Critical Mass Cyber Security Requirement Standard

Version 2.0

Federal Democratic Republic of Ethiopia
Information Network Security Administration

Published: March 2025 | Public

Critical Mass Cyber Security Requirement Standard

Version 2.0

Federal Democratic Republic of Ethiopia
Information Network Security Administration

Published: March 2025 | Public

Contents

Preamble

Governmental and non-governmental organizations in Ethiopia are highly relying on information and communication technology, and information is becoming invaluable economic, political and social asset of the nation and a resource to transform the country. Information is playing vital role to realize an informed and civilized society, to create a democratic, transparent and accountable government, and to assure sustainable economic development.

On the other hand, the reliance on information systems is increasing the vulnerability of organizations to cyber-attacks which are becoming highly complicated, dynamic and destructive. It is essetial to ensure the security of organizational information systems in order to protect organizations from cyber-attacks and to minimize the impact of cyber attacks on the country.

Organizations must build cyber security capability and establish processes which are required to actively manage security risks on their non-electronic and electronic information and information systems. Therefore, this standard is issued by Information Network Security Agency pursuant to Article 13 of Information Network Security Agency Re-establishment Proclamation Execution Council of Ministers Regulation No. 320/2014.

1.Introduction

Ethiopia is at a critical stage in its digital transformation, driven-by its Digital Strategy, Home-grown Economic Reform, 10-year Development Plan, and other initiatives. These reforms and initiatives are accelerating innovation, connectivity, economic growth, and technological advancement of the nation. The technological developments in information technology and the widespread use of the internet expanded the country`s digital landscape. As technological advancement continues to grow, there has been an increase in cyber threats, risks, vulnerabilities, and cybercrime, resulting in an increasing need for cyber security. Hence, the country requires a comprehensive and adaptive cybersecurity standard that ensures resilience, trust, and compliance to address the aforementioned challenges.

The Information Network Security Administration formulated the Critical Mass Cyber Security Requirement Standard (Version 1.0) and commenced implementation in 2016. At the outset of this year, a revised second version of the standard was released, addressing emerging technologies and threats, implementation gaps identified in the first version, the dynamic nature of cyberspace, and organizational bureaucracies in national and international contexts. The standard plays a fundamental role in ensuring resilience, integrity, and account-ability across the country's digital landscape. It is designed to safeguard the country`s critical digital infrastructure, data assets, and national security while supporting its digital transformation efforts. The standard also addresses the increasing need for governance, risk, and compliance by integrating adaptive security measures, artificial intelligence-driven threat intelligence, and risk-based cybersecurity strategies.

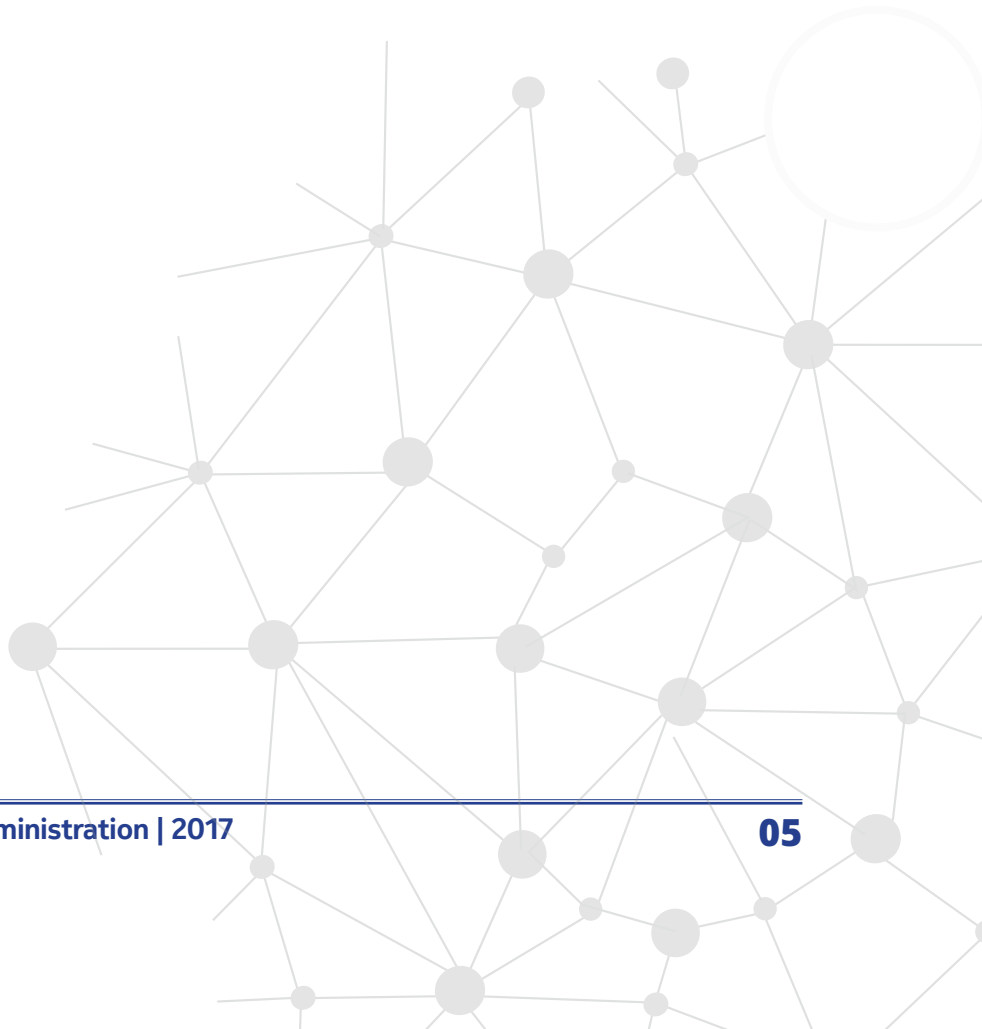
Several key driving factors highlight the necessity of this standard. First, the rapid digital transformation has expanded Ethiopia's digital economy, requiring proactive security measures to protect digital assets. Second, the geopolitical and cyber threat landscape has intensified, with increasing global cyber conflicts and digital espionage, necessitating robust national cyber defense mechanisms. Third, the regulatory and compliance needs continue to grow, pushing for stronger legal frameworks to align with global cybersecurity standards and national security policies. Fourth, cyber resilience for critical infrastructure has become a priority, ensuring that essential sectors such as finance, telecommunications, energy, healthcare, and transportation can mitigate cyber risks. Fifth, the need for data governance and digital sovereignty is more pressing than ever, as securing digital assets is vital for the nation's economic growth, environmental sustainability, and infrastructure advancement. Lastly, strengthening social trust and digital confidence has become crucial for fostering a resilient and inclusive digital society, where citizens and businesses can operate securely.

