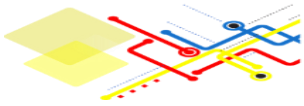
Information Network Security Administration

Critical Infrastructure Sector Designated Standard

Version 1.0



2026

Document Control

I. Document Information

NO	Element	Description
1	Document title	Critical Infrastructure and Sectors Designation Standard
2	Document Reference Number	
3	Version	1.0
4	Publication Date	August, 2026
5	Issuing Authority	Information Network Security Administration

II. Version History

Version	Date	Author / Owner	Summary of Changes
1.0			

Forward

The resilience of Critical Infrastructure is fundamental to the security, sovereignty, economic prosperity, and sustainable development of the country. The essential infrastructure, systems, services, assets, and operational capabilities that support the functioning of the country, the economy, and society are indispensable to the well-being of the nation and the daily lives of its citizens. Their continued operation, security, and resilience are therefore matters of national importance.

As Ethiopia accelerates its digital transformation and the adoption of emerging technologies, the interconnection between physical and digital infrastructure continues to grow. While this transformation creates significant opportunities for innovation and development, it also increases exposure to cyber threats and other risks that can disrupt essential services and undermine national resilience. Protecting Critical Infrastructure has therefore become a strategic national priority requiring a coordinated, risk-based, and whole-of-government approach.

This Standard establishes the national framework for the identification, assessment, classification, designation, and periodic review of Critical Infrastructure. By providing objective criteria, consistent assessment methodologies, and clear governance arrangements, it promotes transparent and evidence-based decision-making while ensuring a harmonized approach to Critical Infrastructure designation across the country.

The protection of Critical Infrastructure is a shared responsibility. Its success depends upon effective collaboration among government institutions, sector regulatory bodies, Critical Infrastructure owners and operators, private sector organizations, and all other relevant stakeholders. Through collective commitment, strong governance, and continuous cooperation, we can strengthen the resilience of our nation's most essential infrastructure and ensure the continuity of services upon which our security, economy, and society depend.

The Information Network Security Administration is committed to working closely with all stakeholders to implement this Standard and to continually strengthen Ethiopia's Critical Infrastructure resilience in response to emerging risks and evolving national priorities. I encourage every responsible institution and organization to apply this Standard diligently and consistently in

fulfilling our shared responsibility to safeguard the nation's essential infrastructure for the benefit of present and future generations.

Together, we will build a resilient, secure, and trusted Critical Infrastructure ecosystem that supports national stability, protects our strategic interests, and contributes to a prosperous and digitally secure Ethiopia.

List of table

Table 1 Recognized Critical Infrastructure Sectors ____ *16*
Table 2 Dimension Weights (W) and Scoring Baselines ____ *34*
Table 3 Classification Thresholds ____ *34*
Table 4 Key Activities in the Identification Phase ____ *40*
Table 5 Key Activities in the Screening Phase ____ *41*
Table 6 Key Activities in the Assessment Phase ____ *42*
Table 7 Key Activities in the Designation Phase ____ *43*
Table 8 Key Activities in the Registration and Review Phase ____ *44*
Table 9: Periodic Review Cycle ____ *47*

List of figures

Figure 1 Critical Infrastructure Selection Process ____ *39*

Acronyms and Abbreviations

Acronym / Abbreviation	Full Name
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CICS	Critical Infrastructure Cybersecurity
CS	Criticality Score
FDRE	Federal Democratic Republic of Ethiopia
ICT	Information and Communication Technology
OT	Operational Technology
ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
IT	Information Technology
IoT	Internet of Things
IIoT	Industrial Internet of Things
SOC	Security Operations Center
MSSP	Managed Security Service Provider
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
INSA	Information Network Security Administration
NBE	National Bank of Ethiopia
GDP	Gross Domestic Product
RTO	Recovery Time Objective
RPO	Recovery Point Objective
BCM	Business Continuity Management
BCP	Business Continuity Plan
DR	Disaster Recovery
DRP	Disaster Recovery Plan
RMF	Risk Management Framework
GRC	Governance, Risk, and Compliance
ISO	International Organization for Standardization
IEC	International Electro technical Commission

ISO/IEC	International Organization for Standardization / International Electro technical Commission
NIST	National Institute of Standards and Technology
CIA	Confidentiality, Integrity, and Availability
DDoS	Distributed Denial of Service
DoS	Denial of Service
TI	Threat Intelligence
TTPs	Tactics, Techniques, and Procedures
SLA	Service Level Agreement
KPI	Key Performance Indicator
KRI	Key Risk Indicator
OT	Operational Technology
AI	Artificial Intelligence
ML	Machine Learning
API	Application Programming Interface
WAN	Wide Area Network
LAN	Local Area Network
VPN	Virtual Private Network
DNS	Domain Name System
IP	Internet Protocol
SD-WAN	Software-Defined Wide Area Network
Cloud	Cloud Computing Environment
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
PDPP	Personal Data Protection Proclamation
MoU	Memorandum of Understanding
SLA	Service Level Agreement
CSO	Chief Security Officer
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CEO	Chief Executive Officer
TCO	Total Cost of Ownership

Contents

Forward iii
PART I - General 1
1.1. Introduction 1
1.2. Objective 2
1.2.1. General Objective 2
1.2.2. Specific Objectives 2
1.3. Scope 3
1.3.1. Coverage 3
1.3.2. Scope of Applicability 3
1.4. Normative References 3
1.5. Legal Basis 4
1.6. Definitions 4
1.6.1. General 4
1.6.2. Additional Definitions 4
PART II - Roles and Responsibilities 7
2.1. Information Network Security Administration 7
2.2. Sector Regulatory Bodies 7
2.3. Independent Organizations 8
2.4. Organizations within Regulated Sectors 9
PART III - Sector Requirement and Critical Infrastructure Domains 11
3.1. Overview 11
3.2. Sector Requirement Principles 11
3.2.1. General Principle 11
3.2.2. Sector Eligibility Requirements 12
3.3. Recognized Critical Infrastructure Sectors 13
PART IV - Critical Infrastructure Designation 17
3.1. Overview 17
3.2. Designation Principle 17
3.3. Criticality Assessment Criteria 18
4.4. Critical Infrastructure Classification Levels 29
4.4.1. Overview 29
4.4.2. Objective 29
4.4.3. The 3- Categories Classification Model (Asset Levels) 29
4.4.4. Classification Determination 31
4.4.5. Criticality Score 32
4.4.6. Dimension Weights (W) and Scoring Baselines 32

4.4.7. Classification Thresholds and Determination 34
4.4.8. Practical Implementation Methodology 37
4.4.9. Classification Review 37
4.4.10. Relationship to Designation 37
4.5. Critical Infrastructure selection Process 39
4.6. Critical Infrastructure Selection Process Description 39
PART V - Review, Reassessment, and Reclassification 45
5.1. General Principles 45
5.2. Objectives 45
5.3. Reassessment Triggers 46
5.4. Periodic Review Cycle 47
5.5. Scope of Reassessment 48
5.6. Reassessment Methodology 49
5.7. Reclassification 49
5.8. De-designation 50
5.9. Notification of Decisions 50
5.10. Recordkeeping and Documentation 50
5.11. Continuous Monitoring 51
PART VI - Compliance and Continuous Improvement 52
6.1 Compliance 52
6.2 Compliance Monitoring 52
6.4 Non-Compliance Management 52
6.5 Continuous Improvement 53
6.6 Review of the standard 54
Annex A: Criticality Assessment Checklist 56
Annex B: Sample Criticality Assessment Calculation 61
B.1 Criticality Assessment Methodology 61
B.2 Assessment Criteria and Weight 62
B.3 Impact Assessment 63
B.4 Criticality Percentage Calculation 63
B.5 Criticality Classification 64

PART I - General

1.1. Introduction

Critical Infrastructure constitutes the foundation upon which national security, economic prosperity, public safety, government continuity, and societal well-being depend. Modern societies rely on a complex and highly interconnected network of organizations, systems, facilities, services, technologies, and operational capabilities that enable the delivery of essential functions necessary for the daily lives of citizens and the effective operation of government and industry.

The increasing digitalization of critical services, the expansion of interconnected technologies, and the growing sophistication of cyber threats have significantly increased the vulnerability of critical infrastructure to disruption. Cyber-attacks, system failures, natural disasters, human error, supply chain disruptions, and other emerging threats can have far-reaching consequences that extend beyond individual organizations and affect multiple sectors simultaneously. Such disruptions may result in economic losses, interruption of essential services, threats to public safety, compromise of national security, and erosion of public confidence.

Effective Critical Infrastructure protection begins with the accurate identification and designation of organizations whose services, assets, systems, or operations are of national significance. A clear and consistent methodology is therefore necessary to ensure that Critical Infrastructures is identified based on objective criteria, measurable impacts, and national priorities. Such an approach enables government institutions, regulators, and infrastructure operators to effectively allocate resources, enhance resilience, strengthen preparedness, and implement appropriate cybersecurity, risk management, and protection measures.

This Standard establishes the national framework for identifying, assessing, classifying, and designating Critical Infrastructure Organizations. It provides a structured, transparent, and risk-based methodology that considers the potential consequences of disruption, the essentiality of services provided, sector interdependencies, and the broader impact on national interests. The Standard further supports the implementation of the Critical Infrastructure Cybersecurity

Proclamation and aligns with internationally recognized principles, standards, and best practices for Critical Infrastructure Cybersecurity and resilience.

By establishing a common framework for Critical Infrastructure designation, this Standard promotes consistency across sectors, enhances coordination among stakeholders, strengthens national cybersecurity governance, and contributes to the protection of essential services that are vital to the security, stability, and sustainable development of the nation.

1.2. Objective

1.2.1. General Objective

The general objective of this Standard is to establish a structured, consistent, and risk-based methodology for the identification, assessment, classification, and designation of Critical Infrastructure and Sectors whose disruption, destruction, compromise, or unavailability may result in significant adverse consequences to national security, economic stability, public safety, government continuity, or societal well-being.

1.2.2. Specific Objectives

This Standard aims to:

- Establish nationally consistent criteria for identifying Critical Infrastructure and Sectors;
- Provide a transparent and evidence-based mechanism for Critical Infrastructure and designation;
- Support the implementation of the Critical Infrastructure Cybersecurity Proclamation;
- Enable risk-informed decision-making for cybersecurity protection and resilience planning;
- Identify Critical Infrastructures whose services are essential to the functioning of the nation;

1.3. Scope

1.3.1. Coverage

This Standard covers the key elements required for the effective implementation of the Critical Infrastructure cybersecurity proclamation. These include sector eligibility determination, criticality assessment criteria, organizational evaluation and classification, designation decision-making processes, roles and responsibilities, as well as mechanisms for periodic review and updating

1.3.2. Applicability

This Standard applies to all sectors and organizations that are designated, or subject to designation, as Critical Infrastructure in accordance with the Critical Infrastructure Cybersecurity Proclamation, including public institutions, state-owned enterprises, private organizations, operators of essential services, and other entities that own, operate, manage, control, or support infrastructure, systems, assets, or services that have been designated, or are determined to be eligible for designation, as Critical Infrastructure under the Proclamation.

