for example through riots
Health of citizens	A security compromise could a disruption of health services in one locality	A security compromise could cause a minor disruption of health services posing a risk to health e.g. spread of disease in a district	A security compromise could cause a major disruption of health services posing a risk to health e.g. spread of disease in several districts	A security compromise could cause an extremely severe disruption of health services posing a risk to health and limited loss of life across some regions of the country	A security compromise could cause a catastrophic failure of health services posing a risk to health and widespread loss of life across the entire country

Sub Category	IL0	IL1	IL2	IL3	IL4
Emergency services	Security compromise could disrupt emergency services in one locality	A security breach could cause a minor disruption of emergency services necessitating re- planning at organizational and district levels	A security compromise could cause a major disruption of emergency services necessitating substantial changes in their organization across several districts to meet service levels	A security compromise could cause an extremely severe disruption of emergency services necessitating drastic changes in their delivery mechanisms e.g. involvement of the Armed Forces to meet service requirements across several regions of the country	A security compromise could cause a catastrophic failure of emergency services posing a risk to the internal stability of the country and requiring assistance from neighbouring countries
Political stability	None	A security compromise could cause minor loss of confidence in Government	A security compromise could cause major loss of confidence in Government	A security compromise could cause could threaten directly Somalia's internal political stability	A security compromise could cause a catastrophic collapse of Somalia's internal political stability
Privacy of citizens	A security compromise could cause short-term agony to an individual e.g. disclosure of borrowing history	A security compromise could cause medium-term agony to an individual or short- term embarrassment to several citizens	A security compromise could cause major and sustained agony to a many citizens and extreme stress to an individual. For example, disclosure of a person's medical history	A security compromise could cause extreme agony to millions of citizens across the country e.g. disclosure of medical records in a national hospital and several regional hospitals	A security compromise could a catastrophic collapse of a national identity management system and disclosure of sensitive records for the majority of citizens

Table 4: Law Enforcement, Public Safety and Public Order

6.2.6 Public Services, Public Utilities and other Critical National Infrastructure

The table below provides a consistent approach for assessing the business impacts of cyber-attacks on CII that support daily life, commerce and the activities of the Government.

Sub Category	IL0	IL1	IL2	IL3	IL4
Confidence in public services	A security compromise reducing in an individual's confidence in a public service e.g. crashing government website	A breach resulting in a minor reduction in confidence in a public service by several individuals and severe reduction in confidence by an individual	A security compromise resulting in a major reduction in confidence in the services a major government department e.g. hacking of a national identity database	A security compromise resulting in extreme loss of public trust in the services of several major government departments leading evident reduction in their use e.g. increased use of private clinics	A security compromise resulting in a catastrophic collapse in public trust in government services leading to loss of revenue with critical impact on service continuity
Communications infrastructure	A security breach causing the disruption telecoms for up to 6 hours	A security breach causing the disruption telecoms for up to 12 hours	A security compromise causing the loss of telecom services in a region for up to 24 hours	A security breach causing the loss of telecom services nationally for up to a week	A security breach causing the loss of telecom services nationally for up to more than 1 week
Power & energy	A security breach causing a local power failure for up to 6 hours	A security breach causing a power failure in a region for up to 12 hours	A security breach causing a power failure in a region for up to 24 hours	A security breach leading to the loss of power nationally for up to a week	A security breach leading to the loss of power nationally for more than 1 week
Water and sewerage	A security breach causing the breakdown of local water and sewerage services for less than 50 homes for more than a week	A security breach causing the breakdown of local water and sewerage services for less than 100 homes for up to 1 month	A security breach causing the breakdown of local water and sewerage services for more than 100 homes for up to 1 month	A security breach causing a severe breakdown of regional water and sewerage services for more than 100 homes for up to 3 months	A security breach causing a catastrophic breakdown of national water and sewerage services for more than 100 homes for more than 3 months
Transport	A security breach causing	A security breach causing	A security breach causing	A security breach	A security breach

Sub Category	IL0	IL1	IL2	IL3	IL4
	the disruption of vital local transport systems for up to 6 hours	the disruption of vital local transport systems for up to 12 hours	a major disruption of vital regional transport systems for up to 24 hours	causing extreme disruption to vital national transport systems for up to a week	causing catastrophic failure of vital national transport systems for over a month
Food supplies	A security breach causing the disruption of the distribution of food supplies at the local level for up to a month	A security breach causing the disruption of the distribution of food supplies at the regional level for up to a week	A security breach causing the disruption of the distribution of food supplies at the regional level for up to a month	A security breach causing the disruption of the distribution of food supplies at the national level for up to a month	A security breach causing the disruption of the distribution of food supplies at the national level for over a month

Table 5: Public Services, Public Utilities and other Critical National Infrastructure

6.2.7 Banking, Financial Services and Public Finance

The table below provides a consistent approach for assessing the business impacts of cyber-attacks on CII that support banking and financial activities of citizens, companies and the Government.

Sub Category	IL0	IL1	IL2	IL3	IL4
Public finances	A security breach causing the loss of public sector money up to USD 1,000	A security breach causing the loss of public sector money several between USD 1,000 and USD 10,000	A security breach causing the loss of public sector money between USD 10,000 and USD 100,000	A security breach causing the loss of public sector money between USD 100,000 and USD 1,000,000	A security breach causing a catastrophic loss of public finances estimated at over USD 1,000,000
Trade and commerce	A security breach that undermines the financial viability of several small businesses in Somalia	A security breach that undermines the financial viability of a medium-sized Somalia-owned business organizations.	A security breach that undermines the financial viability of major Somalia-owned business organization	A security breach that causes extreme damage to trade and commerce in Somalia leading to perceptibly reduced economic growth.	A security breach that causes catastrophic and long-term damage to Somalia's global trade and commerce leading to drawn out recession and high hyperinflation
Banking and financial services	A security breach that causes minor financial loss to an individual	A security breach that causes significant financial loss to an individual causing real pressure on short-term finances and minor financial loss to a group of individuals	A security breach that causes a substantial loss of income for a large number of people causing real pressure on their short-term finances and bankrupting some of the affected individuals	A security breach that financially devastates a large group of individuals e.g. pensioners leading to extensive financial distress including personal bankruptcies and repossession of property such as homes	A security breach that catastrophic, widespread and long-term financial damage across the Somali economy bankrupting major corporations including banks and requiring Government and international intervention

Table 6: Banking, Financial Services and Public Finance

7 Identifying Threat Sources

The next step is to identify and record threat sources. As explained above, a threat source instigates attacks against an information asset. Threat sources often collaborate with threat actors who are the entities that execute attacks. Thus, this framework considers threat actors separately from threat sources.

7.1 Typical Threat Sources

Threat sources include, but are not limited to the following entities:

7.1.1 Insiders

Individuals with legitimate access to protected systems are a problematic threat source. These users, jointly known as insiders, include disgruntled employees, suppliers, facilities teams and partners. Insiders have the following attributes:

7.1.1.1 Capability

The capability of the insiders ranges from no skills at all to the highest degree of capability. Insiders with rudimentary technical capability include clerical staff. Facilities teams such as security guards, cleaners and maintenance teams may have varying degrees of technical capability. On the extreme, insiders such as system administrators have advanced technical skills that allow them to launch sophisticated and bespoke attacks.

7.1.1.2 Motivation

Motivations of insiders may include:

» Curiosity;
» Ego;
» Intelligence;
» Monetary gain;
» Revenge; and
» Unintentional errors and omissions

7.1.1.3 Resources

Insiders have moderate resources to launch sophisticated attacks. Typical, insider attacks involve one person with occasional support from part-timers.

7.1.1.4 Consequences

The possible consequences of insider attacks may include, but may not be limited to the following:

» Assault on an employee;
» Blackmail;
» Computer abuse;
» Fraud and theft;
» Information bribery;
» Input of falsified, corrupted data;
» Interception;
» Malicious code;
» Sale of personal information;
» System bugs;
» System intrusion;
» System sabotage; and
» Unauthorized system access.

7.1.2 Foreign Intelligence Services

Nations have always sought to protect their own interests by covertly obtaining information about plans and actions of hostile (and sometimes friendly) States, organizations and individuals since the beginning of time. ICTs have drawn the interest of foreign intelligence services as sources of intelligence. Foreign intelligence services have the following attributes:

7.1.2.1 Capability

Foreign intelligence services have the most advanced technical skills. Foreign intelligence services, especially those in developed countries, have skills to defeat the most advanced security technologies. Foreign intelligence services have some of the best brains in cryptography2 and cryptanalysis3. Recent events have disclosed that intelligence services also seek to use financial and regulatory pressure to subvert the security of commercial encryption products.

7.1.2.2 Motivation

The motivations of foreign intelligence services may include:

» Political gain;

» Economic gain; and

» Military gain.

7.1.2.3 Resources

Being government-financed, the resources of a foreign intelligence services usually match the wealth of the sponsoring nation.

7.1.2.4 Consequences

The possible consequences of foreign intelligence service attacks may include, but may not be limited to the following:

» Defense advantage;

» Political advantage;

» Economic exploitation;

» Information theft;

» Intrusion on personal privacy;

» Social engineering;

» System penetration; and

» Unauthorized system access (access to classified, proprietary, and/or technology-related information).

7.1.3 Industrial Espionage

Industrial espionage attacks may involve large teams of highly trained individuals attempting to compromise a system either full-time or regularly. Perpetrators of industrial espionage may use tools such as Advanced Persistent Threats (APTs) to gain unfettered access to secrets and intellectual property. ICT suppliers may also act in concert with foreign spies in support of economic and political goals of their nations.

7.1.4 Organized Criminal Syndicates

Organized criminal syndicates exploit the anonymity and global reach of the Internet to conduct attacks without ever having to be at the scene of the crime physically. Because of the global nature of their operations, criminals have the resources and capability to conduct sophisticated attacks. Organized criminal syndicates have the following attributes:

7.1.4.1 Capability

The capabilities of organized criminal syndicates could range from moderate to substantial. Some groups with global reach could have the skills that match those of foreign intelligence services of medium-sized countries. As a result, criminal syndicates may have the capability to launch sophisticated and bespoke attacks. As noted earlier, organized crime syndicates could, and often, serve as threat actors for threat sources notably foreign intelligence services.

7.1.4.2 Motivation

The motivations of organized criminal syndicates may include:

» Destruction of information;

» Illegal information disclosure;

» Monetary gain e.g. from foreign intelligence services or blackmail; and

» Unauthorized data alteration.

7.1.4.3 Resources

The resources of organized criminals range from moderate to substantial.

7.1.4.4 Consequences

The possible consequences of organized criminal syndicate attacks may include, but may not be limited to the following:

» Computer crime (e.g. cyber stalking, ransomware);
» Fraudulent act (e.g. replay, impersonation, interception);
» Information bribery;
» Spoofing; and
» System intrusion.