The Standard is primarily intended for use by government institutions, key critical infrastructures, and private enterprises to effectively manage cyber risks and strengthen their defenses. The standard enables organizations to achieve their objectives through the effective and efficient management of their overall digital assets. Organizations should understand that cyber security is an integral part of national interest and national security, and, therefore, they should make it an integral part of their organization's mission. The standard is structured into two main parts: Part One outlines the foundational concepts, principles, models, and guidelines, while Part Two details specific cybersecurity requirements, operational strategies, and compliance measures. As the standard serves as a blueprint for the country's digital

sovereignty and secure economic growth, it should be implemented as a national cybersecurity minimum requirement to empower organizations, strengthen cyber governance, enhance resilience against cyber threats, integrate security into emerging technologies, and align with its broader digital transformation goals.

Part I

Critical Mass Cyber Security Requirement Foundations



1. Terminologies and Acronyms

1.1 Terminologies

The definitions of terminologies that are used in this document are interpreted as described below.

- **Must:** This word means that the requirement is mandatory (an absolute requirement) of the standard.
- **Must Not:** This phrase means that the requirement is an absolute prohibition of the standard.
- **Should:** This word means that the requirement is "HIGHLY RECOMMENDED" to be implemented. There may exist valid reasons in particular circumstances to ignore a particular requirement, but the full implications must be understood and carefully weighed before choosing a different option. There must be a valid justification for ignoring the requirement or choosing a different option.
- **Should not:** This phrase means that the requirement is "NOT RECOMMENDED" to be implemented. There may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful. Still, the full implications should be understood and the case carefully weighed before implementing any requirement described with this label.
- **May:** This word means that the requirement is "OPTIONAL" to be implemented.

- **Note:** ***The definitions of terms provided in the Cyber Security Dictionary are applicable to this document.***

1.2 Acronyms

AI	Artificial Intelligence
BMIS	Business Model for Information Security
CMCSRS	Critical Mass Cyber Security Requirement Standard
CS	Cyber Security
CSMS	Cyber Security Management System
ICT	Information Communication Technology
INSA	Information Network Security Administration and Challenge
IoT	Internet of Things
IT	Information Technology
OPDCA	Observe, Plan, Do, Check, and Act
PESTLE	Political, Economic, Social, Technological, Legal, and Environmental
RACI	Responsible, Accountable, Consulted, and In formed
SGOC	Strength, Gap, Opportunity, and Challenge

2. Objectives

The main objective of this standard is to secure the country`s critical assets such as information and information systems, technologies, processes, humans, and assets valued as a result of their interaction to protect national interests. The standard aims to enable organizations to effectively achieve their mission by securing these critical assets, thereby supporting the country`s peace, development, and democracy agendas.

The specific objectives of the standard are to:

Create cyber security practices and culture in organizations, bimplement upper-layer Cyber security framework of the nation and create alignment with them, set a foundation for existing and future cyber security standards, methodologies, controls, and other regulations and frameworks, serve as a multi-purpose standard, which enables organizations to get international certifications,

3. Scope of Applicability

This standard applies to Ethiopian`s federal and regional governments as well as key private organizations within the country.

4. Foundations of the Standard

4.1 Standard Parameterization

Standard parameterization describes the nature and behaviour of this standard.