1.4. Normative References

- FDRE Critical Infrastructure Cybersecurity Proclamation No 1426/2018
- FDRE National Cyber Security Policy and Strategy (2021)
- Digital Ethiopia 2030 Strategy (FDRE Office of the Prime Minister)
- Personal Data Protection Proclamation No. 1321/2024
- Computer Crime Proclamation No. 958/2016
- Communications Service Proclamation No. 1148/2019
- National Payment System Proclamation No. 718/2011, as amended by Proclamation No. 1282/2023
- National Bank of Ethiopia IT Management Directives for banks and insurers (SBB/83/2022 and SIB/56/2022)
- Energy Proclamation No. 810/2013 and related Ethiopian Energy Authority frameworks.

1.5. Legal Basis

This Standard is issued under the authority of the Critical Infrastructure Cybersecurity Proclamation No. 1426/2018 and serves as the national methodology for identifying and designating Critical Infrastructure Sectors and Organizations.

In accordance with the Proclamation:

a. The Administration shall designate Critical Infrastructure susceptible to cyber-attacks requiring protection under the Proclamation;
b. The designation shall be based on cybersecurity risk impact assessments, relevant frameworks, international best practices, and national requirements;
c. Organizations designated as Critical Infrastructure shall be entitled to cybersecurity protection and oversight in accordance with applicable laws, directives, standards, and regulations.

1.6. Definitions

1.6.1. General

Unless otherwise specified in this Standard, terms and definitions expressly defined under the Critical Infrastructure Cybersecurity Proclamation shall have the same meaning and interpretation when used in this Standard.

1.6.2. Additional Definitions

For the purposes of this Standard, the following terms and definitions shall apply:

1. **"Critical Infrastructure"** any infrastructure or institution the disruption or compromise of which due to a cyber-attack would have a significant negative impact on national security or national interests, including data, critical systems, networks, services, functions, facilities, information, technologies, and supporting resources that are essential to the continuity, security, and effective operation of such infrastructure or institution.

2. **"Critical Infrastructure Sector"** A sector recognized under Critical Infrastructure Cybersecurity Proclamation No 1426/2018 as providing essential services, functions, or capabilities whose disruption may significantly affect national security, economic stability, public safety, government continuity, societal well-being, or other Critical Infrastructure sectors.
3. **"Designation"** The formal process through which an organization is assessed and officially recognized as a Critical Infrastructure Organization by the Administration in accordance with the requirements of this Standard.
4. **"Interdependency"** The condition whereby the operation, performance, availability, or continuity of one organization, system, service, or sector relies upon another organization, system, service, or sector.
5. **"Cascading Impact"** The propagation of disruption from one organization, system, service, or sector to multiple interconnected organizations, systems, services, or sectors, resulting in broader national consequences.
6. **"Essential Service"** A service, function, or capability whose continuous availability is necessary to maintain national security, public safety, economic activity, government operations, public welfare, or societal stability.
7. **"National Consequence"** The direct or indirect impact resulting from disruption, degradation, destruction, compromise, or unavailability of an organization, system, or service that affects national security, economic stability, public safety, government continuity, societal well-being, or national resilience.
8. **"Sector Lead Authority"** The government institution, regulatory body, or competent authority assigned responsibility for coordinating Critical Infrastructure identification, assessment, and sector-specific designation activities within a particular Critical Infrastructure sector.
9. **"Criticality Assessment"** The structured process of evaluating an organization against the Critical Infrastructure Classification Criteria established under this Standard to determine its level of national significance and eligibility for designation as Critical Infrastructure.
10. **"Criticality Criteria"** The consequence-based assessment factors established under this Standard and used to determine whether an organization qualifies for Critical Infrastructure designation.

11. **"National Critical Infrastructure Registry"** The official record maintained by the Administration containing organizations formally designated as Critical Infrastructure under the Proclamation and this Standard.

PART II - Roles and Responsibilities

2.1. Information Network Security Administration

The Administration shall serve as the national authority responsible for implementing this Standard. The Administration shall:

a. Develop, maintain, and periodically update the Critical Infrastructure Organization Selection Standard;
b. Establish assessment methodologies, procedures, and supporting guidance;
c. Coordinate national Critical Infrastructure identification and designation activities;
d. Review and approve Critical Infrastructure designation recommendations;
e. Designate, reclassify, suspend, or revoke Critical Infrastructure status;
f. Maintain the National Critical Infrastructure Registry;
g. Conduct oversight, monitoring, and compliance verification activities;
h. Coordinate national Critical Infrastructure risk assessments;
i. Issue directives, guidelines, and implementation procedures necessary to apply this Standard.

2.2. Sector Regulatory Bodies

Sector Regulatory Bodies shall support the Administration in implementing this Standard within their respective sectors. Their responsibilities include:

a. Support the identification of organizations, services, systems, and assets that may qualify as Critical Infrastructure within their respective sectors.
b. Provide sector-specific information, technical expertise, and regulatory input to support the identification, assessment, designation, classification, and review of Critical Infrastructure.
c. Validate relevant information and evidence submitted during Critical Infrastructure assessments.

d. Recommend organizations for designation, reclassification, review, or de-designation, where appropriate.
e. Support the Administration in conducting assessments, inspections, verification, and monitoring activities within their respective sectors.
f. Facilitate coordination and communication between the Administration and organizations within their regulatory jurisdiction.
g. Share relevant information on sector risks, dependencies, incidents, and significant changes that may affect the criticality of organizations, services, systems, or assets.
h. Participate in consultation, review, and decision-support activities related to Critical Infrastructure designation and classification.
i. Support the periodic review and reassessment of designated Critical Infrastructure within their respective sectors.
j. Promote awareness and compliance with applicable Critical Infrastructure cybersecurity requirements within their respective sectors.
k. Cooperate with the Administration and other competent authorities to ensure the effective implementation of this Standard.
l. Perform any other responsibilities assigned under the Proclamation, this Standard, or other applicable laws.

2.3. Independent Organizations

Independent Organizations, being organizations operating in sectors or areas where no Sector Regulatory Body has been designated, shall have the responsibilities applicable to Organizations within Regulated Sectors, in addition to the following responsibilities specific to their status as Independent Organizations:

a. Coordinate directly with the Administration on the identification, assessment, designation, classification, review, and cybersecurity matters of Critical Infrastructure.
b. Submit required sector, organizational, technical, operational, and other relevant information directly to the Administration in the absence of a Sector Regulatory Body.

c. Facilitate and cooperate directly with the Administration in assessments, inspections, verification, monitoring, and other regulatory activities.
d. Notify the Administration directly of significant changes in organizational structure, ownership, services, systems, assets, technologies, dependencies, or operations that may affect Critical Infrastructure designation or classification.
e. Participate directly with the Administration in consultations, periodic reviews, reassessments, and other activities relating to Critical Infrastructure.
f. Maintain an appropriate point of contact responsible for coordinating Critical Infrastructure matters directly with the Administration.
g. Perform any additional responsibilities assigned by the Administration in accordance with the Proclamation, this Standard, or other applicable laws.

2.4. Organizations in Regulated Sectors

Organizations operating within sectors having a designated Sector Regulatory Body shall comply with the requirements of this Standard and cooperate with the relevant Sector Regulatory Body and the Administration. Their responsibilities include:

a. Provide accurate and complete information and evidence required for Critical Infrastructure identification, assessment, designation, classification, and review.
b. Participate in Critical Infrastructure assessments, inspections, verification, monitoring, and reassessment activities.
c. Implement applicable Critical Infrastructure cybersecurity requirements and maintain appropriate cybersecurity and resilience measures.
d. Report significant cybersecurity incidents, risks, dependencies, and changes that may affect the criticality or continuity of essential services and functions.
e. Maintain relevant records, documentation, and evidence demonstrating compliance with applicable requirements.
f. Cooperate with the Sector Regulatory Body, the Administration, and other competent authorities in the implementation of this Standard.
g. Participate in consultations, reviews, and other activities relating to Critical Infrastructure designation, classification, and reassessment.

h. Perform any other responsibilities assigned under the Proclamation, this Standard, or other applicable laws.

PART III - Sector Requirement and Critical Infrastructure Domains

3.1. Overview

In accordance with Article 4(1) of the Critical Infrastructure Cybersecurity Proclamation, the Administration hereby recognizes a set of Critical Infrastructure sectors that form the foundation of Ethiopia's national security, economic stability, public safety, and social well-being. These sectors represent the national ecosystem of essential services and constitute the primary domains within which Critical Infrastructure Organizations may be identified and designated.

The purpose of defining sector requirements is to establish a structured national classification boundary for criticality assessment. Sector inclusion does not automatically confer Critical Infrastructure status; rather, it defines eligibility for assessment under Article 4(3).

In addition to the sectors explicitly stated in the Proclamation, the Administration recognizes that modern critical infrastructure is dynamic, digitally dependent, and interconnected, requiring inclusion of emerging and cross-cutting sectors that have become essential to national resilience.

3.2. Sector Requirement Principles

3.2.1. General Principle

The designation of Critical Infrastructure Organizations shall commence with the identification of eligible Critical Infrastructure sectors. A sector shall be included within the Critical Infrastructure domain where its disruption, degradation, destruction, compromise, or unavailability may result in significant adverse consequences to national security, economic stability, public safety, government continuity, societal well-being, or national resilience.

3.2.2. Sector Eligibility Requirements

A sector shall be eligible for designation as a Critical Infrastructure Sector where it meets one or more of the following requirements:

a. The sector provides services that are essential to national security, sovereignty, territorial integrity, constitutional order, or continuity of government.
b. The sector is fundamental to the stability and functioning of the national economy, including financial systems, trade, industrial production, or economic growth.
c. The sector provides services that are essential to public safety, human life, public health, or overall public welfare.
d. The sector delivers essential services required for the daily functioning of society, including energy, water, transportation, telecommunications, healthcare, or food supply.
e. The sector has strong interdependencies with other sectors such that its disruption can cause cascading or systemic national impacts.
f. The sector provides services on which a significant proportion of the population, government institutions, or private sector entities depend.
g. The sector provides services that are not easily substitutable or replaceable within an acceptable timeframe without significant national impact.
h. The sector is identified in national laws, policies, or strategic development plans as essential to national development or resilience.
i. The sector provides foundational enabling infrastructure that supports multiple other sectors, including physical, digital, or hybrid systems.
j. The sector must remain operational during emergencies or crises to ensure continuity of essential national functions.