7.1.5 Hackers/Hacktivists

The Cybersecurity Act requires that operators institute measures to detect and resist a compromise by hackers/hacktivists. This group has the following attributes:

7.1.5.1 Capability

Professional hackers are extremely knowledgeable. Individually, hackers can launch both simple and sophisticated attacks. However, a hacker's capability increases exponentially when allied with a cause. Several cyber threat groups and anonymous online actors have launched significant attacks against high-profile corporate and government targets worldwide. This group has the following attributes:

7.1.5.2 Motivation

The motivations of hackers/hacktivists may include:

» Challenge;
» Ego;
» Rebellion;
» Status; and
» Money

7.1.5.3 Resources

Hackers/hacktivists have minimal to moderate resources. In many instances, hacktivists use opportunistic and unsophisticated tactics to exploit poor security such as lack of patching and weak password policies.

7.1.5.4 Consequences

The consequences of hacker/hacktivists attacks may include, but may not be limited to the following:

» Social engineering;
» System intrusion;
» Break-ins;
» Unauthorized system access.

7.1.6 Extremist Organizations

There are concerns that extremist groups such as terrorists are building capacity to use cyber-attacks against critical infrastructure such as power grids to cause violence against and terrorize civilians. This group has the following attributes:

7.1.6.1 Capability

The capabilities of such extremist groups match those of foreign intelligence services. In the spirit of assuming the worst, this framework expects that extremist groups would have the capacity to launch the most sophisticated attacks. The groups have the following attributes:

7.1.6.2Motivation

Unlike hacktivists who seek to embarrass and cause reputational loss, extremist groups focus on the incitement of physical violence and/or disruption of a way of life. The motivations of extremist groups may include:

- Blackmail;
- Destruction;
- Exploitation;
- Revenge;
- Media Coverage; and
- Economic gain e.g. for State-sponsored groups

Extremist organizations may also seek to:

- Political Gain; and
- Military gain.

7.1.6.3 Resources

Extremist groups would have substantial resources.

7.1.6.4 Consequences

The possible consequences of foreign intelligence service attacks may include, but may not be limited to the following:

- Bomb e.g. harm to CII physical infrastructure;
- Terrorism e.g. creation of chaos;
- Information warfare;
- System attack e.g. distributed denial of service;
- System penetration; and
- System tampering.

7.1.7 Investigative Journalists

Investigative journalists perform an important role in society by reporting on the activities of all branches of Government. However, all organizations must have in place adequate measures to stop the unauthorized and/or untimely publication of sensitive information. This group has the following attributes:

7.1.7.1 Capability

Media organizations could be very capable. The media may use non-technical attacks such as social engineering, bribery and coercion of authorized users including disgruntled employees and contract staff. Investigative journalists may also work with political activists to attack CII to expose perceived weaknesses in Government operations.

7.1.7.2 Motivation

The motivations of investigative journalist may include:

- Media Coverage e.g. disclosure of corruption, abuse of office;
- Political Gain e.g. in support of an agenda;
- Ego;
- Monetary gain;
- Illegal information disclosure e.g. in public interest; and
- Revenge

7.1.7.3 Resources

Investigative journalists may have resources ranging from minimal to substantial. In some countries, investigative journalists have hired private investigators to hack the computers and telephones of Ministers and senior government officials.

7.1.7.4 Consequences

Journalist may work with groups such as hackers/hacktivists. Thus, the impacts of the attacks journalist authorized and/or benefit from may include the following:

- Hacking;
- Social engineering;
- System penetration;
- System break-ins;
- Information bribery;
- Sale of personal information; and
- Unauthorized system access (access to classified, proprietary, and/or technology-related information)

7.2 Calculating Threat Levels

The assessment of threat levels must summarize the following aspects about each threat source:

- Capability
- Motivation
- Clearance/Vetting Level
- Value for Information Security Property
- Threat Level

This framework describes these attributes as follows:

7.2.1 Capability

Capability defines the threat source's ability to exploit vulnerabilities to launch attacks against valuable information assets. This framework measures capability levels on a scale of 1 to 5.

7.2.2 Motivation

Motivate measures the desire driving a threat source's interest in breaching security including monetary gain, ideology, coercion, disaffection and pursuit of notoriety. This framework measures motivation levels on a scale of 1 to 5.

7.2.3 Threat Levels

The primary objective of the assessment is to identify the threat level because the level shows the most potent threat sources. A threat level is a product of a threat source's capability and motivation. The threat level points to ability and desire of a threat source to influence the actions of other entities i.e. threat actors. This framework threat levels on a colored six-level scale ranging from TRIVIAL to CATASTROPHIC as illustrated below:

	1	Capability Levels				
		2	3	4	5	
Motivation Levels	0	Trivial[4]	Trivial	Trivial	Trivial	Trivial
	1	Trivial	Trivial	Low	Low	Moderate
	2	Trivial	Trivial	Low	Moderate	High
	3	Trivial	Low	Moderate	High	Extreme
	4	Low	Low	Moderate	Extreme	Extreme
	5	Low	Moderate	High	Extreme	Catastrophic

Table 7: Threat Levels

7.2.3.1 Threat Source Values for C-I-A Elements

Threat sources may have different levels of interest and ability to inflict damage on the three security properties i.e. confidentiality, integrity and availability. Thus, it is useful to present capability and motivation values for the different properties because the overall threat level e.g. EXTREME might not provide clear guidance on where to focus security countermeasures. For example, an investigative journalist is keener on breaching confidentiality than a terrorist entity that might seek to cause terror by attacking the availability of CII such as the power grids. On the contrary, a foreign intelligence services are capable; well-resourced and able to launch the most sophisticated attacks. As a result, foreign spies typically score maximum points (on a scale of 5) for capability against C-I-A i.e. 5-5-5. However, foreign spies might score less than 5 on the motivation scale because they do not make it their absolute priority to attack every system.

Therefore, for C that is not an absolute priority for the intelligence service but on which they have a full-time hacker and some part-timers. As a result, the motivation could for C-I-A is 3-3-3 for respectively. The table below illustrates how one could present foreign intelligence services example above:

Identifier	Threat Source	Property	Capability	Motivation
1	Foreign Intelligence Services	Confidentiality	5	3
		Integrity	5	3
		Availability	5	3

Table 8: Different threat levels for C-I-A

7.2.4 Impact of Security Vetting on Threat Levels

Operators should perform suitable Baseline Security and National Security Vetting checks to ensure that the character and personal circumstances of the individuals are such that they can be trusted with access to protected computers.

The checks can help reduce threats level as follows:

	Trivial	Threat Levels					
		Low	Moderate	High	Extreme	Catastrophic	
Vetting Levels	None	Trivial	Low	Moderate	High	Extreme	Catastrophic
	BASELINE	Trivial	Trivial	Low	Moderate	Extreme	Extreme
	SECRET	Trivial	Trivial	Trivial	Low	Moderate	Extreme
	TOP SECRET	Trivial	Trivial	Trivial	Trivial	Low	Moderate

Table 9: Impact of Security Vetting on Threat Levels

7.3 Example - Threat Source Assessment

Operators applying this framework should use the example below as a starting point for threat source assessments. The example starts by identifying the threat sources and thereafter assessing their overall threat level as well as C-I-A specific levels. The example also considers the impact of security clearances on the overall threat level.

7.3.1 Example - Threat Sources

The framework earlier on identified the possible threat sources. Operators shall describe the threat sources relevant to their CII project. The example below will be of assistance:

7.3.1.1 Organized Crime Syndicates

This example assumes that organized crime groups are very capable and have the resources to carry out sophisticated attacks including bespoke ones. Unlike spies who have unlimited resources, the capability of the criminal groups is at 4- 4-4 for C-I-A. The criminal groups shall also seek to attack the system repeatedly if a successful attack supports their goals. The example assesses motivation at 4-4-4 for C-I-A. However, the motivation could increase or reduce. The groups would also launch non-technical attacks such as social engineering, bribery and coercion of employees, third party and contract staff.

7.3.1.2 Hackers/Hacktivists

This example regards hackers/hacktivists as a technically capable threat source because of their knowledge of IT. This example recognizes that hackers/hacktivists are more potent as threat actors for threat sources such as foreign intelligence agencies, organized crime syndicates and extremist organizations. Judged alone, this example estimates the capability of hackers/hacktivists at 4-4-5 for C-I-A. Availability is at 5 because Distributed Denial of Service (DDoS) attacks are one of the most common attack techniques of hackers notably hacktivists. Hackers also use the same non-technical skills as other threat sources, notably social engineering. Hackers can have strong motivation to attack specific CII individually and as part of a group. Therefore, this example assesses motivation at 4-4-4 for C-I-A.

7.3.1.3 Extremist Organizations e.g. Terrorists

This example assumes that extremist organizations such as terrorists generally have adequate IT expertise to launch simple attacks. The groups may also lack the resources to conduct sophisticated attacks. Therefore, this example rates the capability of extremist organizations including terrorists as 2-2-4 for C-I-A. Yet, the low rating does not give organizations operating CII reason to ignore this threat source because extremist organizations exist to incite other parties, some of which might be competent, into serving as threat actors on their behalf. Given that extremist organizations gain notoriety through acts that cause fear, their interest in CII is low. Hence, this example rates motivation as 2-2-2 for C-I-A.

7.3.1.4 Investigative Journalists

This example regards investigative journalist as technically able. However, news organizations lack the resources required to mount sophisticated attacks. As such, this example assesses the capability of this threat source at 2-2-2 for C-I-A. On motivation, investigative journalists exist to gain access to confidential information. Hence, this example rates motivation at 3-3-3 for C-I-A. However, the motivation is not the maximum, because unlike sources such as organized criminal syndicates, journalists obey the Act and do not usually do whatever it takes to access sensitive information. In common with other threat sources, investigative journalists use non-technical attacks such as social engineering, bribery and coercion of employees, third party and contract staff.

7.3.1.5 Industrial Espionage

Companies seek to gain commercial advantage by gaining unauthorized access to information about their rivals. This example regards companies conducting industrial espionage as technically able and adequately resourced to launch moderately sophisticated attacks. Therefore, their capability is at 3-3-3 for C-I-A. Financial gain usually motivates the entities that conduct industrial espionage. Thus, this example assesses the motivation of the entities at 3-3-3 for C-I-A. The motivation could be higher if the companies serve as threat actors in support of economic and political goals of threat sources such as their home countries, spy agencies, extremist organizations and even investigative journalists.

7.3.1.6 Insiders

This example identifies several insider threat sources.

7.3.1.6.1 Normal and Privileged Users

As a group, normal and privileged users are a serious threat source with considerable technical capability and resources to conduct attacks against because they already have access. As such, the capacity of this combined group is at 5-5-5 for C-I-A. About motivation, this example assumes that a disaffected employee would seek to attack a CII individually on a part-time basis. As such, the motivation is at 2-2-2 for C-I-A. As noted above, security vetting can help reduce the group's threat level. The example, however, expects that the group is susceptible to pressure to serve as a threat actor for other threat sources such as foreign intelligence services, extremist organizations, organized criminal syndicates and journalists. Thus, risk assessment considers external influence.