Parameter	Description
Generic nature	The standard is designed to be generic and applicable to all organizations. It empowers them and provides flexibility to build capability-building capabilities.
Contextualization	The standard is highly contextualized considering the overall situation of the country.
Abstraction level	The standard primarily targets the strategic level (outcome layer), although tactical and operational levels are also considered.
Targeted perspective	The main targets of the standard are Human, Process, and Structure, and technologies.
Enforcement level	Mandatory – all of the audiences must meet the requirement. Other organizations are encouraged to implement it.
Classification	Public - can be accessed by any interested body.
Order-freedom	Orderly – organizations are not allowed to implement the standard in their way. They should implement what the standard strictly dictates to do. Exceptional cases should be approved by INSA.
Flexibility-detailed	Flexible (outcome orientation) - if it is necessary, organizations can add details that will help to implement the requirements. However, the details should not contradict or mismatch the requirements. The standard should be implemented using the Critical implementation manual.
Development method	Centralized/fairly closed/the standard is developed by INSA.
Questions	What/why – the standard mainly answers 'what' and 'why' questions. However, it also addresses 'how' questions in some sections which require detailed requirements.
Content type	Requirement standard - the standard contains requirements. Organizations will be audited and certified based on the requirements.

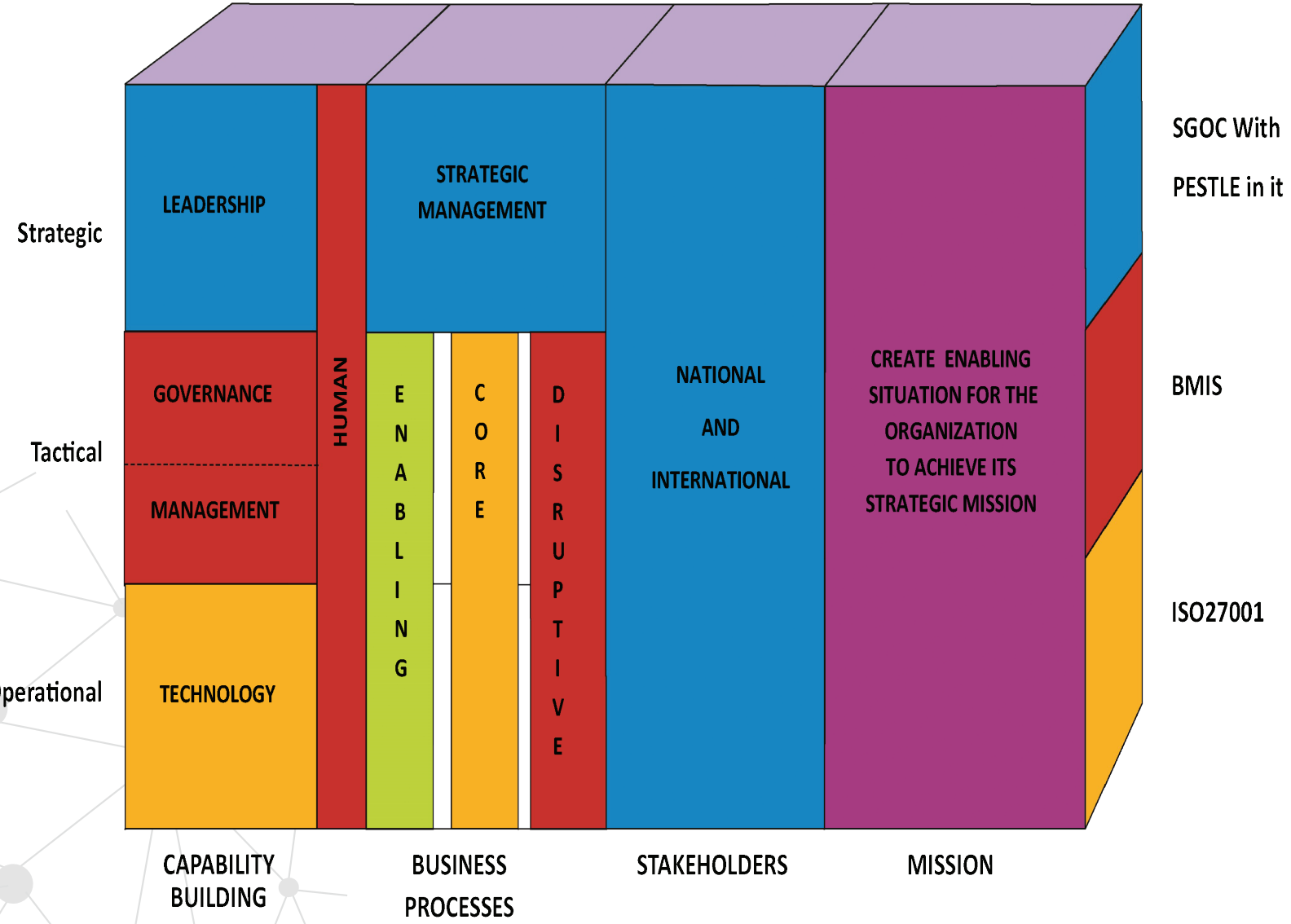


Figure 1. Cyber Security Strategic Management Model of the Standard

The model of the standard is described using the following strategic map.