3.3. Recognized Critical Infrastructure Sectors

No.	Critical Infrastructure Sector	Description	Criticality Rationale	Potential Impact of Disruption
1	Information and Communication Technology (ICT) and Telecommunications	Includes mobile networks, fixed-line communications, internet service providers, data centers, internet exchange points, cloud service providers, satellite communications, and national digital platforms.	Serves as the digital backbone of government, finance, transportation, emergency services, and national security operations.	May cause cascading failures across multiple sectors, disrupt communications, digital services, financial transactions, and government operations.
2	Financial Services	Includes banks and other financial service providers, payment service providers, payment switches and clearing systems, digital wallets and mobile/internet payment platforms, ATMs and POS networks, payment gateways, domestic card and instant payment systems, and other infrastructure and services supporting the national electronic payment ecosystem.	Supports monetary circulation, financial stability, payments, savings, investments, and economic activity.	May halt financial transactions, restrict access to funds, disrupt trade, reduce investor confidence, and create economic instability.
3	Security and Safety Services	Includes defense support systems, police services, intelligence systems, fire and rescue services, emergency communications, and command-and-control systems.	Protects national sovereignty, public safety, and emergency response capabilities.	May weaken defense and law enforcement capabilities, delay emergency response, and increase security risks.

4	Transport and Logistics	Includes aviation, railways, road transport, dry ports, logistics hubs, customs systems, freight operations, warehousing, and supply chain management systems.	Enables movement of goods, services, people, fuel, food, and medical supplies.	May disrupt supply chains, restrict mobility, and delay essential goods distribution, and negatively impact trade and economic activities.
5	Education and Research Infrastructure (Strategic Systems Only)	Includes national examination systems, academic certification systems, education management platforms, and strategic research infrastructure.	Supports human capital development, education continuity, and national innovation capacity.	May disrupt examinations, certification processes, academic progression, and research activities.
6	Health	Includes hospitals, clinics, laboratories, pharmaceutical supply chains, emergency medical services, health information systems, and public health surveillance platforms.	Protects human life, supports healthcare delivery, and safeguards public health.	May result in loss of life, interruption of medical services, disease outbreaks, and public health emergencies.
7	Water and Energy	Includes electricity generation, transmission and distribution systems, petroleum supply, renewable energy infrastructure, water supply systems, wastewater treatment, irrigation, and sanitation services.	Provides essential utilities that support all other critical sectors and public welfare.	May cause widespread service outages, affect public health, disrupt industrial activities, and trigger cascading impacts across sectors.
8	Government Services	Includes digital government platforms, identity management systems, taxation systems, civil registry systems, national	Supports governance, public administration, regulatory functions, and citizen services.	May impair government operations, disrupt public services, delay administrative

		databases, and administrative service delivery platforms.		processes, and reduce public trust.
9	Disaster Management Services	Includes disaster risk management institutions, emergency coordination systems, early warning systems, humanitarian platforms, and crisis management centers.	Supports preparedness, response, recovery, and coordination during disasters and emergencies.	May delay emergency response, increase loss of life, reduce resilience, and worsen disaster impacts.
10	Agriculture	Includes agricultural production systems, livestock systems, irrigation networks, agro-processing facilities, food storage, and food supply chains.	Ensures food security, rural livelihoods, and agricultural productivity.	May lead to food shortages, supply chain disruptions, inflation, and humanitarian challenges.
11	Trade	Includes wholesale and retail trade systems, import and export operations, commodity distribution networks, logistics hubs, and markets supporting the supply of essential goods and services.	Ensures the continuous distribution and availability of essential goods, supports domestic and international commerce, and contributes to economic stability.	May disrupt the supply of essential goods, interrupt domestic and international trade, create market shortages, increase prices, and negatively affect economic stability.
12	Industry	Includes manufacturing facilities and strategic industries such as pharmaceuticals, steel, cement, chemicals, fertilizers, and other industries essential to national development and economic resilience.	Supports industrial production, national development, strategic manufacturing capabilities, employment, and supply chain resilience.	May reduce industrial production, disrupt manufacturing operations and supply chains, limit the availability of essential products, and weaken national economic resilience.

Table 1 Recognized Critical Infrastructure Sectors

PART IV - Critical Infrastructure Designation

3.1. Overview

The Administration shall implement a consequence-based Critical Infrastructure Classification Standard to determine whether an infrastructure qualifies as Critical Infrastructure.

The designation shall be based on the severity of the national consequences that may result from the disruption, degradation, destruction, compromise, or unavailability of the infrastructure, particularly due to cyber-attacks, system failures, operational disruptions, natural hazards, or hybrid threats.

Critical Infrastructure shall not be designated solely based on sector affiliation, ownership, or the nature of the operating entity. Designation shall be determined through an assessment of the infrastructure's criticality, the essentiality of the services it supports, its dependencies and interdependencies, and the potential impact of its disruption on national security, economic stability, public safety, government continuity, societal well-being, and national resilience.

3.2. Designation Principles

A) Consequence-Based

Critical Infrastructure designation shall be guided by the potential consequences of disruption, degradation, destruction, compromise, or unavailability, particularly where such consequences could materially affect national security, the national economy, and public safety, continuity of government, societal well-being, or national resilience.

B) Impact and Cascading Effects

Designation shall be guided by a consequence-driven assessment that considers the scale, severity, duration, and potential cascading effects of disruption, including those arising from cybersecurity incidents and other disruptive events.

C) Essential Functions and Dependencies

Designation shall take into account whether infrastructure supports or enables essential national functions, provides indispensable services, or serves as a foundational dependency for other Critical Infrastructure. Where significant dependencies exist, the potential impact of even a short-term disruption shall be considered in determining criticality.

1. Critical Infrastructure shall be designated where its disruption, degradation, destruction, compromise, or unavailability would result in significant adverse consequences that materially affect national security, the national economy, public safety, government continuity, societal well-being, or national resilience.
2. Designation shall be based on a consequence-driven assessment that considers the scale, severity, duration, and cascading effects of the impact, particularly in relation to cyber incidents and other disruptive events.
3. In applying this principle, the Administration shall determine whether the infrastructure supports or enables essential national functions, delivers indispensable services, or serves as a foundational dependency for other Critical Infrastructure. Where such dependencies exist, even a short-term disruption may be sufficient to justify designation as Critical Infrastructure.

3.3. Criticality Assessment Criteria

4.3.1. Security Impact Criterion (National Stability and Sovereignty)

4.3.1.1. Objective

The Security Impact Criterion shall be used to assess whether the disruption, degradation, compromise, or unavailability of an organization's services, systems, assets, or operational capabilities could adversely affect the national security, sovereignty, territorial integrity, constitutional order, diplomatic interests, or continuity of the nation. This criterion shall identify organizations whose failure could result in consequences extending beyond organizational boundaries and create significant risks to national stability, governance, public security, or national resilience.

4.3.1.2. Assessment Requirements

An organization shall be assessed against this criterion to determine whether it performs functions or operates assets that are essential to national security or continuity of government and shall be considered to meet this criterion where one or more of the following conditions apply:

a. The organization provides services or capabilities that support national defense, security, or sovereignty.
b. The organization supports the continuity of government, executive decision-making, or constitutional functions during normal operations or national emergencies.
c. The organization operates or supports command, control, communication, intelligence, or strategic coordination systems used by government or national security authorities.
d. The organization provides essential capabilities for national emergency management, disaster response, or inter-agency crisis coordination.
e. The organization manages information, systems, or infrastructure whose compromise could significantly affect national security or governmental operations.
f. The organization provides services whose disruption could be exploited by hostile actors to undermine national security, public order, or state resilience.

4.3.1.3. Assessment Considerations

The assessment shall consider, where applicable:

a. National Defense and Sovereignty: The extent to which the organization supports military readiness, national defense capabilities, strategic assets, border protection, or territorial integrity.
b. Government Continuity: The extent to which the organization contributes to the uninterrupted operation of government institutions, executive leadership, constitutional authorities, or critical public administration functions.
c. Intelligence and National Security Operations: Whether the organization supports intelligence collection, analysis, information sharing, security coordination, or other national security functions.

d. **Emergency and Crisis Coordination:** The extent to which the organization contributes to disaster management, emergency response, civil protection, national incident coordination, or continuity of essential government services.
e. **Diplomatic and International Obligations:** The extent to which disruption of the organization's services could affect Ethiopia's diplomatic relations, international commitments, regional cooperation, or treaty obligations.
f. **Cyber Warfare and Hostile Exploitation:** The likelihood that disruption, compromise, or unauthorized access could be exploited for espionage, sabotage, cyber warfare, influence operations, or other malicious activities affecting national interests.

4.3.1.4. Designation Requirement

An organization shall be considered to meet the Security Impact Criterion where INSA determines that disruption or compromise of the organization's services, systems, or operations would result in a significant adverse impact on national security, sovereignty, continuity of government, constitutional order, or national resilience.

Evidence supporting this determination shall be documented as part of the Critical Infrastructure designation assessment.

4.3.2. Economic Impact Criterion (National Productivity and Financial Stability)

4.3.2.1. Objective

The Economic Impact Criterion shall be used to determine whether the disruption, degradation, compromise, or unavailability of an organization's services, systems, assets, or operational capabilities could adversely affect the economic stability, productivity, financial systems, trade, employment, or sustainable economic development of the nation.

The criterion shall identify organizations whose disruption would result in significant economic consequences extending beyond the organization and create substantial risks to national economic resilience, financial stability, or the continuity of essential economic activities.

4.3.2.2. Assessment Requirements

INSA shall assess an organization against this criterion to determine whether the organization performs functions or operates assets that are essential to the continuity and stability of the national economy.

An organization shall satisfy this criterion where one or more of the following conditions apply:

a. The organization provides services, infrastructure, or capabilities that are essential for the operation and continuity of the national economy.
b. The organization supports the stability, integrity, or continuity of the national financial system, including banking, payment, settlement, clearing, securities, or other financial market infrastructures.
c. The organization enables national or international trade, logistics, transportation, distribution, or supply chain operations that are essential to economic continuity.
d. The organization operates facilities, systems, or infrastructure that are critical to industrial production, commercial activities, or the delivery of essential economic services.
e. The organization provides products or services whose disruption would result in significant economic losses, widespread business interruption, or reduced national productivity.
f. The organization employs a significant workforce or supports economic activities upon which substantial employment, income generation, or livelihoods depend.
g. The disruption, degradation, or compromise of the organization's services could significantly reduce investor confidence, disrupt financial markets, or adversely affect national economic stability.