7.3.1.6.2 Supplier Staff Insider Threat

This example also considers the threat posed by suppliers, third parties, or contracted staff performing highly privileged support functions. Due to the nature of their roles, such personnel possess specialized technical expertise and resources that could enable sophisticated attacks. Accordingly, their capability to compromise the confidentiality, integrity, and availability (C-I-A) of a system is assessed as 4-4-4. Similar to other privileged insiders, this example assumes that a disaffected supplier staff member would conduct attacks against CII on an individual and part-time basis. Therefore, their motivation is assessed as 2-2-2 for C-I-A. Privileged supplier personnel may also be vulnerable to external influence from other threat actors, including foreign intelligence services, which may infiltrate IT companies through planted operatives. Consequently, appropriate security vetting and personnel screening measures can help reduce this threat level.

7.3.1.6.3 Partners

The third insider threat source relates to partners, including government and private sector organizations connected to CII systems. These partners possess significant technical capabilities and resources that could enable sophisticated attacks if misused. Accordingly, their capability to compromise the confidentiality, integrity, and availability (C-I-A) of systems is assessed as 5-5-5. Trusted government and private sector organizations generally have limited motivation to attack systems from which they benefit. Where incidents occur, they are more likely to involve a single individual acting independently and on a part-time basis. Therefore, this example assesses their motivation as 2-2-2 for C-I-A. However, connections from trusted partners may be vulnerable to infiltration or exploitation by other threat actors, including foreign intelligence services. Partner personnel may also be exposed to risks such as bribery, coercion, or blackmail, similar to other insider threat sources.

7.3.2 Summary - Threat Source Identification

The table below summarizes the activity involving the identification of threat sources. The table utilizes the threat level calculation guidance in Table 8 and the values presented in the example outlined in section 7.3.1 above.

Identifier	Threat Source Name	Property	Capability	Motivation	Threat Level
1	Foreign Intelligence Services	Confidentiality	5	3	Extreme
		Integrity	5	3	Extreme
		Availability	5	3	Extreme
2	Organized Crime Groups	Confidentiality	4	4	Extreme
		Integrity	4	4	Extreme
		Availability	4	4	Extreme
3	Hackers/Hacktivists	Confidentiality	4	4	Extreme
		Integrity	4	4	Extreme
		Availability	5	4	Extreme
4	Extremist Organizations	Confidentiality	2	2	Trivial
		Integrity	2	2	Trivial
		Availability	4	2	Moderate
5	Investigative Journalists	Confidentiality	3	3	Moderate
		Integrity	3	3	Moderate
		Availability	3	3	Moderate
6	Industrial Espionage	Confidentiality	3	3	Moderate
		Integrity	3	3	Moderate
		Availability	3	3	Moderate
7	Insiders – Internal Normal & Privileged	Confidentiality	5	2	High
		Integrity	5	2	High
		Availability	5	2	High
8	Insiders – Supplier Staff	Confidentiality	4	2	Moderate
		Integrity	4	2	Moderate
		Availability	4	2	Moderate
9	Insiders – Partners	Confidentiality	5	2	High
		Integrity	5	2	High
		Availability	5	2	High

Table 10: Threat sources with threat levels

8 Identify Threat Actors

This section focuses on an approach for identifying and determining threat actor capabilities. The section addresses threat actors because the framework treats them separately from threat sources. As discussed earlier, threat sources and actors have an intricate relationship. The main difference lies in susceptibility to external influence factor such as coercion, blackmail and bribery. Indeed, external influence is the factor that typically turns a threat source into an actor.

8.1 Threat Actor Types

This framework focuses on the type of attacks that a threat actor might perpetrate. This is a dynamic concept because it shows that threat actors can mount different attacks depending on factors such as the level of access privileges and type of connection. This framework considers the following threat actor types:

8.1.1 Normal Users

Normal users on their own have limited capability to launch attacks. Hence, their capability is a lowly 2. However, some users may have more advanced privileges because of the nature of their jobs e.g. as managers with approval privileges. Hence, this framework raises their capability to 3 on a scale of 5. This group's motivation to attack a CII is estimated at 2. The actor's motivations may include curiosity, ego, influence by spies, monetary gain and revenge. Given that bribery and coercion, occur at level 4 on the threat source motivation scale, external influence is 4.

8.1.2 Privileged Users

Privileged users such as system and network administrators have expert IT knowledge. Although, privileged users may lack resources to gain top ranking in capability, it is prudent to assess their capacity at 5. However, their motivation is at 2. Being insiders, motivations include curiosity, ego, influence by spies, monetary gain and revenge. Given that bribery and coercion occurs at level 4 on the threat source motivation scale, the external influence for this group is 4.

8.1.3 Partners

Partners have the highest capacity to launch attacks against system at 5. The group also has a motivation of 2. Possible motivations include curiosity, ego, influence by spies, competitive advantage and economic espionage. In common with other threat actors, bribery and coercion for this group occurs at level 4 on threat source motivation scale. Thus, the external influence for this group is 4.

8.1.4 Suppliers

Suppliers are insiders. Suppliers have a capability of 4 and inherent motivation of 2. The group includes external system and network administrators. In common with other threat actors, bribery and coercion for this group occurs at level 4 on threat source motivation scale. Possible motivations include competitive advantage and economic espionage. Thus, the external influence for this group is 4.

8.1.5 Consumers

Consumers have the same characteristics as normal users. However, unlike normal users, this group does not contain privileged users with approval privileges. Therefore, their inherent capability and motivation are at 2 and 2 respectively. Motivations may include curiosity, ego, influence by spies, monetary gain and information disclosure. In common with other threat actors, bribery and coercion for this group occurs at level 4 on threat source motivation scale. Thus, the external influence for this group is 4.

8.1.6 Third Parties

As the name suggests, third parties do not have a direct link to the CII. However, these are connections linking to a system of partners of a CII owner or operator. Such third parties are susceptible to infiltration by other threat sources such as hackers/hacktivists. The attack groups willing to piggyback on third party connections to attack a CII are capable of mounting sophisticated attacks and motivated enough to attack the system constantly, bribe and coerce. Motivations may include curiosity, influence by spies, monetary gain, competitive advantage and economic espionage. As such, third party capability and motivation are 4 and 4 respectively.

8.1.7 Facilities

Facilities team threat actor types include security guards, cleaners and building maintenance personnel. The threat actors in this category are insiders because they have physical and often logical access to sensitive information assets. Usually, such threat actors have very limited technical capacity and motivation to attack CII capabilities. As such, the capacity and motivation of facilities is 1 and 1 respectively. Facilities threat actors are liable to external influence. Motivations may include curiosity, influence by monetary gain, revenge and ego. Thus, the external influence for this group is 4.

8.1.8 Physical Intruders

Parties that attempt to gain physical access to CII capabilities are highly capable and motivated. As such, their capability and motivation are 5 and 4 respectively. Break-ins are typically attack techniques of foreign intelligence services and organized criminal syndicates. Motivations of intruders may include influence by spies, monetary gain, competitive advantage and economic/industrial espionage.

8.1.9 Supply Chain Actors

Threat actors within the supply or acquisition chain have similar attributes to suppliers. Hence, their inherent capacity is 4 and motivation of 2. This framework presents a category for supply chain actors because some of these entities do much more than simply supply goods and/or services. In some sectors, such as telecoms, supply chain actors may manage large chunks of the infrastructure. The supply chain security is a major area of focus for the Government and private sector because operatives of foreign intelligence services increasingly target the supply chain. As such, the external influence is 4. Security measures such as national security assessment can reduce this group's threat level.

8.1.10 Disasters

Natural disasters constitute a threat actor because they cause interruptions and/or destruction to CII services. In this Standard, disasters have capability of 1 and 0 motivation. In truth, the capability estimates of 1 is purely academic. Natural disasters can destroy everything. Hence, organizations must assume the worst. In accordance with the NISP, organizations must have adequate business continuity and disaster recovery measures. Organizations, could for instance, mitigate natural disaster risks by transferring them e.g. through insurance.

8.2 Summary - Threat Actor Identification

The table below summarizes the activity involving the identification of threat actors. The table utilizes the guidance in Table 8 to calculate the threat level from the values presented in the example outlined in section 8.1 above.

Threat Actor Type	Threat Actors (Values in brackets refer to Capability, Motivation)	Capability	Motivation 1	Threat Level 1 no External Influence	Motivation 2	Threat Level 2 with External Influence
Normal Users	Normal users (2,2) Managers (3.2)	3	2	Low	4	Moderate
Privileged Users	System Administrator (5,2) Network Administrator (5,2) Firewall Administrator (5,2) Backup Personnel (5,2)	5	2	High	4	Extreme
Partners	MDA Staff (5,2)	5	2	High	4	Extreme
Suppliers	Supplier System Administrator (4,2) Supplier System Administrator (4,2) Supplier Network Administrator (4,2)	4	2	Moderate	4	Extreme
Consumers	MDA Staff (2,2)	2	2	Trivial	4	Low
Third Parties	Hackers/Hacktivists (4,4)	4	4	Extreme	4	Extreme
Facilities	Security Guards (1,1) Cleaners (1,1) Building Maintenance Personnel (1,1)	1	1	Trivial	4	Low
Physical Intruders	Burglars (1,1) Foreign Intelligence Services (5,4)	5	4	Extreme	4	Extreme
Intermediaries	Couriers (1,1) IT Maintenance subcontractors (3,1)	3	1	Low	4	Moderate
Supply Chain Actors	System integrators (4,2)	4	2	Moderate	4	Extreme
Disasters	Force Majeure (1,0)	1	0	Trivial	0	Trivial

Table 11: List of Threat Actors and External Influence

9 Risk Assessment

In accordance with ISO/IEC 27005, this section summarizes the detailed information security risk assessment as opposed to the more generic high-level assessment. In this Standard, risk assessment combines all the steps completed above comprising of:

- Asset identification;
- Grouping of assets into security domain,
- Valuing assets by determining the business impact of a security incident;
- Identification of threat sources;
- Determination of threat actors; and
- Categorization of threat actors into threat actor types.

This section uses the information in the completed steps above to present the approach for creating a list of risks with a Risk Level for each risk.

9.1 Purpose of Risk Assessment

As noted above, this section helps organizations operating CII comply with their obligation to adopt a formal, consistent and policy-guided approach to prioritize risks. In particular, this section aims to:

Ensure that ICT solution procurements contain security requirements;

ICT solutions contain apt controls to secure CII capabilities and assets; and

Support the risk management activities including the development of the Risk Management Accreditation Plan.

9.2 Risk Assessment Considerations

Parties applying this framework must use the following information as input for the risk assessment activity:

9.2.1 Organizational Risk Appetite

The organizational statement of information Risk Appetite states the level and type of information risks a given organization is willing to accept, tolerate or survive in the pursuit of its goals.

9.2.2 Threat Sources & Actors

Risk assessment activities shall rely on the information contained in the previous sections that determined threat source and threat actors.

9.2.3 Attack Methods

Organizations increase the security of CII if they identify and defend against the accidental and deliberate methods a relevant threat actor may use to breach confidentiality, integrity and availability. The Table below shows how to present the attack methods against named threat actor types. The attack methods focus on information (C-I-A) and systems/ infrastructure (configuration). The Table below uses the example of normal and privileged users. Organizations should use the format to identify attack methods for actor types relevant to their project.