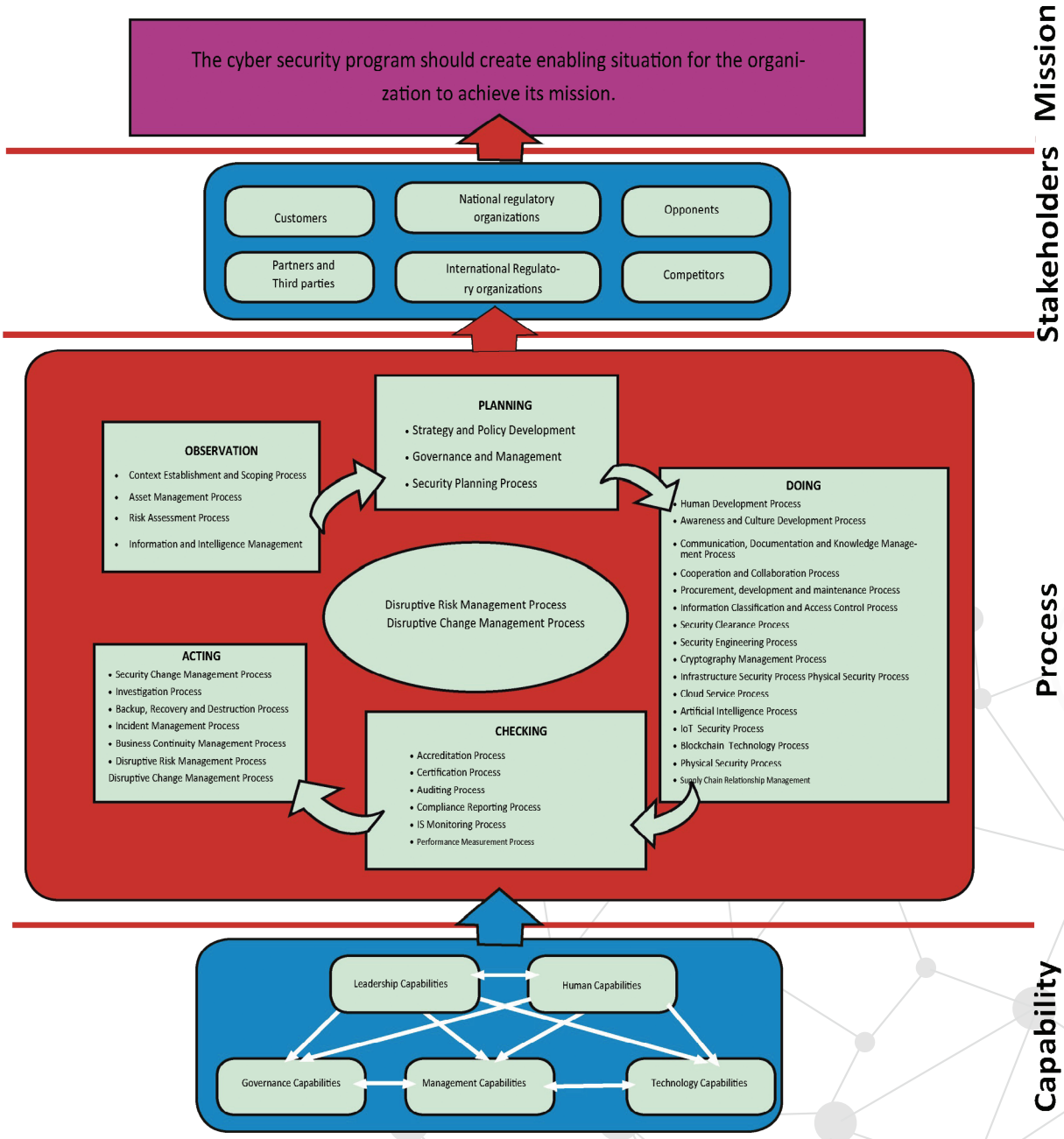


Figure 2. Cyber Security Strategy Map of the Standard

4.2 Concept of the Standard

The concept of the Critical Mass Cyber Security Requirement will be presented by using:

a) Model
b) Framework
c) Architecture
d) Content

The model will be presented in the following subsection. The others are presented in their respective sections of Part II.

4.3 Model

A Cyber Security Strategic Management Model is developed to express the concept of the minimum Critical Mass Cyber Security Requirement Standard. The model contains three dimensions.

1. **Perspective Dimension (D1):** This dimension contains Capability-Building, Process, and Stakeholders perspectives of cyber security.
2. **Level Dimension (D2):** This dimension contains strategic, tactical, and operational levels of cyber security. Capability-building, processes, and stakeholders have these three levels.
3. **Analysis Dimension (D3):** This dimension is used to analyze cyber security at the strategic, tactical, and operational levels, focusing on capability building, processes, and stakeholders. The strategic level can be analyzed using SGOC with PESTLE in it. The tactical level can be analyzed using BMIS (governance, tercon-nections). The operational level can be analyzed using ISO27001 (operation, support, and other relevant clauses).