4.3.2.3. Assessment Considerations

In assessing this criterion, INSA shall consider, as applicable, the following factors:

a. Contribution to National Economy: The extent to which the organization contributes directly or indirectly to Ethiopia's Gross Domestic Product (GDP), economic output, productivity, revenue generation, or strategic economic development.

b. **Financial System Stability**: The organization's role in supporting banking services, payment systems, securities markets, financial transactions, settlement systems, monetary operations, or other components of the national financial ecosystem.
c. **Trade and Supply Chain Continuity**: The extent to which the organization enables domestic commerce, international trade, import and export activities, transportation networks, logistics services, distribution systems, or supply chain continuity.
d. **Industrial and Commercial Productivity**: The organization's contribution to manufacturing, industrial production, commercial operations, service delivery, or other economic activities essential to maintaining national productivity.
e. **Employment and Income Stability**: The number of employees, contractors, dependent businesses, or communities that rely on the organization for employment, income generation, or economic sustainability.
f. **Investor Confidence and Market Stability**: The potential impact that disruption of the organization's services could have on domestic or foreign investment, financial market confidence, business continuity, economic competitiveness, or overall market stability.

4.3.2.4. Designation Requirements

An organization shall satisfy the Economic Impact Criterion where INSA determines, based on the assessment conducted in accordance with this Standard, that the disruption, degradation, compromise, or unavailability of the organization's services, systems, assets, or operations would result in a significant adverse impact on one or more of the following:

a. National economic stability;
b. National productivity;
c. Financial system stability;
d. Trade and supply chain continuity;
e. Industrial or commercial operations;
f. Employment and income stability;
g. Investor confidence or market stability; or
h. Ethiopia's sustainable economic development.

INSA shall document the assessment results, supporting evidence, justification, and designation decision as part of the Critical Infrastructure designation process in accordance with this Standard.

4.3.3. Social Impact Criterion (Public Welfare and Human Safety)

4.3.3.1. Objective

The Social Impact Criterion shall be used to determine whether the disruption, degradation, compromise, or unavailability of an organization's services, systems, assets, or operational capabilities could adversely affect public safety, human life, public health, essential services, or the overall welfare of the population of the nation.

The criterion shall identify organizations whose disruption could cause significant consequences to citizens' safety, health, or access to essential services, based on the severity, duration, geographic scope, number of persons affected, and potential impact on social stability and public trust.

4.3.3.2. Assessment Requirements

INSA shall assess an organization against this criterion to determine whether the organization provides services that are essential for sustaining human life, public safety, or societal well-being.

An organization shall satisfy this criterion where one or more of the following conditions apply:

a. The organization provides essential services necessary for the protection of human life, public safety, or physical well-being.
b. The organization provides or supports healthcare services, medical treatment, emergency medical response, pharmaceuticals, or medical supply chains.
c. The organization provides essential utilities or services including water supply, sanitation, electricity, or energy distribution required for basic human survival and societal functioning.
d. The organization provides transportation, logistics, or mobility services that are essential for access to healthcare, food, employment, or emergency services.
e. The organization supports food supply chains, agricultural distribution, or essential goods distribution required for population sustenance.

f. The organization provides emergency response services, disaster response coordination, rescue operations, or public safety services.
g. The disruption, degradation, or compromise of the organization's services could result in significant harm to public welfare, public health, or social stability.

4.3.3.3. Assessment Considerations

In assessing this criterion, INSA shall consider, as applicable, the following factors:

a. **Risk to Human Life and Public Safety**: The extent to which disruption of the organization's services could directly or indirectly result in injuries, fatalities, or threats to physical safety.
b. **Public Health Impact**: The organization's role in supporting hospitals, healthcare systems, medical supply chains, disease prevention, public health monitoring, and emergency medical response capabilities.
c. **Population Dependency Level**: The number of individuals, households, or communities that depend on the organization's services for survival, safety, or essential daily needs.
d. **Essential Service Continuity**: The extent to which the organization provides or supports essential services such as water, electricity, energy, food supply, transportation, or other fundamental services required for daily life.
e. **Social Stability and Public Confidence**: The potential impact that disruption of services may have on public trust, social order, civic confidence, or the likelihood of unrest or instability.
f. **Impact on Vulnerable Groups**: The extent to which disruption disproportionately affects vulnerable populations, including children, elderly persons, persons with disabilities, low-income communities, and other at-risk groups.

4.3.3.4. Designation Requirements

An organization shall satisfy the Social Impact Criterion where INSA determines, based on the assessment conducted in accordance with this Standard, that the disruption, degradation, compromise, or unavailability of the organization's services, systems, assets, or operations would result in a significant adverse impact on one or more of the following:

a. Human life or public safety;
b. Public health systems or healthcare delivery;
c. Essential services required for daily life;
d. Food, water, energy, or transportation systems;
e. Social stability or public confidence; or
f. Vulnerable population groups.

INSA shall document the assessment results, supporting evidence, justification, and designation decision as part of the Critical Infrastructure designation process in accordance with this Standard.

4.3.4. Interdependency and Cascading Impact Criterion

4.3.4.1. Objective

The Interdependency and Cascading Impact Criterion shall be used to determine the extent to which the disruption, degradation, compromise, or unavailability of an organization's services, systems, assets, or operational capabilities could adversely affect other critical infrastructure sectors through interconnected systems, dependencies, and shared service relationships.

The criterion shall identify organizations whose failure could trigger cascading disruptions across multiple sectors, amplify national risk, and result in systemic or nationwide operational impact affecting both public and private sector services.

4.3.4.2. Assessment Requirements

INSA shall assess an organization against this criterion to determine whether the organization operates as a foundational enabler within the national critical infrastructure ecosystem or has significant dependencies with other critical sectors.

An organization shall satisfy this criterion where one or more of the following conditions apply:

a. The organization provides services, systems, or infrastructure that are essential inputs to one or more critical infrastructure sectors.

b. The organization is a key enabler of essential services in sectors such as energy, telecommunications, financial services, transportation, healthcare, water, or digital infrastructure.
c. The organization operates platforms, networks, or systems that are widely used across multiple critical sectors, including shared ICT, cloud, data, or communication services.
d. The disruption, degradation, or failure of the organization would likely propagate to dependent organizations or sectors through technical, operational, or service interdependencies.
e. The organization participates in upstream or downstream supply chains that are essential for the continuous operation of other critical infrastructure entities.
f. The organization provides centralized or shared services whose failure would result in simultaneous disruption across multiple sectors or geographic regions.

4.3.4.3. Assessment Considerations

In assessing this criterion, INSA shall consider, as applicable, the following factors:

a. Cross-Sector Dependencies: The extent to which other critical infrastructure sectors rely on the organization's services, systems, or outputs for their own operational continuity.
b. Cascading Failure Potential: The likelihood that disruption of the organization would trigger sequential or simultaneous failures in dependent systems, organizations, or sectors.
c. Systemic National Impact: The potential for widespread disruption affecting multiple sectors of the economy, government services, or national infrastructure systems.
d. Digital and Technological Interconnections: The degree of integration with ICT systems, cloud infrastructure, data centers, communication networks, or other digital platforms supporting critical services.
e. Supply Chain Interdependencies: The organization's role within upstream and downstream supply chains that are essential for the continuous functioning of critical infrastructure sectors.
f. Strategic Enabling Role: The extent to which the organization functions as a shared service provider, platform, or enabling infrastructure supporting multiple critical sectors simultaneously.

4.3.4.4. Designation Requirement

An organization shall satisfy the Interdependency and Cascading Impact Criterion where INSA determines, based on the assessment conducted in accordance with this Standard, that the disruption, degradation, compromise, or unavailability of the organization's services, systems, assets, or operations would result in cascading or systemic impacts affecting multiple critical infrastructure sectors.

INSA shall document the assessment results, interdependency mapping, supporting evidence, justification, and designation decision as part of the Critical Infrastructure designation process in accordance with this Standard.

4.3.5. Service Essentiality Criterion

4.3.5.1. Objective

The Service Essentiality Criterion shall be used to determine the extent to which the services provided by an organization are essential, irreplaceable, or fundamental to the functioning of the State, national economy, and society of the nation.

The criterion shall identify organizations whose service disruption would significantly affect national continuity, governance, economic stability, or public welfare, particularly where alternative service provision is limited, insufficient, or unavailable within an acceptable timeframe.

4.3.5.2. Assessment Requirements

INSA shall assess an organization against this criterion to determine whether the services it provides are essential for the continuous functioning of government, economy, or society.

An organization shall satisfy this criterion where one or more of the following conditions apply:

a. The organization provides services that are essential for the functioning of government operations, public administration, or constitutional functions.
b. The organization provides services that are critical to national economic stability, financial systems, or key productive sectors.

c. The organization provides services that are essential for public welfare, safety, health, or the delivery of basic needs.
d. The services provided by the organization are not readily substitutable within an acceptable timeframe without causing significant national, economic, or social disruption.
e. The organization is a primary or sole provider of a service that is fundamental to national operations or societal functioning.
f. The interruption of services would result in severe operational constraints for government, business continuity failures, or widespread service disruption.

4.3.5.3. Assessment Considerations

In assessing this criterion, INSA shall consider, as applicable, the following factors:

a. Essential Nature of Services Provided: The degree to which the organization's services are fundamental to the functioning of government, economy, or society, including whether they are classified as essential services.
b. Availability of Alternative Providers: The existence, adequacy, and readiness of alternative service providers, including redundancy, substitution capacity, and market competition.
c. Government and Institutional Dependency: The extent to which government institutions, public authorities, or critical national functions depend on the organization's services.
d. Population Dependency Scale: The number of individuals, communities, or sectors that rely on the organization's services for daily operations or essential needs.
e. Service Uniqueness and Irreplaceability: The degree to which the services are unique, specialized, or cannot be replicated or replaced by other providers within an acceptable timeframe.
f. Maximum Tolerable Outage Duration: The acceptable duration of service disruption before significant national, economic, or social impacts occur, including recovery time objectives and resilience thresholds.

4.3.5.4. Designation Requirement

An organization shall satisfy the Service Essentiality Criterion where INSA determines, based on the assessment conducted in accordance with this Standard, that the services provided are essential to national continuity and cannot be adequately substituted, replaced, or restored within an acceptable timeframe without causing significant adverse impact.