Threat Actor Type	Attack Method		
	Confidentiality	Integrity	Availability
Normal User	**Accidental Disclosure** Users accidentally disclose information to users without a valid Need-to-Know and/or security clearance.	**Accidental Corruption** User accidentally reduces the accuracy and completeness of information	**Accidental Disruption** User actions accidentally stop authorized entities from accessing and using information assets and systems upon demand
	Deliberate Disclosure Users deliberately disclose information to users without a valid Need-to-Know and/or security clearance.	**Deliberate Corruption** Users deliberately reduce the accuracy and completeness of information	**Deliberate Disruption** User actions deliberately stop authorized entities from accessing and using information assets and systems upon demand
Privileged User	**Accidental Disclosure** Users accidentally disclose information to users without a valid Need-to-Know and/or security clearance.	**Accidental Corruption** User accidentally reduces the accuracy and completeness of information	**Accidental Disruption** User actions accidentally stop authorized entities from accessing and using information assets and systems upon demand
	Deliberate Disclosure Users deliberately disclose information to users without a valid Need-to-Know and/or security clearance.	**Deliberate Corruption** Users deliberately reduce the accuracy and completeness of information	**Deliberate Disruption** User actions deliberately stop authorised entities from accessing and using information assets and systems upon demand
	Configuration Change User changes configuration leading to the disclosure of information to users without a valid Need-to-Know and/or security clearance	**Configuration Change** User changes configuration leading to the reduction of the accuracy and completeness of information	**Configuration Change** User changes configuration that stops authorised entities from accessing and using information assets and systems upon demand

Table 12: Threat Actors and Attack Methods

9.2.4 Identification of Vulnerabilities

Vulnerabilities are weaknesses in security controls that threat actors may exploit to harm assets or organizations. This framework suggests that CII organizations identify vulnerabilities after determining threat sources and actors. This Standard uses the word "suggest" by design because vulnerability assessment can occur at any stage of the risk assessment process. Indeed, vulnerability assessments may actually be the first activity of a risk management process.

9.2.5 Vulnerable Areas

In accordance with ISO/IEC 2700, this framework requires CII operators to consider potential security vulnerabilities in the following areas:

- Security governance, organizational structure, roles and accountabilities
- Processes and procedures;
- Management routines;
- Personnel
- Physical environment;
- Information system configuration;
- Hardware, software or communications equipment; and
- Dependence on external parties i.e. supply chain risks

As noted earlier, this framework suggested that vulnerability assessment follows threat source and actor identification. The advice finds support in the ISO/IEC 27001 observation that vulnerabilities without corresponding threats may not require action. Organizations must record and monitor all vulnerabilities for potential changes. The activity must produce:

A list of vulnerabilities in relation to assets, threats and controls; and

A list of vulnerabilities that do not relate to any identified threat for review.

Annex D of ISO/IEC 27005 contains useful examples of vulnerabilities in various security areas and threats that might exploit these weaknesses. The list should provide a starting point during threat and vulnerability assessments.

9.2.6 Threat Actors and Security Domains

The assessments shall identify the security domains that threat actor affect. The new illustration uses the threat level with the external influence factor to show the worst-case scenario.

Threat Actor Type	Threat Level (with Influence)	Threat Actors (Values in brackets refer to Capability, Motivation)	Affected Security Domain (SD)		
			SD1	SD2	SD(nth)
Normal Users	Low	Normal users (2,2)	ü	ü	ü
		Managers (3.2)		ü	
Privileged Users	High	System Administrator (5,2)	ü	ü	ü
		Network Administrator (5,2)	ü	ü	ü
		Firewall Administrator (5,2)	ü	ü	
		Backup Personnel (5,2)		ü	
Partners	High	MDA Staff (5,2)		ü	
Suppliers	Moderate	Supplier System Administrator (4,2)			ü
		Supplier System Administrator (4,2)	ü		
		Supplier Network Administrator (4,2)	ü		
Consumers	Trivial	MDA Staff (2,2)		ü	
Third Parties	Extreme	Hackers/Hacktivists (4,4)	ü	ü	ü
Facilities	Trivial	Security Guards (1,1)	ü	ü	ü
		Cleaners (1,1)	ü	ü	
		Building Maintenance Personnel (1,1)		ü	ü
Physical Intruders	Extreme	Burglars (1,1)	ü	ü	ü
		Foreign Intelligence Services (5,4)	ü	ü	ü
Intermediaries	Low	Couriers (1,1)	ü	ü	ü
		IT Maintenance subcontractors (3,1)	ü	ü	ü
Supply Chain Actors	Moderate	System integrators (4,2)		ü	
Disasters	Trivial	Force Majeure (1,0)	ü	ü	ü

Table 13: Threat Actors and affected Security Domains

9.3 Risk Levels

Parties applying this Standard shall use the table below to calculate Risk Level. As noted under "Risk Management Concepts," the level of risk describes the magnitude of risk as expressed in terms of the combination of impacts and their likelihood. Accordingly, the Table below shows that the Risk Level is a product of the comparison of the business impacts of risk realization and the likelihood of occurrence. As a reminder, the framework showed earlier that classification levels correlate with business impact levels.

Very Low Low			Likelihood					
			Medium	**Medium-High**	**High**	**Very High**		
Impact of Risk Realisation	**UNCLASSIFIED**	IL0	Very Low	Very Low	Low	Low	Low	Low
	UNCLASSIFIED -PERSONAL	IL1	Very Low	Low	Low	Medium	Medium	Medium
	OFFICIAL	IL2	Low	Low	Medium	Medium	Medi-um-High	Medium- High
	SECRET	IL3	Low	Medium	Medium	Medi-um-High	High	High
	TOP SECRET	IL4	Medium	Medium	Medium-High	High	Very-High	Very-High

Table 14: Risk Levels

10 Risk Assessment Model

As noted earlier, this framework regards in-depth risk assessment as the process that involves the identification and valuation of assets, the assessment of threats to those assets and assessment of vulnerabilities. The Table below summarizes the risk assessment process.

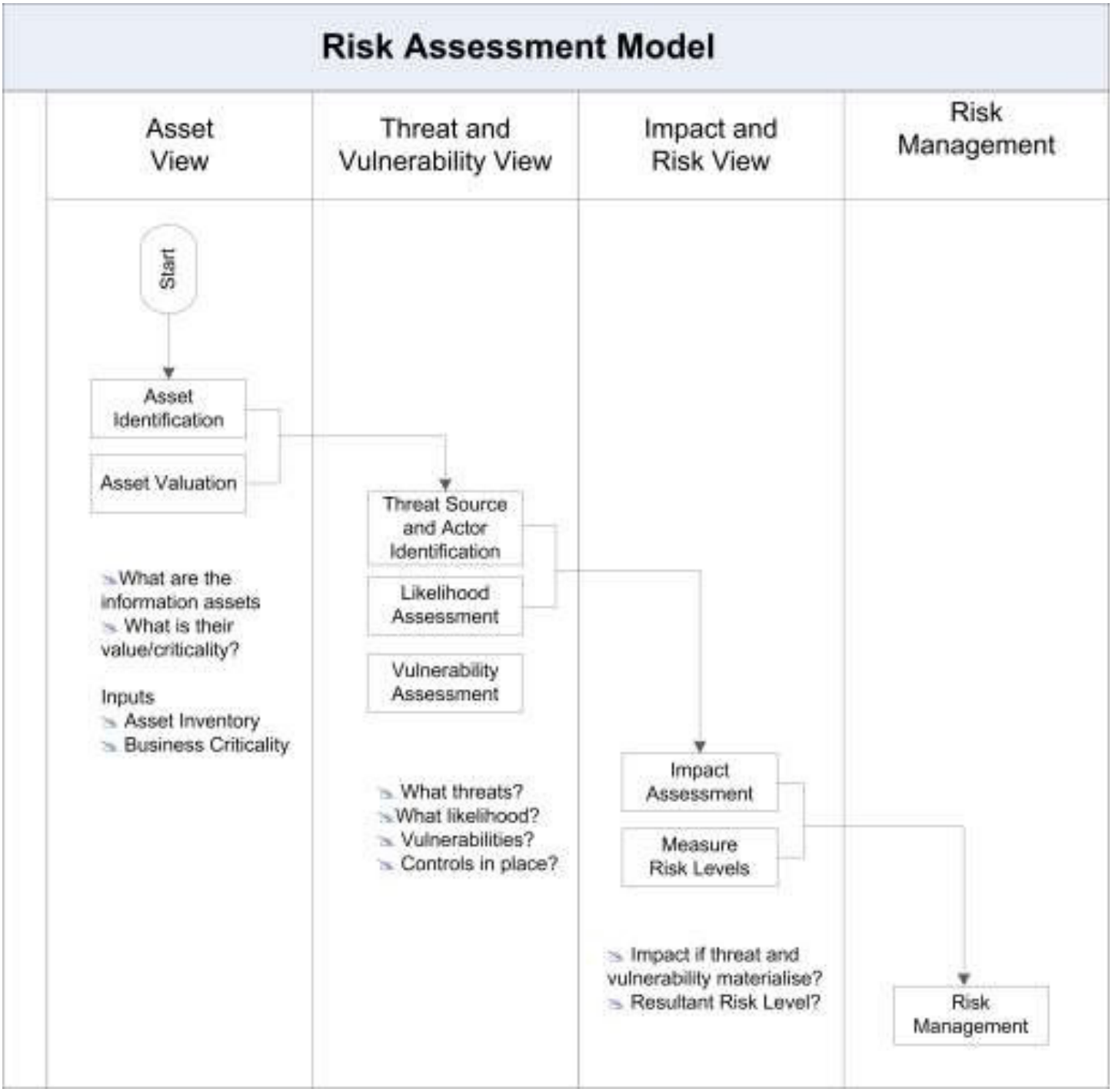

Figure 2: Risk Assessment Model

10.1 Assessing Risks

Given that, the framework has captured the information in the asset, threat and vulnerability views already, the next step identifies and assesses the risks that each threat actor type poses. The framework uses the two examples of the threat actor types for which it identified attack methods as examples. Parties using this Standard shall continue the activity for the other threat actor types.

10.1.1 Example 1 - Normal Users

The risk assessment table below uses information from Tables 8, 11 and 12.

Threat Actor Type	**Normal User**		**Affected Security Domain:**		**SD1**			
Property	**Attack Method**	**Capability**	**Motivation** (Influence)	**Threat Level** (Capability + Motivation)	**Impact Level of Risk Realization**	**Likelihood**	**Risk Level** (Impact + Likelihood)	**Risk ID**
Confidentiality	Accidental Disclosure	2	4	Low	4	Low	Medium	1
	Deliberate Disclosure	2	4	Low	4	Very Low	Medium	2
Integrity	Accidental Corruption	2	4	Low	4	Medium	Medium-High	3
	Deliberate Corruption	2	4	Low	4	Low	Medium	4
Availability	Accidental Disruption	2	4	Low	3	Medium	Medium	5
	Deliberate Disruption	2	4	Low	3	Very Low	Low	6

Table 15: Normal User Risk Assessment

10.1.2 Example 2 - Privileged Users

The risk assessment table below uses information from Tables 8, 11 and 12. The risk assessment chooses different likelihoods to those of normal users.