4.4 Core Principles

a) **Risk-based:** Organizations should implement cyber security solutions (controls) based on risk assessment.

b) **Embedded security:** Organizations should embed cyber security into their structures and processes.

c) **Cost-effective:** Cyber security solutions should be cost-effective, requiring minimal resources and technology. They should feature innovative methods that are both cost-effective and contextualized. Additionally, the solutions should be as simple as possible, easily understood, and easy to operate.

d) **Focus on human, process, and structure:** Organizations should focus on building their human capability, establishing effective cyber security processes, and creating favorable cyber security structures. They should foster a culture of continuous learning. Additionally, they should evaluate their human capability, processes, and structure, taking corrective measures as needed.

e) **Tipping point:** Organizations should use this standard as a tipping point, i.e. a critical point in the organization's cyber security capability and process to transform the cyber security and make it self-sustaining (irreversible). The standard is a game changer that enables organizations to change different aspects of their cyber security, such as their culture, human capabilities, structure, and processes.

f) **Balance:** There should be a balance between each perspective of organizational cyber security. There should be a balance between chaos and order, i.e. the dynamic nature of cyber threats and the static nature of organizational bureaucracy.

g) **Alignment:** Organizations' cyber security programs should align with national cyber security governing frameworks and directives. Organizational cyber security processes should be aligned with organizational governance.

4.5 Characteristics

a) **Developmental:** The process should promote developmental outcomes, fostering natural growth while avoiding shortcuts. It should focus on building internal capabilities and proactively reducing vulnerabilities from the inside out.

b) **Disruptive:** There should be massive mobilization, with leadership and management driven by a disruptive mindset. Processes should be designed with this mindset, and behaviors that encourage transformation should be cultivated.

c) **Cyber Characteristics:** the characteristics of cyber should be considered, and organizations should focus on managing internal vulnerabilities and threats

4.6 Strategy and Methodology

a) **OPDCA with RACI in it:** OPDCA cycle will be used in cyber security capability building and processes, and Responsible, Accountable, [to be] Consulted, and [to be] Informed (RACI) bodies will be identified at each stage.

b) **Transformative risk management:** Risk management driven by transformative change management (transformative risk management) will be the main approach (process), which drives the implementation of the standard.

c) **Top-down Leadership approach:** all processes will be led and managed with a top-down approach. Leaders and man-

agers will take responsibility for the organization's cyber security, build cyber security leadership and management capability, get and share information, and engage themselves and others in ensuring the organization`s cyber security.

d) **Centralized and distributed responsibilities:** Responsibilities will be centralized at the national level, while others will be distributed among organizations. At the organizational level, some responsibilities will be centralized within the organization's responsible body (cyber security unit), and others will be distributed across each organizational unit and to all employees.

e) **Strong and strict regulatory and institutionalism mechanism:** there will be a strong and strict regulatory and institutional mechanism to enforce the standard.

f) **Integrated with national and organizational initiatives and perspectives:** The cyber security issues at the national and organizational levels will be symbiotic with their respective national and organizational initiatives and perspectives. There will be holistic symbiosis.

Part II

Critical Mass Cyber Security Requirement Focus Areas

Part II introduces the focus areas of the Critical Mass Cyber security Requirement Standard, which are based on the Strategic Cyber security Management Model presented in Part I. These focus areas include capability building, processes, stakeholders, and mission that address cyber security requirements at strategic, tactical, and operational levels.

5. Capability Building

5.1 Framework and Architecture

The capability building focus area aims at creating dynamic and continually learning cyber security capabilities to carry out cyber security tasks of the organization effectively. This focus area is described using the capability-building framework shown in Figure 3 below. The main components of the framework are leadership, governance, management, human, and technology. The leadership leads all the capabilities top-down with a disruptive mindset. Human capability is the central part that builds all personnel's capability, playing the leadership, governance, management, and operational roles. In addition, it raises end-user awareness and fosters a security culture within the organization.

The capability-building architecture, shown in Figure 4, presents the main components of each capability.