INSA shall document the assessment results, supporting evidence, justification, dependency analysis, and designation decision as part of the Critical Infrastructure designation process in accordance with this Standard.

4.4. Critical Infrastructure Classification Levels

4.4.1. Overview

Following the strategic identification of critical sectors and key institutional entities, establishing a robust methodology to classify and rank specific cyber assets (networks, systems, and data repositories) is the vital operational step required to convert high-level national policy into an actionable defense mechanism. Without a standardized, objective framework, cybersecurity regulatory bodies and institutional leaders face severe challenges in resource optimization—potentially over-allocating budget to non-critical systems while leaving vital core infrastructure under-protected.

4.4.2. Objective

The objective of the Critical Infrastructure Classification Levels is to provide a consistent and risk-based approach for categorizing designated Critical Infrastructure according to the severity of the consequences resulting from its disruption, degradation, compromise, or unavailability. The classification supports the prioritization of cybersecurity investments, regulatory oversight, resilience planning, incident response, and national resources to ensure that organizations with the greatest potential impact receive the highest level of protection.

4.4.3. The 3- category Classification Model (Asset Levels)

In alignment with modern function-centric cybersecurity standards, all institutional cyber assets are bucketed into a clear, three-category hierarchy:

Category I – Nationally Critical Infrastructure

Category I includes critical infrastructures whose disruption would result in severe or catastrophic consequences to national security, public safety, economic stability, public health, government continuity, or the operation of multiple critical infrastructure sectors.

Organizations classified as Category I constitute the infrastructure of the highest national significance and require the highest levels of protection, resilience, and regulatory oversight.

Typical characteristics include:

- Nationwide impact;
- Severe disruption of essential services;
- Significant national security implications;
- Major economic consequences;
- Extensive cascading effects across multiple sectors;
- Limited or no viable alternatives;
- Prolonged recovery periods.

Category II – Highly Critical Infrastructure

Category II includes critical infrastructures whose disruption would result in significant national, multi-regional, or multi-sector consequences but would not create catastrophic nationwide impacts.

Organizations classified as Category II provide highly important services that support national resilience and sector continuity.

Typical characteristics include:

- Significant regional or multi-sector impact;
- Major service disruption;
- High economic or operational consequences;
- Strong dependency relationships with other critical sectors;

- Limited service alternatives;
- Moderate to high recovery complexity.

Category III – Significant Critical Infrastructure

Category III includes critical infrastructures whose disruption would result in substantial sectoral, regional, or localized consequences and would significantly affect the delivery of essential services within a critical infrastructure sector.

Organizations classified as category III remain important to national resilience but generally have a more limited impact when compared to category I and category II critical infrastructures.

Typical characteristics include:

- Sector-specific impact;
- Significant operational disruption;
- Limited cascading consequences;
- Availability of alternative service providers;
- Moderate recovery requirements;
- Primarily sector-level consequences.

4.4.4. Classification Determination

The classification of a designated Critical Infrastructure shall be determined as follows:

a. The classification shall be based on the results of the Criticality Assessment conducted in accordance with Section 4.3 of this Standard.
b. The Administration shall evaluate the overall level of criticality arising from the assessment.
c. The Administration shall assign a classification category that reflects the severity of actual or potential consequences associated with the disruption, degradation, compromise, destruction, or unavailability of the organization's critical services, systems, assets, or operations.
d. The classification determination shall consider the following factors:

- The results of the criticality assessment;
- The overall criticality score (where applicable);
- The national significance of the organization;
- Sector-specific considerations;
- Interdependencies with other critical infrastructure;
- Any other relevant technical, operational, or national security factors.

e. The assigned classification shall represent the critical infrastructure's overall level of national significance.
f. The classification shall be used to determine applicable Critical Infrastructure Protection requirements, regulatory obligations, resilience measures, and oversight arrangements.

4.4.5. Criticality Score

The overall criticality of a designated critical infrastructure shall be determined by calculating its Criticality Score (CS). The Criticality Score shall be derived by multiplying the score assigned to each assessment criterion by its corresponding strategic weight and summing the results:

CS = (I_SI x W_SI) + (I_EC x W_EC) + (I_SO x W_SO) + (I_II x W_II) + (I_SE x W_SE)

Variables Defined:

- **I (Impact Score):** The assessed severity of a compromise for a specific dimension.
- **W (Strategic Weight Multiplier):** The relative importance of that dimension to the nation or organization.

Each assessment criterion shall be assigned an impact score ranging from **1 (Low)** to **5 (Critical)** in accordance with the assessment methodology specified in this Standard.

4.4.6. Dimension Weights (W) and Scoring Baselines

The weighting assigned to each assessment criterion reflects a consequence-based approach to determining the national criticality of the Critical Infrastructure. The weighting hierarchy prioritizes the protection of national interests, continuity of essential services, societal resilience,

and systemic stability while ensuring that economic considerations are proportionately reflected in the overall assessment.

Assessment Criterion	Weight	Strategic Logic	Justification
Security Impact (WSI)	**5**	National security is the foremost responsibility of the State and the primary objective of Critical Infrastructure protection. Therefore, criteria directly affecting national security, public safety, government continuity, and national sovereignty receive the highest priority.	Security Impact is assigned the highest weighting because disruption affecting these interests can result in catastrophic and potentially irreversible consequences for the nation. Such impacts cannot be readily compensated through alternative arrangements and therefore constitute the principal determinant of criticality.
Service Essentiality (WSE)	**4**	Critical Infrastructure exists to ensure the uninterrupted delivery of services that are indispensable to the functioning of government, the economy, and society. Protecting these services is fundamental to national resilience.	Although essential services directly support national stability, their consequences are generally evaluated after direct national security impacts. Accordingly, Service Essentiality receives the second-highest weighting as the primary measure of operational importance.
Social Impact (WSO)	**3**	The resilience of society depends on maintaining public health, safety, public confidence, and social stability. Significant social disruption can amplify national crises even where security is not directly compromised.	Social Impact is assigned a medium-high weighting because it measures the extent to which disruption affects the population and public welfare. While these consequences are significant, they are generally secondary to national security and essential service continuity.
Interdependence Impact (WII)	**3**	Modern Critical Infrastructure functions as an interconnected ecosystem. Dependencies between sectors increase the likelihood that disruption within one organization may propagate rapidly across multiple	Interdependence Impact receives the same weighting as Social Impact because cascading failures can significantly magnify the overall consequences of an incident. Although interdependency is an indirect characteristic rather than a direct

		sectors, producing cascading national consequences.	impact, it is a key indicator of systemic risk and national resilience.
Economic Impact (WEC)	**2**	Economic stability is an important national objective; however, economic consequences are generally considered recoverable over time through financial, regulatory, and policy interventions.	Economic Impact receives a lower weighting because financial losses, although potentially substantial, are typically less immediate and less irreversible than impacts affecting national security, essential services, societal stability, or systemic interdependencies. It therefore serves as a supporting criterion in determining overall criticality.

Table 2 Dimension Weights (W) and Scoring Baselines

4.4.7. Classification Thresholds and Determination

4.4.7.1. Classification Thresholds

The Critical Infrastructure classification shall be determined based on the calculated **Criticality Percentage (CP)** derived from the Criticality Score (CS) in accordance with Section 4.4.5.

The classification thresholds are established to ensure that critical infrastructures are categorized according to the severity of potential consequences resulting from disruption, degradation, compromise, destruction, or unavailability of their critical services, systems, assets, or operations.

The Administration shall assign classification levels as follows:

Criticality Percentage	Criticality Score Range	Classification Level
80% – 100%	68 – 85	Category I – Nationally Critical Infrastructure
60% – 79%	51 – 67	Category II – Highly Critical Infrastructure
40% – 59%	34 – 50	Category III – Significant Critical Infrastructure
Below 40%	Below 34	Not Designated as Critical Infrastructure

Table 3 Classification Thresholds

4.4.7.2. Justification for Classification Thresholds

The classification thresholds are established using a consequence-based and risk-informed approach to ensure that Critical Infrastructure designation reflects the relative severity of potential national impacts.

The thresholds are designed to prioritize organizations based on their contribution to national security, essential service continuity, societal resilience, economic stability, and cross-sector dependency.

The rationale for each classification level is as follows:

Category I – Nationally Critical Infrastructure (80%–100%)

Category I represents Infrastructure of the highest national significance. The 80% threshold ensures that only organizations demonstrating exceptionally high criticality across multiple impact dimensions are classified at the highest level.

Infrastructures within this category are expected to have significant scores in the highest-priority dimensions, particularly Security Impact and Service Essentiality, because their disruption could result in catastrophic consequences affecting national security, government continuity, essential services, public safety, or multiple critical infrastructure sectors.

The higher threshold reduces the risk of over-classification and ensures that the highest level of regulatory oversight, protection requirements, and national resources are directed toward organizations with the greatest potential consequences.

Category II – Highly Critical Infrastructure (60%–79%)

Category II represents infrastructure whose disruption would result in significant national or cross-sector consequences but would not cause catastrophic nationwide impacts.

Infrastructure in this category provides highly important services and functions that contribute to national resilience and sector continuity. They require enhanced cybersecurity protection, resilience measures, and regulatory oversight proportionate to their level of criticality.

Category III – Significant Critical Infrastructure (40%–59%)

Category III represents infrastructure whose disruption would cause substantial consequences within a specific sector or service domain.

Although the impact may not extend to national-level disruption, these infrastructures remain important to the continuity and resilience of critical infrastructure sectors and therefore require appropriate protection and risk management measures.

Not Designated (<40%)

Infrastructures scoring below 40% do not demonstrate sufficient national consequence to qualify as Critical Infrastructure under this Standard.

Such infrastructures shall continue to manage cybersecurity risks in accordance with applicable cybersecurity requirements; however, they shall not be subject to the additional Critical Infrastructure-specific obligations established under this Standard.

4.4.8.3 Minimum Qualification Criteria for Category I

To ensure that Category I classification reflects both the overall criticality level and the strategic importance of the organization, the infrastructure shall be classified as **Category I – Nationally Critical Infrastructure** only when:

a. The Criticality Percentage is **80% or greater**;
b. The Security Impact score is **4 or higher**; and
c. The Service Essentiality score is **4 or higher**.

Where the infrastructure achieves the overall category I threshold but does not meet the minimum qualification criteria, the Administration shall determine the appropriate classification level based on the complete assessment results and documented justification.