Threat Actor Type	Privileged User		Affected Security Domain:		SD1			
Property	**Attack Method**	**Capability**	**Motivation** (Influence)	**Threat Level** (Capability + Motivation)	**Impact Level of Risk Realization**	**Likelihood**	**Risk Level** (Impact + Likelihood)	**Risk ID**
Confidentiality	Accidental Disclosure	5	4	Extreme	4	Medium	Medium- High	7
	Deliberate Disclosure	5	4	Extreme	4	Medium	Medium- High	8
	Configuration Change	5	4	Extreme	4	Medium-High	High	9
Integrity	Accidental Corruption	5	4	Extreme	4	High	Very- High	10
	Deliberate Corruption	5	4	Extreme	4	Medium	Medium- High	11
	Configuration Change	5	4	Extreme	3	High	High	12
Availability	Accidental Disruption	5	4	Extreme	3	High	High	13
	Deliberate Disruption	5	4	Extreme	3	Medium	Medium	14
	Configuration Change	5	4	Extreme	3	Very-High	High	15

Table 16: Privileged User Risk Assessment

11 Prioritized Risks

The purpose of this last step is to create an easy-to-understand list of all risks starting from the highest Risk Levels to the ones with lower Risk Levels. As a minimum requirement, the prioritized list of risks shall have the following fields:

» Risk ID;
» Security Domain;
» Threat Actor Type;
» Risk Description; and
» Risk Level

Parties applying this Standard may add as many fields as necessary for their business and security requirements.

11.1 Table of Prioritized Risks

The table below presents the prioritized risks from the two examples in 10.1.1 (normal users) and 10.1.2 (privileged users).

Risk ID	Security Domain (Number)	Threat Actor	Risk Description (Format[5])	Risk Level
10	SD[N]	Privileged User	***Given that*** privileged users have powerful privileges [identify the privileges] ***and that*** [e.g. it is difficult to monitor their access] ***there is a risk that*** their accidental actions [specify actions and/or system] would significantly reduce the accuracy and completeness of information [specify system] ***leading to*** [e.g. serious damage the [organization's] finances and reputation etc]	Very High
9	SD[N]	Privileged User	Confidentiality – Configuration change [use format in Risk ID 10 above to describe risk]	High
12	SD[N]	Privileged User	Integrity - Configuration Change	High
13	SD[N]	Privileged User	Availability – Accidental disruption	High
15	SD[N]	Privileged User	Availability – Configuration Change	High
7	SD[N]	Privileged User	Confidentiality – Accidental Disclosure	Medium-High
8	SD[N]	Privileged User	Confidentiality – Deliberate Disclosure	Medium High
11	SD[N]	Privileged User	Integrity – Deliberate Corruption	Medium-High
3	SD[N]	Normal User	Integrity – Accidental Corruption	Medium-High
14	SD[N]	Privileged User	Availability – Deliberate Disruption	Medium
1	SD[N]	Normal User	Confidentiality – Accidental Disclosure	Medium
2	SD[N]	Normal User	Confidentiality – Deliberate Disclosure	Medium
4	SD[N]	Normal User	Integrity – Deliberate Corruption	Medium
5	SD[N]	Normal User	Availability – Accidental Disruption	Medium
6	SD[N]	Normal User	Availability – Deliberate Disruption	Low

Table 17: Prioritized List of Risks

11.2 Risk Assessment Summary

Parties using this framework shall create a summary to provide a quick view of the risks identified. The simple statement that should appear as follows:

11.2.1 Executive Summary

The risk assessment identified [e.g. 200] risks each with unique ID including:

10 Very-High Risks	**50 High Risks**
30 Medium-High Risks	**60 Medium Risks**
40 Low Risks	**10 Very-Low Risks**

11.2.2 Summary Description

The next step is to create a summary description of the risks by threat actor type. Below are examples on risks affecting supply chain and third parties.

11.2.2.1 Supply Chain Attacks

The acquisition of compromised hardware and software poses momentous risk to the confidentiality, availability and availability of [CII Project] infrastructure. The level of risk is significant across [CII Project Name] infrastructure giving rise to 5 Very High Risks, 15 High Risks and 3 Medium High Risks. The compromise of hardware and software assets during their acquisition poses a significant threat to [CII Project Name] given that it supports national security activities. [CII Project Name] team must put in place a range of governance, information, personnel and physical security controls to mitigate the risk.

11.2.2.2 Attacks via Third Parties

External connections from the Internet that terminate in Zone X (Security Domain 1) pose a significant risk to the Confidentiality, Integrity and Availability of [CII Project] infrastructure. 3 Very High, 10 High and 3 Medium High Risks threaten the security of the infrastructure within Zone X and other Security Domains within the [CII Project]. [CII Project] must harden Zone X to address this risk. Zone X requires strong technical controls to identify threats from the Internet. [CII Project] must also adopt information and personnel security controls to bolster the technical measures such as the use of enforceable exchange agreements.

12 National Risk Treatment Methodology

12.1 Purpose and Scope

This section defines the national methodology for treating cybersecurity risks identified through the Somalia National Cybersecurity Risk Management Framework and for ensuring consistent, transparent, and auditable decisions on how risks are handled across all Critical Information Infrastructure (CII) and other covered entities. It is aligned with ISO/IEC 27005 and ISO/IEC 27001 requirements on information security risk treatment and risk treatment planning. The methodology applies to:

1. All risks included in the national and sectoral prioritized risk lists produced under the Framework.
2. All ministries, agencies, and regulated operators designated as CII or otherwise in scope of this Framework.

12.2 Principles for Risk Treatment

National risk treatment decisions shall be guided by the following principles:

1. Alignment with national risk appetite. Treatment options must be consistent with the national and sector-specific risk appetite
2. Proportionality. Controls and other measures must be proportionate to the assessed risk level, potential harm to national interests, and the criticality of affected assets and services.
3. Compliance. Treatment must satisfy applicable legal, regulatory, and contractual obligations, including requirements related to critical infrastructure protection, data protection, financial stability, and national security.
4. Cost-effectiveness. Treatment options should balance the cost and complexity of implementation against the expected reduction in risk.
5. Accountability. Each risk must have a designated risk owner who is accountable for selecting the treatment option, approving the risk treatment plan, and accepting residual risk.
6. Traceability and evidence. All treatment decisions and rationales must be documented in national and sectoral risk registers.

12.3 Risk Treatment Options

For every risk above the defined acceptance criteria, the risk owner shall select one or more of the following risk treatment options.

12.3.1 Risk Avoidance

Risk avoidance involves deciding not to start, or to discontinue, the activity that gives rise to the risk. At national level this may include, for example:

- Decommissioning or disabling legacy systems that cannot be secured to an acceptable level.
- Avoiding the introduction of high-risk technologies or services into critical national systems where adequate safeguards are not feasible.
- Terminating cross-border connectivity, data flows, or third-party relationships that pose unacceptable risks to national security or critical services.

Risk avoidance is appropriate when:

- The assessed risk exceeds national risk appetite and cannot be reduced to an acceptable level through feasible controls.
- The business or national strategic benefits of continuing the activity are outweighed by the potential impact of a compromise.

12.3.2 Risk Mitigation

Risk modification mitigation involves implementing technical, organizational, procedural, or physical controls to reduce the likelihood and/or impact of the risk to an acceptable level. Mitigation is the default treatment option and should be considered first where:

» The risk level is above national or sectoral thresholds but can be reduced through feasible and cost-effective controls.

» The underlying activity is essential to national services and cannot be reasonably avoided.

12.3.3 Risk Transfer

Risk sharing transfer involves transferring or sharing a portion of the financial or operational consequences of a risk with a third party, while recognizing that accountability for the risk cannot be fully outsourced. Examples include:

» Purchasing cyber insurance to cover incident response, business interruption, and liability costs.

» Outsourcing certain services (e.g. managed security operations, cloud hosting) to providers under contractual arrangements that specify security obligations and liabilities.

» Allocating responsibilities and liabilities through public–private partnership agreements or sectoral contracts.

Risk sharing is appropriate when:

» Risks are financial or operational in nature and can be partially offset through insurance or contractual arrangements.

» Third parties are better positioned to manage certain aspects of the risk (e.g. specialized detection capabilities) while the Government or CII operator retains oversight.

12.3.4 Risk Acceptance

Risk acceptance involves consciously retaining the residual risk after assessment and, where appropriate, after applying other treatment options. Risk may be accepted when:

» The assessed risk level is within the defined acceptance criteria for the relevant sector or asset.

» The cost, complexity, or operational impact of additional treatment measures would be disproportionate to the expected risk reduction.

» There are no feasible treatment options, but the activity is essential for the delivery of critical services.

Risk acceptance decisions must:

» Be formally documented, including justification, assumptions, and conditions.

» Be approved at an appropriate management level

» Define monitoring requirements and review triggers (e.g. changes in threat level, exploitation of a vulnerability, or new regulatory mandates).

12.4 Method for Selecting Treatment Options

12.4.1 Inputs to Treatment Decisions

Risk treatment decisions shall use, at a minimum, the following inputs:

» Assessed risk level (likelihood and impact) for each scenario, as determined by the national risk assessment model.

» Asset criticality, business impact ratings, and classification levels derived from earlier steps (asset valuation and business impact analysis).

» National and sectoral risk appetite and tolerance parameters.

» Legal, regulatory, and contractual

requirements (including sector-specific regulations).

» Cost–benefit analysis of potential treatment options (including implementation, operation, and maintenance costs).

» Dependencies on external parties (e.g. cross-border data flows, regional infrastructure, supply chain).

12.4.2 Decision Process

Risk owners shall apply the following decision process for each risk:

» Validate that the risk scenario, cause, assets, and assessed risk level are correct and remain current.

» Assess whether the activity causing the risk can be stopped, delayed, or redesigned without unacceptable impact on national objectives; if yes and justified, select risk avoidance.

» Identify and evaluate potential controls that could reduce likelihood or impact.

» For each candidate control set, estimate the residual risk level and compare it to national and sectoral risk acceptance criteria.

» Where residual risk or implementation costs remain high, assess whether insurance, outsourcing, or other arrangements can share or transfer part of the financial or operational impact.

» If, after considering avoidance, mitigation, and sharing, residual risk remains but is within acceptance criteria, propose risk retention with documented justification and monitoring arrangements.

» Record the chosen treatment option(s), rationale, selected controls, responsible parties, implementation timelines, and residual risk in the risk register and risk treatment plan and obtain formal approval.

12.4.3 National Risk Treatment Plan

At national and sectoral levels, the outputs of the treatment decisions shall be consolidated into formal risk treatment plans by SOM-CIRT. Each risk treatment plan shall include, at a minimum:

» Reference to the risk identifier and description in the national/sectoral risk register.

» Responsible risk owner and implementing parties (e.g. lead ministry, sector regulator, CII operator).

» Implementation schedule, milestones, and required resources.

» Expected residual risk level and justification that it falls within the defined acceptance criteria.