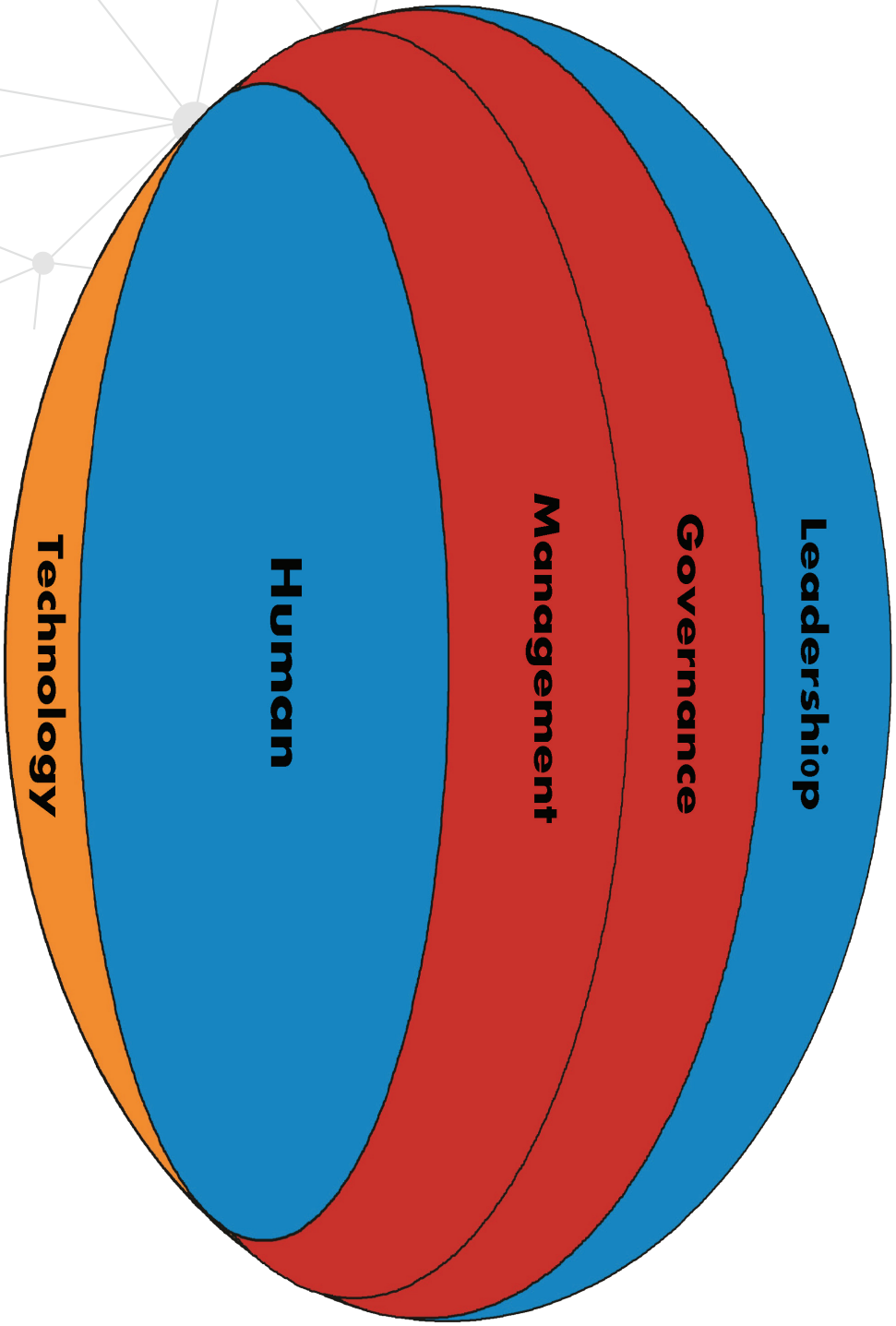


Figure 3. Capability Building Framework

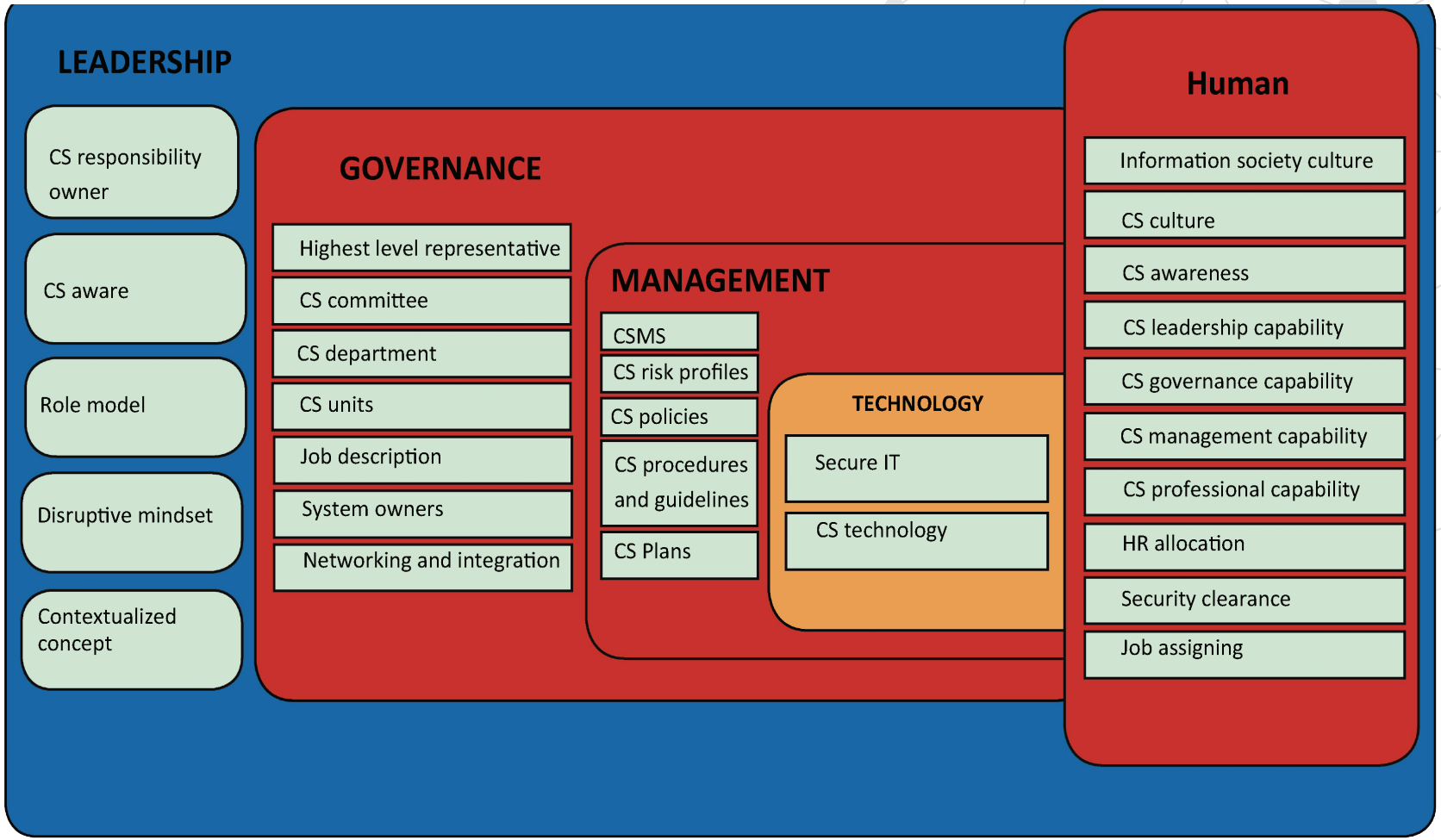


Figure 4. Capability Building Architecture

5.2 Capability Building Principles

Capability-building activities should be conducted based on the core principles outlined in Part I. Additionally, the following principles should also be taken into account.

1. **Ownership:** The leader should hold the highest responsibility and decision making power for the organizations` cyber security, and the cyber security leadership should be an integral part of overall organizational leadership.
2. **Self-leadership:** The leader should demonstrate self-leadership to achieve the cyber security objectives of the organization.
3. **Avoid conflict of interests:** Conflict of interests should be avoided while creating a cyber security structure and job description.
4. **Transparency and accountability:** There should be transparency and accountability at each level, and a check and balance system should be created.
5. **Integration and collaboration:** The cyber security unit should be integrated with other or ganizational units, fostering symbiosis at every level and within each unit. Organization should perform cyber security tasks in a symbiotic manner. Similarly, there should be symbiosis at the sector and national level. Organizational cyber security units should collaborate with respective national units.
6. **Holistic:** Cyber security solutions should be holistic and address comprehensive threats.

7. **Continually learn and live:** The CSMS should be continuously updated up-to-date by learning from each event and incident. Employees at each level of the organization should also learn and be aware of incidents continuously.
8. **Proactive:** The technology and other capabilities should enable the organization to proactively protect against cyber security attacks.

5.3 Leadership Capability

The objective of this capability building is to develop leadership capability that drives organizational cyber security.

a) The top leadership should possess strategic awareness and leadership capability in cyber security, continually be aware of strategic cyber security risks, and learn cyber security leadership.
b) The top leadership should take the overall responsibility for the cyber security of the organization and should serve as a role model for its improvement.
c) The top leadershi p should understand and enforce national cyber security programs and regulations applicable to the organization.