4.4.8. Practical Implementation Methodology

To successfully level assets across the organization, the framework dictates a rigorous and repeatable four-stage process:

- **Comprehensive Asset Inventory:** Establish a definitive registry documenting every hardware node, software stack, database schema, and environment.
- **Dependency Mapping:** Map horizontal and vertical connections between systems to capture Interdependence Impacts accurately.
- **CIA Triad Impact Analysis:** Scrutinize assets against risk scenarios to determine the concrete blast radius across the 5 dimensions.
- **Mathematical Weighting:** Apply the scoring algorithm to ensure high-consequence risks cross the threshold to become Level 1 assets automatically.

4.4.9. Classification Review

The classification assigned to a designated Critical Infrastructure shall be reviewed during periodic reassessments or whenever significant changes occur that may affect the organization's criticality, including changes in services, assets, operational responsibilities, ownership, interdependencies, technology, or risk environment.

Where reassessment determines that the level of criticality has changed, the Administration may upgrade, downgrade, maintain, or revoke the classification as appropriate.

4.4.10.Relationship to Designation

Classification shall not replace the designation process but shall form part of the designation outcome. Every infrastructure designated as Critical Infrastructure shall be assigned a classification category reflecting its assessed level of national significance.

The assigned classification shall be used to determine the scope and intensity of Critical Infrastructure Protection requirements applicable to the organization.

This section fits naturally after the Critical Infrastructure Selection Process and before Review & Reassessment, because classification is the outcome of the assessment and designation process, not a separate activity.

4.5. Critical Infrastructure selection Process

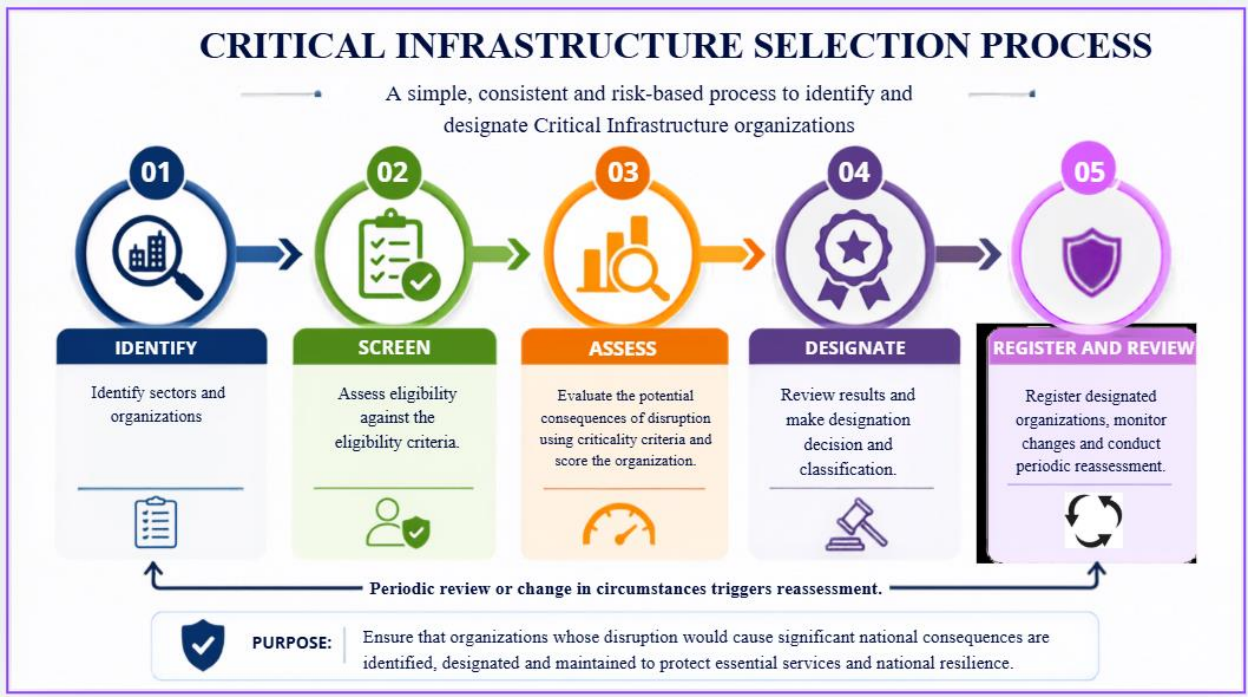


Figure 1 Critical Infrastructure Selection Process

4.6. Critical Infrastructure Selection Process Description

Critical Infrastructure Selection Process refers to the structured method used by a government or organization to identify, evaluate, and designate systems, assets, or sectors as "critical infrastructure" because their disruption would have a significant impact on national security, economy, public health, or safety.

Purpose

To identify and prioritize infrastructure whose disruption, destruction, or compromise would have significant consequences for national security, economic stability, public safety, public health, or the delivery of essential services, and to ensure that appropriate protection and resilience measures are applied.

Critical Infrastructure Selection Process – (Identification Phase)

The Identification Phase is the first and most important stage in selecting and designating Critical Infrastructure (CI). Its purpose is to identify assets, systems, and services and determine which of them may constitute critical infrastructure. Identification Phase aims to:

- Establish a complete inventory of infrastructure assets.
- Understand essential services and their dependencies.
- Identify potential critical infrastructure candidates.
- Provide the foundation for risk and impact assessment.

NO	Activities	Description
1	Asset Identification	Identify all information systems and infrastructure, including hardware (servers, networks, and data centers), software applications, communication systems, databases, cloud services, and other supporting ICT infrastructure.
2	Service Identification (Essential Services Mapping)	Identify services that support national or sector operations, including electricity supply, banking transactions, telecommunications services, government digital services, and healthcare systems.
3	Stakeholder Identification	Identify organizations responsible for the ownership, operation, management, regulation, or support of identified assets, systems, and services, including: government agencies, private sector operators, regulators, service providers, and critical suppliers.
4	Data and Information Flow Mapping	Identify how information moves between systems. Map input/output systems, communication channels, and interconnections between sectors.
5	Dependency Identification	Identify dependencies such as power supply dependency, internet connectivity, third-party services, cloud providers, and shared platforms
6	System Boundary Definition	Define the scope of each system, including internal systems, external interfaces, and third-party integrations.
7	Preliminary Criticality Screening	Conduct an initial screening of CI based on the following factors: Service importance, user population affected, and national or sector dependency level.

Table 4 Key Activities in the Identification Phase

1. Critical Infrastructure Screening Process – (Screening Phase)

The Screening Phase is the second stage of the Critical Infrastructure Selection Process. It is used to filter and-prioritize identified infrastructure assets and services to determine which ones require detailed criticality and risk assessment. The Screening Phase aims to:

- Eliminate non-critical infrastructure from further assessment.
- Identify infrastructure with potential national or sector significance.
- Prioritize resources for detailed evaluation.
- Create a shortlist of candidate CIs.

Key Activities in the Screening Phase

No	Activities	Description
1	Apply Initial Screening Criteria	Evaluate identified infrastructure against predefined criteria, such as essential service delivery, national importance, sector importance public safety impact, economic impact, and government dependency.
2	Determine Essential Service Support	Assess whether the infrastructure supports national security functions, government operations, financial services, telecommunications, energy services, healthcare services, transportation services, and water and sanitation services.
3	Conduct High-Level Impact Assessment	Estimate the consequences of disruption, including service outage, financial loss, public safety risks, national security implications, and social disruption.
4	Assess Dependency and Interconnectivity	Identify cross-sector dependencies, supply chain dependencies, third-party service dependencies, and cascading failure potential.
5	Priorities Candidate Infrastructure	Group assets according to their potential criticality.

Table 5 Key Activities in the Screening Phase

2. Critical Infrastructure Assessment Process – Assessment Phase

The Assessment Phase is the stage where shortlisted infrastructure assets and services are subjected to a detailed criticality, risk, and impact assessment to determine whether they should be designated as CI. The Assessment Phase aims to:

- Evaluate the criticality of infrastructure assets and services.
- Analyze the consequences of disruption, compromise, or destruction.
- Assess risks, dependencies, and vulnerabilities.
- Provide evidence for CI designation decisions.

Key Activities in the Assessment Phase

No	Activities	Description
1	Criticality Assessment	Determine the importance of the infrastructure to national security, economic stability, public safety, public health, government operations, and essential service delivery.
2	Impact Assessment	Assess the potential consequences of disruption, including national security impact, economic impact, public safety and health impact, government impact, and social impact.
3	Dependency Analysis	Conduct dependency analysis to evaluate cross-sector dependencies, interconnected systems, supply chain dependencies, third-party service providers, and cascading failure risks.
4	Vulnerability Assessment	Identify weaknesses in technology, processes, personnel, physical security, and third-party relationships.
5	Threat Assessment	Assess threats such as cyber-attacks, insider threats, terrorism and sabotage, natural disasters, and human error.
6	Risk Assessment	Assess the probability of disruption, magnitude of impact, existing controls, and residual risks.

Table 6 Key Activities in the Assessment Phase

3. Critical Infrastructure Designation Process – Designation Phase

The Designation Phase is the fourth stage of the Critical Infrastructure Selection Process, where infrastructure assets, systems, or services that meet the criticality and risk assessment criteria are officially designated as CI. The Designation Phase aims to:

- Officially identify and recognize CI.
- Ensure critical assets receive appropriate protection and oversight.
- Establish regulatory and security obligations for CI operators; and
- Support national security, economic stability, and public safety.

Key Activities in the Designation Phase

No	Activities	Description
1	Review Assessment Results	Review criticality assessment findings, verify impact assessment results, and validate risk and dependency analysis, and confirm that designation criteria have been met.
2	Designation Decision	Meets the national CI designation threshold; supports essential services; has significant national or sector impact; and requires enhanced protection measures.
3	Classification and Categorization	Assign the infrastructure to the appropriate category: Category 1, Category 2, or Category 3.

Table 7 Key Activities in the Designation Phase

4. Critical Infrastructure Registration and Review Process – Registration and Review Phase

The Registration and Review Phase is the final and ongoing stage of the Critical Infrastructure Selection Process. It ensures that designated CI is formally recorded, monitored, and periodically reassessed to remain accurate and relevant as threats, technologies, and national priorities evolve. The Registration and Review Phase aims to:

- Maintain an up-to-date inventory of designated CIs.
- Ensure the continued relevance of CI designations.
- Monitor changes in criticality, risks, and dependencies.
- Support continuous improvement of the CI protection program; and
- Add new critical infrastructure and remove assets that no longer meet designation criteria.