» Monitoring, reporting, and review arrangements, including performance indicators and triggers for re-assessment.

SOM-CIRT shall periodically review aggregated treatment plans to:

» Ensure that treatment decisions are consistent with national policy, risk appetite, and sector priorities.

» Identify systemic or cross-sector risks that require coordinated national programs or investments.

» Adjust guidance, baselines, and minimum controls where emerging threats or incidents demonstrate that residual risk is no longer acceptable.

12.4.4 Governance, Monitoring and Review

National risk treatment results shall be owned and approved by the highest decision-making body of each Critical Information Infrastructure (CII) operator (e.g. Board of Directors, Executive Committee, or equivalent authority), and shall be reviewed, updated, and re-approved at least annually in accordance with this Framework and applicable national cybersecurity legislation.Each CII operator shall prepare and submit its updated risk treatment plan, including associated residual risk acceptance decisions, to SOMCIRT within the timelines and in the format prescribed by the Authority.

Failure by a CII operator to fulfil these obligations may constitute willful non-compliance under the applicable Cybersecurity Act, including Article 20 relating to non-compliance with statutory obligations, which provides that such non-compliance constitutes an offence punishable by a fine not exceeding USD 3,000 or its equivalent in Somali Shillings, imprisonment for a term not exceeding six months, or both. Risk treatment is an iterative and continuous process and shall be integrated into national cybersecurity governance mechanisms. At a minimum:

- Risk treatment plans shall be reviewed at least annually, or earlier where significant changes occur in threats, vulnerabilities, technologies, business operations, or national priorities.
- SOMCIRT shall maintain oversight of implementation progress for high-priority risks affecting critical services and national security.
- Lessons learned from cybersecurity incidents, exercises, audits, and assessments shall be incorporated into updated treatment measures, control requirements, and risk acceptance criteria.

APPENDIX 1

1. CYBERSECURITY MATURITY MODEL FOR SOMALIA

1.1. Preamble

Somalia adopts a five-level national cybersecurity maturity model to establish a common and regulator-ready framework for measuring the cybersecurity capability of Critical Information Infrastructure (CII) operators and other high-priority entities. The model aligns cybersecurity maturity expectations with the National Cybersecurity Risk Management Framework, annual risk treatment obligations, board-level accountability, and regulatory reporting requirements to the National Communications Authority. The model supports the progression of institutions from reactive and informal cybersecurity practices to risk-informed governance, measurable performance, resilience, and continuous improvement. It also provides a structured and nationally consistent approach for the National Communications Authority and sector regulators to establish minimum cybersecurity expectations, prioritize regulatory oversight, and strengthen national cyber resilience across critical sectors.

1.2. Context

The existing National Cybersecurity Risk Management Framework already establishes a structured approach to cybersecurity risk assessment, including asset identification, threat source analysis, threat actor identification, risk assessment, prioritization, and risk management planning. It also states that organizations operating critical information infrastructure should adopt a formal, consistent, and policy-guided approach to prioritise risks and support risk management and accreditation activities. Building on that foundation, this model complements the risk framework by assessing

institutional capability, not just individual risk scenarios. This is reinforced by the governance and compliance expectations already reflected in the framework discussion developed for national risk treatment methodology. Under that approach, the highest decision-making body of each critical infrastructure operator is expected to own and approve the risk treatment decisions, ensure it is reviewed and updated annually, and submit the resulting risk treatment plan and residual risk decisions to the NCA.

The model also enables proportional regulation. Entities at lower maturity levels can be targeted for remediation plans, technical assistance, and closer oversight, while entities at higher levels can be expected to demonstrate stronger measurement, assurance, and cross-sector coordination. For operators, the model provides a roadmap for improvement. Instead of treating compliance as a one-time documentation exercise, it frames cybersecurity as an organizational capability that must be governed, measured, and improved year after year.

1.3. Design Principles

The model is based on six design principles as noted below:

» Alignment with the national risk management framework and not operate as a separate, conflicting assessment structure.

» Each maturity level is defined in clear policy and operational terms so that boards, executives, assessors, auditors, and the NCA can apply it consistently.

» It is risk-based. Maturity should not be measured only by the existence of policies; it should also reflect whether cyber risk is identified, treated, monitored, escalated, and governed in proportion to the criticality of services and assets.

» It should be evidence-based. Organizations should be able to demonstrate maturity through approved policies, risk registers, treatment plans, metrics, audit results, exercise records, and reports submitted to regulators.

» It should support annual review and regulatory reporting. This reflects the expectation that risk treatment methodology is owned by the highest decision body, conducted at least annually, and submitted to the NCA.

» It should support progressive improvement. The model encouraged organizations to move steadily from ad hoc compliance toward resilient, measurable, and nationally integrated cybersecurity practice.

1.4. The Five Maturity Levels

1.4.1. Initial

At Level 1, cybersecurity practices are ad hoc, fragmented and mainly reactive. Activities depend heavily on individual effort rather than institutional governance, and there is little assurance that essential risks are being identified or managed consistently. Organizations at this level may have isolated technical controls, but these are not supported by an approved strategy, a formal risk management process, or clear accountability structures. Incident response is improvised, records are incomplete, and management reporting is limited or absent. From a policy perspective, Level 1 indicates material exposure for any entity delivering essential or critical services. Where a critical infrastructure operator remains at this level, the NCA will regard it as a priority case for remedial oversight because weak governance significantly increases the probability of unmanaged national cyber risk.

1.

4.2. Developing

At Level 2, the organization has started to recognize cybersecurity as a formal management issue and has introduced some structured practices. Basic policies designated focal points, and selected controls may exist, but implementation remains incomplete and inconsistent across functions or systems. Risk assessments at this stage are usually limited in scope and are often performed for specific projects, audits, or regulatory requests rather than as part of a mature enterprise-wide risk management cycle. Reporting to leadership may occur occasionally, but there is not yet a structured board-level oversight mechanism or systematic annual submission to the regulator. Level 2 reflects transitional capacity. It is stronger than purely reactive practice, but it still leaves critical weaknesses in consistency, assurance, and accountability that must be addressed before an operator can be considered reliably compliant with national cybersecurity obligations.

1.4.3. Defined

At Level 3, cybersecurity governance and risk management are formally documented, standardized, and communicated across the organization. Policies, procedures, and roles are formally approved, and there is a repeatable and risk-based process for identifying assets, assessing threats and vulnerabilities, prioritizing risks, and selecting treatment actions. This is the level at which the organization begins to align clearly with the national framework and recognized international standards and best practices such as International Organization for Standardization ISO/IEC 27001 and ISO/IEC 27005, as referenced in the developed treatment methodology. Incident response, compliance tracking, control implementation, and training are no longer isolated activities but parts of a structured cybersecurity programme. From a national policy standpoint, Level 3 is the minimum recommended target maturity level for critical infrastructure operators. At this level, an operator can demonstrate that it has the internal structure needed to meet annual obligations, maintain auditable evidence, and respond coherently to supervisory review.

1.4.4. Managed

At Level 4, cybersecurity is actively governed, monitored, measured, and integrated into business and operational decision-making. The highest decision-making authority reviews risk information, approves treatment priorities, and oversees residual cyber risk acceptance in a structured and periodic manner. Risk treatment decisions are linked to budgets, projects, procurement, business continuity and resilience planning, and third-party oversight. Metrics and indicators are used to track implementation and performance, while internal audit or independent assurance provides continuous assurance mechanisms to verify whether controls and governance processes are operating effectively. This level is especially important for national resilience because it transforms cybersecurity from a compliance exercise into an operational and strategic management discipline. Operators at Level 4 are typically capable of performing annual reviews credibly, submitting meaningful reports to the National Communications Authority, and responding effectively to evolving threat conditions.

1.4.5. Optimizing

At Level 5, cybersecurity capability is continuously assessed and improved through evidence, cyber threat intelligence, exercises, incidents, audits, and cross-sector collaboration. Security considerations are embedded in strategic planning, transformation programmes, and major organizational decisions rather than being introduced late in the process. The organization not only manages its own risks effectively but also contributes to organizational and national resilience through sector-wide collaboration and information sharing, coordinated exercises, and support for sectoral improvement initiatives. It uses lessons learned to refine controls, strengthen governance, and improve response readiness as part of a continuous improvement cycle. In policy terms, Level 5 represents national and international best practice. It should be encouraged for the most systemically important Critical Information Infrastructure (CII) operators and may serve as a benchmark for sector leaders, but it should not be treated as the baseline compliance requirement for all regulated entities.

1.5. Domain structure for assessment

To make the model practical and measurable, maturity should be assessed across a common set of cybersecurity capability domains derived from the Framework and associated treatment methodology. These domains should include governance and leadership, risk management, asset and information protection, technical and operational security controls, incident management, third-party and supply chain security, resilience and recovery, cybersecurity awareness and workforce capability, assurance and audit, and regulatory reporting. The minimum mandatory controls are documented in the Cybersecurity Compliance Framework. A domain-based assessment structure enables assessors to determine not only an overall maturity level but also specific capability gaps and areas requiring improvement. An operator may, for example, demonstrate relatively strong technical controls while remaining weak in governance, third-party oversight, regulatory compliance, or board-level accountability. This approach is particularly valuable for regulatory oversight because it supports risk-based and targeted remediation planning. Rather than issuing generic directives, the National Communications Authority may require operators to implement targeted corrective actions in the domains that present the greatest operational, sectoral, or national cyber risk.

1.6. Governance expectations

The maturity model should expressly state that accountability for cybersecurity resides at the highest level of organizational decision-making within critical infrastructure operators. Accordingly, the Board of Directors, Executive Committee, or equivalent apex authority should own the organization's cybersecurity maturity posture, approve annual maturity assessments, and oversee corrective action and improvement plans. This governance expectation ensures that decisions relating to cyber risk treatment, cybersecurity investment, residual risk acceptance, resilience planning, and legal compliance are made by individuals with the authority to direct organizational resources, priorities, and strategic objectives. For this reason, the model requires each Critical Infrastructure (CI) operator to conduct a formal annual

cybersecurity maturity assessment and submit the approved results, including improvement actions and risk treatment updates, to the National Communications Authority. This requirement establishes a direct governance and accountability linkage between organizational self-assessment, executive oversight, and national cybersecurity supervision.

1.7. Regulatory and legal implications

The maturity model should be used as a supervisory instrument. The NCA will use annual submissions to monitor compliance trends, identify systemic cybersecurity weaknesses, and direct inspections or enforcement action where appropriate. This is especially relevant considering Article 20 of the Somalia Cybersecurity Act on non-compliance with obligations as provided in the user-supplied legal extract. Where a critical infrastructure operator willfully neglects required obligations, the Act provides for criminal or penal consequences including a fine not exceeding USD 3,000, or equivalent in Somali Shillings, or imprisonment for up to six months, or both. Persistent failure to assess maturity, implement treatment plans, maintain governance records, or submit annual reports may be treated as evidence of wider non-performance and broader governance failure under the legal framework.