d) The top leadership should develop a contextualized cyber security concept of the organization, i.e. clearly describe 'what is cyber security for the organization?'
e) The top leadership should set the strategic direction of cyber security in the organization.
f) Cyber security should be symbiotic and organic part of the organization's business strategy and risk management.

g) Cyber security should be led with a disruptive mindset and the perspective of disruptive risk management.

h) Cyber security should be led strategically top-down with strong and strict regulatory and institutional mechanisms.

i) Integrated security capabilities should be led with an organizational view, but specialized capabilities should be led under national cyber security.

j) The top leadership should allocate optimum resources that is 0.5% of the organization's annual budget for cyber security.

5.4 Governance Capability

The objective of this capability building is to create a competent institutional structure and security governance that continuously builds human capability and ensures the execution of an organizational cyber security program.

a) The cyber security roles and responsibilities should be embedded into the job description of all hierarchies.

b) The structure should be process-based, comprising hierarchical and networking modes.

c) Organizations should have a representative in the highest level of management who fully engages in the organization's cyber security program(s). This person should lead both the Cyber Security Department and the Security Committee of the organizations.

d) Organizations should have a Cyber Security Department that reports to the highest level of management. This department should have full power over cyber security matters.

e) Organizations should have cyber security management,

human security (cyber security awareness and culture), information technology security, incident detection and management, and internal information security auditing units. Some of the units can be merged if it is applicable to the organization.

f) Organizations should have an organizational-level security committee that comprises representatives of the various departments (business units).

g) Organizations should assign cyber security liaison officers at different layers.

h) An organization`s cyber security structure should be highly networked with internal counterparts and national respective structures.

i) Networking of interested employees on cyber security should be encouraged.