Key Activities in the Registration and Review Phase

Registration Phase		
No	**Activities**	**Description**
1	Establish and Maintain a CI Register	Create a centralized national CI register, record designated infrastructure assets, systems, and services, maintain ownership and operator information, and record classification levels and designation dates.
2	Document Designation Decisions	Store assessment reports and supporting evidence, maintain records of approval decisions, and track designation history and updates.
3	Register Infrastructure Changes	Record significant changes in ownership, technology, services provided, dependencies, and risk profile.
Review Phase		
1	Periodic Reassessment	Conduct reviews at defined intervals (e.g., annually or every 2 years) to determine whether infrastructure remains critical.
2	Trigger-Based Reviews	Perform reviews when significant events occur, such as major cyber incidents, infrastructure upgrades, organizational restructuring, new technologies or services, changes in national priorities, and emerging threats.
3	Review Criticality and Impact	Reassess national security impact, economic impact, public safety impact, essential service dependency, and cross-sector dependencies.
4	Review Risk and Threat Landscape	Evaluate new cyber threats, vulnerabilities, supply chain risks, and technology changes.
5	Reclassification or De-designation	Based on review results maintain designation, upgrade classification, downgrade classification, and remove CI designation if criteria are no longer met.

Table 8 Key Activities in the Registration and Review Phase

PART V - Review, Reassessment, and Reclassification

4.1. General Principles

Critical Infrastructure designation shall not be considered permanent and shall remain subject to continuous review throughout the lifecycle of the designated organization.

The Administration shall ensure that all designation decisions remain accurate, relevant, risk-informed, and aligned with national security, economic stability, public safety, and national resilience objectives.

Periodic review and reassessment shall be conducted to determine whether the critical infrastructure continues to satisfy the designation criteria established under this Standard.

Review activities shall be evidence-based and shall consider changes in the organization's operations, services, dependencies, threat environment, risk profile, and national significance.

The Administration may conduct reviews at any time where circumstances indicate that the criticality of an organization may have materially changed.

4.2. Objectives

The Administration shall conduct periodic reviews and reassessments to ensure that Critical Infrastructure designation decisions remain valid, accurate, and aligned with current national priorities and risk conditions.

The review and reassessment process shall be conducted to:

- Verify that designated organizations continue to provide nationally significant services or functions.
- Assess whether organizations continue to meet the designation criteria established under this Standard.
- Identify changes in criticality, dependencies, interdependencies, and operational importance.

- Evaluate the impact of technological, operational, organizational, regulatory, or ownership changes.
- Identify emerging threats, vulnerabilities, and risks that may affect criticality status.
- Maintain the accuracy and reliability of the National Critical Infrastructure Registry.
- Support national resilience, preparedness, and risk management efforts; and
- Determine whether an organization should retain its designation, be reclassified, or be removed from the National Critical Infrastructure Registry.

Review and reassessment activities shall be conducted periodically or whenever significant changes occur that may affect an organization's criticality status

4.3. Reassessment Triggers

The Administration may initiate a reassessment where there is reason to believe that the criticality status of an organization has changed or may no longer reflect its current level of national significance.

Reassessment may be conducted in response to significant changes affecting the organization, including:

- Organizational restructuring, mergers, acquisitions, or ownership changes;
- Expansion, reduction, or modification of critical services or functions;
- Significant changes to systems, infrastructure, technologies, or operational processes;
- Changes in dependencies, interdependencies, supply chains, or service relationships;
- Major cybersecurity incidents, physical security incidents, or service disruptions;
- Changes in national threat conditions or risk environments;
- Newly identified critical dependencies or systemic impacts;
- Information that may affect the original designation decision;
- Findings from audits, inspections, investigations, exercises, or lessons learned activities;
- Recommendations from Sector Forum Committee or other competent authorities; or
- Requests submitted by the designated organization.

The Administration may also initiate reassessment whenever it determines that circumstances exist which could materially affect an organization's Critical Infrastructure designation status.

4.4. Periodic Review Cycle

The Administration shall establish and maintain a periodic review program for all designated Critical Infrastructure to ensure that designation decisions remain valid, accurate, and aligned with evolving national priorities, risk conditions, and operational changes.

The periodic review frequency shall be determined based on the assigned Critical Infrastructure classification category, sector-specific risks, threat environment, operational complexity, interdependencies, and the importance of the services provided.

Unless otherwise determined by the Administration, designated Critical Infrastructure shall be reviewed according to the following review cycle:

Critical Infrastructure Classification	Periodic Review Period
Category A – Nationally Critical Infrastructure	At least once every **year**
Category B – Highly Critical Infrastructure	At least once every **two years**
Category C – Significant Critical Infrastructure	At least once every **three years**

Table 9: Periodic Review Cycle

The Administration may initiate an earlier review where significant changes occur, including changes in ownership, operational scope, service dependency, threat conditions, technology environment, sector importance, or any event that may affect the criticality classification of the infrastructure.

The periodic review shall determine whether the Critical Infrastructure classification remains appropriate and whether reclassification, modification, suspension, or de-designation is required in accordance with this Standard.

.

Periodic reviews may include:

- Review of organizational and operational information;
- Self-assessments and compliance submissions;
- Interviews and stakeholder consultations;
- Site visits and inspections;
- Technical assessments and evaluations;
- Dependency and interdependency analysis;
- Risk assessments and impact evaluations; and
- Other verification activities deemed necessary by the Administration.

The Administration may determine the scope, depth, and methodology of each review based on the nature, criticality, and risk profile of the organization.

4.5. Scope of Reassessment

The reassessment may consider any factors necessary to determine whether the infrastructure continues to meet the requirements for Critical Infrastructure designation.

The scope of the reassessment shall be determined by the Administration based on the purpose of the review, the nature of the changes identified, the organization's role, and its potential national significance. The reassessment may include a review of the organization's services, functions, operations, dependencies, interdependencies, risk profile, resilience capabilities, and other relevant information affecting its criticality status.

The Administration may conduct either:

- A **comprehensive reassessment**, covering all applicable designation criteria; or
- A **targeted reassessment**, focusing on specific changes, incidents, risks, or areas of concern.

The scope and depth of the reassessment shall be proportionate to the organization's criticality, the significance of the identified changes, and the potential impact on its designation status.

4.6. Reassessment Methodology

The reassessment methodology shall provide a structured and proportionate approach for evaluating whether an organization continues to meet the requirements and criteria associated with its designation.

The Administration may apply one or more assessment methods depending on the purpose, scope, complexity, and circumstances of the reassessment. The methodology may include the review and analysis of relevant information, documentation, operational data, risk assessments, incident records, sector-specific information, stakeholder input, and any other evidence considered necessary to support the reassessment.

Reassessment may be conducted through comprehensive or targeted reviews and may consider changes in organizational structure, services, functions, dependencies, operating environment, risk profile, resilience capabilities, or other factors that could affect the organization's status.

The methodology shall be risk-based, evidence-driven, and proportionate to the criticality of the organization and the potential consequences of any changes identified. The Administration may adapt the methodology as necessary to address emerging risks, sector developments, technological changes, or other relevant considerations.

4.7. Reclassification

Following a reassessment, the Administration may determine that an organization’s classification should be maintained or modified.

Reclassification decisions shall be based on documented evidence and assessment results. Depending on the outcome of the reassessment, the Administration may maintain the existing designation, upgrade or downgrade the organization's classification, transfer the organization to a different sector classification, designate additional services or functions as critical, or modify designation conditions and requirements. All reclassification decisions shall be recorded in the National Critical Infrastructure Registry.

4.8. De-designation

The Administration may remove a Critical Infrastructure designation where reassessment demonstrates that the organization no longer satisfies the applicable designation criteria. De-designation may occur where one or more of the following conditions apply:

- critical services have been discontinued;
- national significance has materially decreased;
- dependencies and systemic impacts no longer meet designation thresholds;
- organizational functions have been transferred to another entity;
- operations have ceased;
- sector restructuring has altered criticality determinations; or
- assessment results indicate that the designation is no longer justified

Prior to de-designation, the Administration may provide the organization with an opportunity to submit relevant information or clarification. All de-designation decisions shall be documented and recorded in the National Critical Infrastructure Registry.

4.9. Notification of Decisions

The Administration shall formally notify affected organizations of decisions concerning review, reassessment, reclassification, or de-designation.

Notifications shall communicate the assessment findings, classification outcomes, effective dates, required actions, and any applicable review or appeal mechanisms.

4.10. Recordkeeping and Documentation

The Administration shall maintain records of all review, reassessment, reclassification, and de-designation activities. Records shall include the methodologies applied, information reviewed, stakeholder consultations conducted, findings and conclusions reached, decisions and approvals issued, supporting evidence considered, and updates made to the National Critical Infrastructure

Registry. Such records shall be retained in accordance with applicable legal, regulatory, and information management requirements.

4.11. Continuous Monitoring

The Administration may implement continuous monitoring mechanisms to identify changes that could affect Critical Infrastructure designation status.

Continuous monitoring may involve threat intelligence, incident reporting mechanisms, sector risk assessments, regulatory reporting, open-source intelligence, national resilience assessments, and information-sharing arrangements with relevant stakeholders. Information obtained through continuous monitoring may be used to initiate reassessment activities.

PART VI - Compliance and Continuous Improvement

6.1 Compliance

Organizations designated as Critical Infrastructure shall comply with applicable requirements established under the Critical Infrastructure Cybersecurity Proclamation, directives, regulations, standards, guidelines, and other instruments issued by the Administration.

Compliance shall support the protection, resilience, security, and continuity of critical services and infrastructure.

6.2 Compliance Monitoring

The Administration may establish mechanisms to monitor compliance with applicable Critical Infrastructure requirements. Compliance monitoring may include:

- Self-assessments;
- Compliance reporting;
- Document reviews;
- On-site assessments;
- Audits and inspections;
- Technical evaluations;
- Risk assessments;
- Follow-up reviews;
- Other verification activities as deemed necessary.

The scope, frequency, and methodology of monitoring activities shall be determined based on risk, sector characteristics, criticality level, and other relevant considerations.

6.3 Non-Compliance Management

Where non-compliance is identified, the Administration may require corrective actions, improvement plans, remediation measures, or other actions necessary to address identified

Deficiencies. The Administration may establish timelines, reporting requirements, and follow-up activities to verify the effective implementation of corrective measures.

6.4 Continuous Improvement

The Critical Infrastructure designation standard shall be subject to continual review and improvement to ensure its effectiveness, relevance, consistency, and alignment with national priorities, emerging risks, and evolving operational environments. Continuous improvement is essential to maintaining a designation standard that accurately reflects the changing criticality of organizations, technological advancements, sector developments, and national security considerations.