1.7.1. Recommended regulatory position

The most balanced national policy position is to require all Critical Information Infrastructure (CII) operators to achieve at least Level 3 cybersecurity maturity within a defined transition period and to progressively advance toward Level 4 maturity for systemically important sectors, particularly the financial services sector. Level 3 establishes the minimum conditions necessary for repeatable governance, formally documented processes, effective risk management, and coherent regulatory engagement, while Level 4 establishes the stronger management, assurance, and operational discipline required for high-consequence and nationally significant environments. National implementation should also combine regulatory supervision with institutional capacity-building initiatives. Lower-maturity operators will require not only regulatory oversight and enforcement pressure, but also technical guidance, cybersecurity awareness, workforce training, sectoral support mechanisms, and phased remediation planning if the maturity model is to strengthen actual national cyber resilience rather than merely produce compliance documentation.

APPENDIX 2

2. NATIONAL GUIDELINES FOR EMERGING TECHNOLOGY RISK MANAGEMENT

2.1. Purpose

These national guidelines establish a technology neutral approach for assessing and managing risks arising from emerging technologies used in support of critical services, public administration, and other essential national functions. They complement the National Cybersecurity Risk Management Framework and are intended for all public and private organizations that own or operate critical information infrastructure or other systems of national importance. The guidelines apply to any "emerging technology" that introduces new or significantly changed digital capabilities, architectures, or dependencies, including but not limited to data-intensive systems, automated decision-support tools, pervasive sensing, autonomous systems, and integrated cloud-based platforms. They are designed so that the same principles remain valid as new technologies appear over time.

2.2. Guiding principles

National risk management for emerging technologies should be guided by the following principles:

1. Technology neutrality through focus on governance, risk and assurance outcomes, not on specific products, vendors, or technical designs.
2. Risk-based proportionality through oversight and controls increasing with the criticality of services, sensitivity of data, level of autonomy, and potential national impact.
3. Lifecycle orientation to ensure risk management covers the entire lifecycle from concept and procurement through design, implementation, operation, change, and decommissioning.
4. Governance led management to ensure highest decision making body approves risk appetite, major deployment decisions, and residual risk acceptance for high-impact technologies.
5. Evidence-based assurance where organizations must be able to demonstrate how risks are identified, assessed, treated, and monitored using documented artefacts (risk registers, assessments, test results, incident records, audit findings).
6. Secure-by-design and by default where security and resilience considerations are embedded into planning and design rather than added late in the lifecycle.
7. Human accountability where responsibility for the use and consequences of emerging technologies remains with accountable human decision-makers.

2.3. Definitions and classification

Each organization should maintain a working definition of "emerging technology" for internal use that reflects these guidelines and its own context. At minimum, a deployment should be classified as emerging technology if it:

1. Introduces new or significantly altered digital capabilities, architectures, or dependencies in core services.
2. Increases automation, connectivity, or data intensity in ways that materially change the risk profile.
3. Relies heavily on external platforms, vendors, or complex ecosystems that are not yet fully understood or proven in the local context.

Organizations should classify emerging technology uses into risk tiers based on factors such as service criticality, data sensitivity, scale of impact, and degree of autonomy. Higher tiers trigger stricter governance, assessment and assurance expectations.

2.4. Governance and accountability

The highest decision-making body of each critical infrastructure operator (Board, Executive Committee, or equivalent) should own and oversee emerging technology risk management. This body should approve the organization's emerging technology risk management policy, set risk appetite, and endorse residual risks for high impact deployments. Each emerging technology deployment should have clearly designated roles cutting across a business owner, a technical owner, and a risk owner. These roles must be responsible for ensuring that the guidelines are applied consistently, that risk assessments are carried out, that treatment plans are implemented, and that incidents are escalated appropriately.

2.5. Lifecycle based risk management

Emerging technologies should be managed using the same core steps outlined in the National Cybersecurity Risk Management Framework, extended across the full technology lifecycle.

2.5.1. Concept and design

Before approving any major emerging-technology initiative, organizations should:

1. Describe the intended purpose, benefits, and affected services.
2. Analyze the external and internal context using the framework's perspectives (e.g. threat environment, legal obligations, organizational capabilities).
3. Identify high-level risks and dependencies, including reliance on third parties or external infrastructure.
4. Decide whether the proposed deployment is consistent with the organization's risk appetite and national expectations for critical infrastructure.

2.5.2. Development

During development, organizations should:

1. Define security and resilience requirements in specifications, contracts, and acceptance criteria.
2. Require suppliers and partners to support risk management obligations (for example, by providing documentation, assurance reports, and incident notification).
3. Identify key architectural choices and control points where risk can be reduced through design (segmentation, monitoring, logging, fail-safes, etc.).

2.5.3. Deployment and operation

Before production deployment, a documented risk assessment must be conducted using the national framework's structure (asset identification, threat and vulnerability analysis, risk evaluation and prioritization). The assessment should explicitly consider how the new technology changes the risk profile relative to existing systems.

In operation, organizations should:

1. Monitor performance, security, and resilience indicators relevant to the technology.
2. Maintain configuration and change records, including major updates, integrations, or parameter changes.
3. Ensure that staff understand their roles and the limitations of the technology in their processes.

2.5.4. Change and decommissioning

Major changes to emerging technology deployments (architecture changes, major feature introductions, migration to new platforms) must trigger a review of the risk assessment. Decommissioning should be planned to ensure that data, access credentials, configurations, and dependencies are handled securely and that residual risks are documented and, where relevant, removed.

2.5.5. Risk assessment structure

Emerging technology risk assessments should follow the structure of the National Cybersecurity Risk Management Framework but apply it in a technology-neutral way.

At minimum, an assessment should cover:

1. Context including objectives of the deployment, stakeholders, legal and regulatory considerations, and risk appetite.
2. Assets and dependencies including primary and supporting assets (data, systems, processes, people, third parties) and their relationships.
3. Threat sources and actors including insiders, external attackers, suppliers, integrators, service providers, and environmental threats.
4. Vulnerabilities and failure modes including weaknesses in governance, processes, technical design, configuration, supply chain, and human factors specific to the deployment.
5. Risk evaluation including likelihood and impact estimations, using the same risk criteria and scales as in the national framework.
6. Prioritization including ranking of risks and identification of those requiring treatment in the near term.

This structure allows the same methodology to be used for any emerging technology, whether it relates to analytics, automation, connectivity, sensing, or other functions.

2.5.6. Risk treatment for emerging technologies

Risk treatment options for emerging technologies should follow the national methodology. These options include avoid, mitigate, transfer, or accept.

Each organization's emerging-technology risk treatment plan should specify the chosen option for each priority risk, the actions to be taken, responsible parties, and target dates, and should be integrated with the broader risk management plan required under the framework.

2.6. Monitoring, incident response, and learning

Emerging technology deployments should be subject to ongoing monitoring and incident management consistent with the national framework. Monitoring should track performance and security indicators that would reveal deterioration, misuse, or unexpected behavior in the technology. Incident response plans should consider technology specific failure modes and define how to contain, recover, communicate, and, where necessary, temporarily suspend or roll back the deployment. Lessons learned from incidents, near misses, audits, and exercises should feed back into updated risk assessments, improved design choices, and refined governance arrangements.

This creates a continuous improvement loop that remains valid regardless of the technology in use.

2.7. Regulatory reporting and national oversight

For critical infrastructure operators, emerging-technology risk assessments and treatment plans should form part of the annual risk assessment submission to the National Communications Authority, as required by the framework. Operators should clearly identify which parts of their risk registers relate to emerging technologies and how these risks are being managed.

The NCA may use this information to:

1. Monitor systemic dependencies on particular emerging technologies or vendor ecosystems.
2. Identify recurring governance or risk management weaknesses across sectors.
3. Issue guidance, recommendations, or, where necessary, directives to address high-impact risks.

Because the guidelines are technology neutral, this oversight model remains applicable as new technologies emerge, without frequent rewriting of core policy

APPENDIX 3

3. CHANGE MANAGEMENT STRATEGY

3.1. Preamble

Somalia's economic stability, public safety and national security increasingly depend on digital systems and interconnected networks that support critical infrastructure. These systems are exposed to a widening range of threats. Based on this, the Somalia National Cybersecurity Risk Management Framework establishes the official, riskbased method that all Critical Infrastructure (CI) operators must use to identify, analyse, evaluate and treat cybersecurity risks to confidentiality, integrity and availability. This is line with the Somalia Cybersecurity Act that requires regular and systematic risk assessments and mandates that CI operators submit annual reports to the National Communications Authority (NCA) for oversight and coordination. Failure to comply may trigger enforcement measures under provisions such as Article 20 on noncompliance with obligations, with potential fines and other sanctions. At the same time, critical infrastructure operators may face several resource constraints that my slow implementation. This strategy therefore sets out the change management programme for the NCA to support national implementation of the framework. It acknowledges resource constraints and uneven maturity across operators but maintains a clear position that cybersecurity for critical infrastructure is a public interest obligation and a shared responsibility between Government, regulators, CI operators and the wider ecosystem.

3.2. Context

3.2.1. Vision

The vision for the change management strategy is that all designated CI operators adopt a common, systematic approach to cybersecurity risk management, anchored in the National Cybersecurity Risk Management Framework. By the end of the first two years after the framework's launch, each operator's board or top management should:

1. Understand its critical information assets and security domains.
2. Have a documented and approved risk appetite for information and cyber risk.
3. Use the national method to identify threat sources, threat actors, vulnerabilities and risk levels.
4. Approve and oversee risk treatment plans and residual risk acceptance, with annual submissions to the NCA.

At national level, NCA will consolidate operator submissions into a coherent view of sectoral and crosssector risks, prioritised by business impact categories such as security and defense, law enforcement and public order, public services and critical utilities and banking and public finance.

3.2.2. Urgency

The urgency stems from three converging pressures:

1. Threat escalation. The framework recognises capable and motivated threat sources each with distinct capability and motivation profiles. Their ability to exploit vulnerabilities in CI systems has grown faster than local defensive capacity.
2. Structural vulnerabilities. The framework highlights vulnerabilities across governance, processes, personnel, physical environment, system configuration and supply chains, including reliance on third parties and system integrators that may themselves be targeted.
3. Legal obligations. The Cybersecurity

Act requires that CI operators conduct regular risk assessments using a formal, consistent, policyguided approach and submit annual assessments to the NCA, with penalties for noncompliance.

There is a risk that CI operators treat the framework as a narrow compliance requirement, generating lowquality risk registers that do not meaningfully improve resilience for the nation.

3.2.3. Shared responsibility

The framework and the Solaw position cybersecurity as a shared responsibility. NCA sets the methodology and supervises. Sector regulators contextualise and reinforce. CI boards assume primary accountability for risk and operators implement controls in their own environments. Threat sources have resources and capability beyond the capacity of any single operator. National resilience therefore depends on coordinated action, privileged information sharing, common risk language and mutually reinforcing regulatory expectations. The strategy emphasises that resource constraints do not remove obligations.

3.2.4. Stakeholder mapping and segmentation

3.2.5. Stakeholder categories

NCA will segment CI operators into categories to tailor interventions. Within each category, NCA will map the following:

» Current cyber maturity (using the fivelevel national maturity model).