The Administration shall establish mechanisms to periodically evaluate the effectiveness of the designation standard assessment methodologies, classification criteria, governance arrangements, and implementation processes. Such evaluations shall seek to identify opportunities for improvement, address implementation challenges, strengthen assessment consistency, and enhance the overall effectiveness of Critical Infrastructure identification and designation activities.

Continuous improvement activities may include:

- Periodic review and revision of this Standard and related implementation documents;
- Evaluation of the effectiveness, efficiency, and consistency of designation processes and assessment methodologies;
- Analysis of lessons learned from cyber incidents, operational disruptions, emergencies, exercises, simulations, and national response activities;
- Assessment of emerging cyber threats, vulnerabilities, attack techniques, and evolving risk scenarios that may affect Critical Infrastructure sectors;
- Consideration of technological developments, digital transformation initiatives, and emerging technologies that may influence infrastructure criticality;
- Review of changes in national priorities, sector structures, economic conditions, and public service dependencies;
- Benchmarking against international standards, frameworks, guidelines, and recognized best practices;

- Collection and evaluation of feedback from Sector Forum Committee, designated organizations, regulators, technical experts, and other relevant stakeholders;
- Identification of emerging critical sectors, services, technologies, and dependencies requiring inclusion within the national Critical Infrastructure framework;
- Enhancement of assessment tools, scoring methodologies, and designation procedures based on implementation experience and evidence-based findings.

The Administration shall promote a culture of continuous improvement to ensure that the Critical Infrastructure designation standard remains responsive, risk-based, and capable of addressing current and future national requirements.

6.5 Review of the standard

The Administration shall periodically review this Standard to ensure its continued suitability, adequacy, effectiveness, and alignment with the objectives of the Critical Infrastructure Cybersecurity Proclamation. The review process shall assess whether the Standard remains capable of supporting the identification and designation of organizations whose disruption could result in significant national consequences.

The review of the standard shall consider changes in the national operating environment, critical service dependencies, sector-specific developments, technological innovation, cybersecurity risks, and evolving national priorities. The review process may also evaluate the effectiveness of existing assessment criteria, governance arrangements, classification methodologies, designation thresholds, and implementation mechanisms.

The Administration shall ensure that reviews consider, where applicable:

- National security priorities and strategic interests;
- Economic development objectives and critical economic dependencies;
- Public safety, public health, and societal welfare considerations;
- Government continuity and essential public service delivery requirements;
- Technological developments, digital transformation initiatives, and emerging technologies;

- Changes in the national and global cybersecurity threat landscape;
- Emerging Critical Infrastructure sectors, services, and operational domains;
- Cross-sector interdependencies and systemic risk considerations;
- National and international incident trends, lessons learned, and threat intelligence;
- Relevant international standards, frameworks, and recognized best practices;
- Findings from audits, assessments, exercises, and implementation reviews;
- Recommendations from Sector Forum Committee, regulators, designated organizations, and other stakeholders.

Where necessary, the Administration may revise, update, expand, or replace provisions of this Standard to address identified gaps, emerging risks, technological changes, policy developments, or evolving national requirements. Any revisions shall be communicated through appropriate directives, guidelines, amendments, or updated versions of the Standard.

Annex A: Criticality Assessment Checklist

No.	Criticality Criterion	Assessment Area	Assessment Question	Yes/No	Evidence / Remarks	Impact Score (1–5)
1	**Security Impact**	National Defense and Sovereignty	Does the infrastructure support national defense, military readiness, or strategic security capabilities?			
			Does the infrastructure support protection of territorial integrity, border security, or national sovereignty?			
			Could disruption of the infrastructure affect strategic national assets or defense-related operations?			
		Government Continuity and National Governance	Does the infrastructure support continuity of government operations or essential public administration functions?			
			Could disruption affect executive decision-making, constitutional authorities, or critical government functions?			
			Does the infrastructure provide capabilities required for government operations during emergencies or crises?			
		Intelligence and National Security Operations	Does the infrastructure support intelligence, security coordination, information sharing, or national security operations?			
			Could compromise of the infrastructure expose information that may affect national security interests?			
			Could unauthorized access, manipulation, or disruption enable espionage, sabotage, or hostile activities?			
			Does the infrastructure support disaster management, emergency response, or national crisis coordination?			

		Emergency Response and Crisis Management	Could disruption reduce the ability of authorities to respond effectively to national emergencies?			
			Does the infrastructure provide essential capabilities during major incidents or national crises?			
		Diplomatic and International Interests	Could disruption affect Ethiopia's diplomatic relations, international commitments, or regional cooperation?			
			Does the infrastructure support services essential to international obligations or strategic partnerships?			
		Cyber Threat and Hostile Exploitation	Could disruption or compromise of the infrastructure be exploited by hostile actors to affect national interests?			
			Could the infrastructure become a target for cyber warfare, espionage, sabotage, or influence operations?			
			Could compromise of the infrastructure create cascading impacts affecting national security or resilience?			
2	**Economic Impact**	National Economic Contribution and Productivity	Does the infrastructure provide services, systems, or capabilities essential for continuity and stability of the national economy?			
			Does the infrastructure contribute significantly to economic output, productivity, revenue generation, or strategic economic development?			
			Could disruption significantly reduce national productivity or economic performance?			
		Financial System Stability	Does the infrastructure support banking, payment systems, settlement systems, clearing services, securities markets, or financial infrastructure?			

			Could disruption affect stability, integrity, or continuity of the national financial system?			
		Trade and Supply Chain Continuity	Does the infrastructure support trade, logistics, transportation, distribution, or supply chain continuity?			
		Industrial and Commercial Productivity	Does the infrastructure support manufacturing, industrial production, commercial operations, or essential economic services?			
		Employment and Income Stability	Could disruption result in significant employment losses, income reduction, or livelihood impacts?			
		Investor Confidence and Market Stability	Could disruption affect investor confidence, market stability, or economic resilience?			
3	**Social Impact**	Risk to Human Life and Public Safety	Does the infrastructure provide services essential for protecting human life, public safety, or physical well-being?			
		Public Health and Healthcare Services	Does the infrastructure support healthcare services, medical response, pharmaceuticals, or public health operations?			
		Population Dependency and Essential Services	Do significant numbers of individuals, households, or communities depend on the infrastructure for essential needs?			
		Food, Transportation, and Social Support Systems	Does the infrastructure support food supply, transportation, logistics, or essential goods distribution?			
		Emergency Response and Public Safety Services	Does the infrastructure support emergency response, disaster management, rescue operations, or public safety services?			

		Social Stability and Public Confidence	Could disruption negatively affect public trust, social order, or community stability?			
		Vulnerable Groups	Could disruption disproportionately affect vulnerable populations?			
4	**Interdependency Impact**	Cross-Sector Dependencies	Does the infrastructure provide services or capabilities essential to other Critical Infrastructure sectors?			
			Do other Critical Infrastructure entities depend on the infrastructure for operational continuity?			
		Cascading Failure Potential	Could disruption trigger failures in dependent organizations, systems, or services?			
		Systemic National Impact	Could disruption create widespread impacts affecting national infrastructure, government services, or economic activities?			
		Digital and Technological Interconnections	Does the infrastructure support shared ICT, cloud, data centers, communication networks, or digital platforms?			
		Supply Chain Interdependencies	Does the infrastructure provide essential products, services, or resources required by other critical sectors?			
		Strategic Enabling Role	Does the infrastructure function as a shared service provider or enabling capability supporting multiple sectors?			
5	**Service Essentiality**	Essential Nature of Services	Does the infrastructure provide services essential for government, economic, or societal functioning?			
		Alternative Provider Availability	Are alternative providers available with sufficient capacity and readiness?			

		Government Dependency	Do government institutions or critical national functions depend on the services provided?			
		Population and Sector Dependency	Do individuals, communities, organizations, or sectors rely on the services provided?			
		Service Uniqueness and Irreplaceability	Is the service unique, specialized, or difficult to replace within an acceptable timeframe?			
		Maximum Tolerable Outage	Would a short-term interruption result in significant national, economic, or social consequences?			

Annex B: Sample Criticality Assessment Calculation

B.1 Criticality Assessment Methodology

The Criticality Score is calculated by evaluating the impact of disruption against predefined assessment criteria and their assigned strategic weights.

The Criticality Score shall be calculated using the following formula:

$$CS=(ISI\times WSI)+(ISE\times WSE)+(ISO\times WSO)+(III\times WII)+(IEC\times WEC)$$

Where:

Symbol	Description
CS	Criticality Score
I	Impact Score assigned during assessment
W	Weight assigned to each assessment criterion

B.2 Assessment Criteria and Weight

No.	Assessment Criterion	Weight	Maximum Score Contribution
1	Security Impact (SI)	5	25
2	Service Essentiality (SE)	4	20
3	Social Impact (SO)	3	15
4	Interdependence Impact (II)	3	15
5	Economic Impact (EC)	2	10
	Total Maximum Score	17	85

Note:
Each impact criterion is assessed on a scale of **1 to 5**, where:

Impact Score	Description
1	Very Low Impact
2	Low Impact
3	Moderate Impact
4	High Impact
5	Very High Impact

B.3 Impact Assessment

Criterion	Impact Score (I)	Weight (W)	Calculation	Weighted Score
Security Impact (SI)	5	5	5 × 5	25
Service Essentiality (SE)	5	4	5 × 4	20
Social Impact (SO)	4	3	4 × 3	12
Interdependence Impact (II)	4	3	4 × 3	12
Economic Impact (EC)	5	2	5 × 2	10
			Total Criticality Score	79

B.4 Criticality Percentage Calculation

The maximum possible score is:

$$\text{Maximum Score} = (5\times5) + (5\times4) + (5\times3) + (5\times3) + (5\times2)$$
$$\text{Maximum Score} = 25+20+15+15+10=85$$

The Criticality Percentage is calculated as:

$$\text{Criticality Percentage} = (\text{Actual Score} / \text{Maximum Score})\times100$$

$$\text{Criticality Percentage} = (79 / 85)\times100$$

Criticality Percentage=92.9%

B.5 Criticality Classification

Criticality Percentage	Classification
80% – 100%	Criticality Level 1 – Nationally Critical Infrastructure
60% – 79%	Criticality Level 2 – Highly Critical Infrastructure
40% – 59%	Criticality Level 3 – Significant Critical Infrastructure
Below 40%	Not Classified as Critical Infrastructure

Assessment Result

Based on the calculated Criticality Percentage of **92.9%**, the National Payment Processing Infrastructure is classified as:

Criticality category 1 – Nationally Critical Infrastructure