» Dependency on outsourced ICT and security functions.

» Exposure to specific threat sources and actors as described in the framework (e.g., high exposure to foreign intelligence services for telecoms, high exposure to organized crime for financial services).

3.2.6. Talent and cost gap analysis

The talent and cost gap are not uniform as shown below:

1. Banks and telecom operators generally employ dedicated security staff and have experience with risk management and audit processes. Their main challenge is integrating the national method into existing frameworks and avoiding duplicate reporting.
2. Utilities and some enterprises are managed by small ICT teams focused on operations rather than security, with limited capacity to perform structured risk assessments across complex OT and IT environments.
3. Sub national and smaller CI operators may have no dedicated security staff at all, relying fully on vendors or general IT support. These entities are most likely to claim inability to comply or inability to hire, making them priority targets for shared services and practical, low cost options.
4. Suppliers and integrators are explicitly recognised as threat actors with significant capability and motivation to affect CI via the supply chain, but they can also be key partners in delivering controls and monitoring.

This segmentation will inform the communication, training, capacity building and enforcement approaches described later in the strategy.

3.3. Governance

3.3.1. National governance

At national level, the following roles and structures have been identified:

Structure	Role
NCA management	a) Approves the national framework and this change strategy b) Sets expectations for compliance timelines and enforcement posture. c) Receives annual, consolidated national risk and maturity reports.
NCA Cybersecurity Directorate	a) Owns the framework's interpretation, guidance and templates b) Leads the change programme and manages stakeholder engagement c) Coordinates with SOM CIRT and sector regulators on implementation priorities and responses to major incidents.
SOMCIRT	a) Provides threat intelligence aligned to the framework's threat sources and attack methods (e.g., specific campaigns by hacktivists organized crime or foreign intelligence services) b) Coordinates incident reporting and response across CI, linking incident data back to identified risks and vulnerabilities.

Table 18: National Governance

3.3.2. Sector regulatory coordination

To avoid fragmented requirements and compliance fatigue, the NCA will establish a cyber risk coordination forum. This forum will be chaired by NCA, with participation from financial, telecom, energy, transport, health and other relevant regulators. The main responsibilities include the following:

1. Adopt the framework's core definitions, business impact categories, threat and risk levels as common reference points.
2. Align sector specific regulations to the national framework
3. Coordinate supervisory planning so operators receive coherent, sequenced requests rather than overlapping assessments and audits.

3.3.3. Operator level governance

The highest decision-making body for each CI operator must own and approve the risk treatment methodology and annual risk assessment outputs, including residual risk acceptance. In addition, a named senior executive (e.g., Chief Risk Officer, CIO or equivalent) should be appointed as the accountable cyber risk owner responsible for coordinating assessments, treatment plans and submissions to NCA. Internal governance should ensure that asset owners, system owners and process owners participate in risk identification and valuation, consistent with the framework's definition of assets and asset ownership. NCA will make board level accountability mandatory and will require evidence of board approval with each annual submission. Where an operator lacks a Board, top management will take full accountability for compliance.

3.4. Phased communication and change

roadmap

The roadmap is structured into three phases.

3.4.1. Phase one focusing on awareness and mobilization

The duration will be six months to:

1. Create broad awareness of the framework, legal obligations and the twenty four month transition period.
2. Secure visible commitment from CI boards/ top management and sector regulators.
3. Establish basic understanding of core concepts.

To this end, NCA will undertake the following:

1. Formal launch:

» Joint press conference and circulars from NCA and relevant ministries.

» Publication of the framework to designated CI operators.

b) Sector engagement

» • Sector specific launch events (financial, telecom, energy, transport, health) cohosted with sector regulators.

» • Presentation of case scenarios illustrating how threat sources and threat actors could impact CI, using examples from the framework.

c) Awareness materials

» Development of infographics, FAQs and short videos explaining the key terms as well as the steps of the risk assessment process outlined in the framework.

» Translation and adaptation into plain language versions where necessary.

The NCA will track and monitor the following milestones:

1. At least 90% of CI operators reached via direct communication by month three.
2. At least 70% of CI boards/top management have held a formal briefing on the framework and recorded a resolution committing to implementation by month six.

3.4.2. Phase two focusing on deep implementation and support

The duration will be twelve months to:

1. Equip CI operators with the knowledge, tools and support needed to perform risk assessments and design treatment plans.
2. Develop local capacity through training and Centres of Excellence.
3. Pilot and refine implementation approaches.

To this end, NCA will undertake the following:

1. Provision of implementation support with guidance on interpreting the threat levels table, capability/motivation scales and risk levels matrix.
2. Training programmes including these:

» Executive training for boards and senior executives covering governance responsibilities, risk appetite and supervision of cyber risk.

» Practitioner training for risk, ICT and security staff on applying the framework.

3. Support channels:

» Establish a cyber risk support desk (email, portal, hotline) at SOMCIRT.

» Publish anonymised examples of goodquality asset catalogues, domain models and risk registers.

The NCA will track and monitor the following milestones:

» At least 60% of operators have trained staff in the methodology by month 12.

» At least 50% of operators have completed a first full cycle of risk assessment and drafted treatment plans by month 18.

3.4.3. Phase three focusing on validation and optimization

The duration will be five months to:

1. Validate quality and consistency of risk assessments.
2. Embed the framework into regulatory and internal processes.
3. Establish a baseline national cyber maturity profile.

To this end, NCA will undertake the following:

1. Supervisory review and audits:
2. National maturity assessment using the five level national maturity model, NCA will score operators across domains such as governance, risk management, control implementation, incident response and supplychain security.
3. Institutionalisation through the following:

» Integration of annual risk assessment submissions into licensing and permit renewal processes for CI operators where applicable.

» Establishment of a supervisory cycle combining selfassessments, periodic independent reviews and targeted audits.

The NCA will track and monitor the following milestones:

1. At least 80% of operators have completed one full assessment cycle and implemented initial treatments by month 24.
2. Board/ top management level reporting on cyber risk becomes routine, with at least annual updates tied to framework outputs.

3.5. Capacity building and resource strategy

3.5.1. Addressing the talent gap

3. NCA will establish National Cybersecurity Academy (NCSA) to:

» Provide domainspecific implementation guidance grounded in the national framework.

» Host communities of practice and peerlearning sessions.

» Support smaller operators through shared workshops and clinics.

» The CoEs shall coordinate with SOMCIRT to ensure alignment with national threat intelligence and policy directions.

4. NCA will establish an accredited expert pool through the development of the criteria and a certification process for cybersecurity service providers who demonstrate proficiency in applying the framework. CI operators may engage these providers (from local firms, larger operators or individual consultants) to support assessments, with assurance of common methodology and quality.
5. SOMCIRT will operate national platforms for:

» Threat intelligence sharing, with indicators and advisories categorised according to threat sources (e.g. organized criminal syndicates, extremist organizations), motivations and targeted security properties (confidentiality, integrity, availability).

» Incident reporting and coordination, structured in ways that feed back into risk assessments and continuous improvement.

3.6. Resistance management

3.6.1. Anticipated resistance

The following resistance patterns are anticipated:

1. Cost objections where operators argue that tools, external consultants or dedicated staff are unaffordable.
2. Talent objections where operators claim they cannot hire or retain cybersecurity staff.
3. Complexity objections where operators perceive the framework as too complex or for large organizations only.
4. Competing priorities where operators prioritise other regulatory or business initiatives and delay implementation.

3.6.2. Principles for managing resistance

1. Clear communication of the following:

» Annual risk assessment and submission to NCA using the national methodology, including coverage of assets, security domains, threats, vulnerabilities and risk levels.

» Board level approval of the methodology, risk appetite, treatment plans and residual risk acceptance.

» Implementation of basic controls for high risk areas identified in the risk assessment.

b) Structured flexibility in the following:

» How operators organize their internal teams (dedicated vs. shared roles).

» Flexibility in the use of shared services, CoEs or accredited experts.

» Flexibility in sequencing lower impact controls, provided that risk based rationale is documented.

c) Operators claiming inability to comply shall submit the following:

» A partial risk assessment demonstrating at least initial effort.

» A capacity improvement plan indicating how they will use CoEs, expert pools or SECaaS solutions to close gaps.

d) Establish incentives and sanctions as noted below:

» Positive incentives through public recognition of early adopters and leaders.

» Sanctions using graduated measures from warnings and binding directives to administrative penalties and legal enforcement in line with relevant provisions (e.g. Article 20 on noncompliance).

3.7. Monitoring metrics

3.7.1. Change process indicators

NCA will track the following key performance indicators:

1. Percentage of CI operators that received formal notification and launch materials.
2. Percentage of operators whose boards/ top management have issued formal resolutions committing to implementation.
3. Number of staff trained by sector and role
4. Percentage of operators that completed at least one full risk assessment cycle by month 18.

3.7.2. Technical and maturity indicators

Building on the national five level maturity model, NCA will also track:

» Percentage of high-risk items implemented controls before the next assessment cycle.

» Frequency and impact of major incidents affecting confidentiality, integrity or availability and whether they relate to previously identified risks.

NCA will consolidate findings into an annual national report to inform policymakers, sector regulators and CI operators and to guide refinement of the framework, capacity building priorities and regulatory measures.

References

This Standard is consistent with the risk management approach contained in the ISO/IEC series of standards. The following standards are particularly relevant:

5. IEC/ISO 31010 - Risk Management – Risk Assessment Techniques, International Electrotechnical Commission (IEC), Geneva, Switzerland.
6. ISO 31000 - Risk Management — Principles and Guidelines, International Standards Organization (ISO), Geneva, Switzerland.
7. ISO Guide 31073 - Risk Management — Vocabulary, International Standards Organization (ISO), Geneva, Switzerland.
8. ISO/IEC 27005 - Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, International Standards Organization (ISO)/International Electrotechnical Commission (IEC), Geneva, Switzerland.
9. ISO/IEC 27001 - Information Technology — Security Techniques — Information Security Management Systems — Requirements, International Standards Organization (ISO)/ International Electrotechnical Commission (IEC), Geneva, Switzerland.
10. ISO/IEC 27003: 2017 - Information Technology — Security Techniques — Information Security Management System implementation guidance, International Standards Organization (ISO) /International Electrotechnical Commission (IEC), Geneva, Switzerland.
11. US ISO/IEC 27002 - Information Technology — Security Techniques — Code of Practice for Information Security Management, International Standards Organization (ISO)/ International Electrotechnical Commission (IEC), Geneva, Switzerland.
12. ISO/IEC 27005- Information Technology — Security Techniques — Information Security Risk Management, International Standards Organization (ISO)/International Electrotechnical Commission (IEC), Geneva, Switzerland.
13. ISO/IEC 27007- Information Technology — Security Techniques — Guidelines for Information Security Management Systems Auditing, International Standards Organization (ISO)/ International Electrotechnical Commission (IEC), Geneva, Switzerland.

Hay'adda Isgaarsiinta Qaranka
الـهيئـة الوطنيـة للإتـصالات
National Communications Authority

NATIONAL CYBERSECURITY RISK MANAGEMENT FRAMEWORK