5.5 Management Capability

The objective of this capability building is to build sound, sustainable, and continually updated cyber security systems that assure the efficient execution of cyber security concepts, enable the building of optimum human capabilities and transform knowledge and wisdom into systems.

a) Organizations should adopt a risk-based approach to cyber security.

b) All the components of the management system should be integrated and symbiotic with each other.

c) The CSMSs should be embedded into the culture and vibe of the organization and be continuously updated.

d) Organizations should have comprehensive cyber security risk profiles that shape all components.

e) Organizations should have a transformational management framework.

f) Organizations should have a comprehensive cyber security policy. The policy comprises cyber security disruptive change management and risk management strategic issues.

g) Organizations should have operational Cyber Security Procedures.

h) Organizations should have CSMS. The performance of the CSMS should be continuously evaluated and improved.

i) Organizations should have a strategic and operational cyber security management plan.

j) Organizations should have a security risk management plan, an incident response plan, a business continuity plan, and other related security plans.

k) Organizations should align all organizational systems with the cyber security policy.

l) The CSMS should take 80% of its content from the national and sectorial CSMS and 20% based on the context of an organization.

5.6 Human Capability

The objective of this capability building is to build cyber security enabling cultural values, awareness, knowledge, and skill.

a) Organizations should have information society cultural values such as valuing information, information sharing, and continual learning and dynamism. They should also cultivate information society abilities, including logical reasoning, analytical thinking, and critical thinking.

b) Organizations should have cyber security cultural values such as proactivity, knowledge-based trust, confidence, and security behavior. They also cultivate cyber security abilities such as risk-based thinking.

c) Every respective stakeholder of organizations should be responsible for the cyber security of the organization.

d) Optimum human resources should be allocated for maintaining the cyber security of organizations. Recruitment and promotion should be based on the National Cyber Security Career Path. Organizations can contextualize the National Cyber Security Career Path to their situation but should retain its basic principles and philosophies.

e) Employees who engage in cyber security and manage (administer) the country's critical information systems should be provided security clearance at a national level.

f) The security clearance of all cyber security employees and critical information systems managers (administrators) should be continually updated starting from recruitment.

g) Security professionals and critical information systems managers (administrators) of organizations are assigned tasks and granted authorization based on security clearance and briefings.

h) Cyber security managers should have the capability of managing cyber security based on the National Cyber Security Career Path.

i) Cyber security professionals should have the professional capability of securing the information system based on the National Cyber Security Career Path.

j) All employees should have cyber security awareness and be aware of cyber security risks related to their actions. They should report cyber security incidents and suspicious events to Cyber Security Department and should implement the control directions provided by the department.

5.7 Technology Capability

The objective of this capability building is to create security-enhancing technological capability.

a) Organizations should continually assure the security of the technologies they acquire.

b) Organizations should deploy and utilize critical cyber security technologies based on risk assessment and defense in depth principles.

c) Organizations should have a secure network infrastructure. As a minimum:

1. There should be a formal process for approving and testing network designs, and configurations. Network access rights, configurations, and designs should be tested and updated every six months;

2. The network should be segregated based on risk assessment, access control policy, level of trust, and classification of information stored and processed;

3. Network security controls, firewall, and IPS/IDS (and other relevant network security devices) should be installed based on the risk level for the segregated network. Organizations should install one or more firewalls (or equivalent network security devices) on the boundary of the organization's internal network(s);

4. The default administrative password for any firewall (or other network security device) must be changed to an alternative and strong password;

5. There should be a business justification, approved by the authorized body, for the use of services, protocols, and ports (for each rule that allows network traffic to

pass through the firewall). This should be documented, including the security features implemented for those features;

6. All insecure or unapproved services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, TFTP, RPC, rlogin, RSH or rexec) should be disabled (blocked) unless a compensating control is implemented;

7. Firewall rules that are no longer required should be removed or disabled on time;

8. The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.

d) Organizations' computers and network devices (including wireless access points) should be securely configured. As a minimum:

1. Unnecessary user accounts should be removed or disabled.

2. Any default password for a user account should be changed to a strong, alternative password.

3. Unnecessary software, including applications, system utilities, and network services, should be removed or disabled.

4. The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).

5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops and configured to disable (block) unapproved connections by default.

6. All system components should be configured based on industry-accepted standards and vendor advisory hardening guides that enable to mitigate all known security vulnerabilities.

e) User accounts of organizations' information systems should be managed through robus t access control. As a minimum:

1. All user account creation should be subject to a provisioning and approval process.
2. Special access privileges should be restricted to a limited number of authorized individuals.
3. Details about special access privileges should be documented, stored in a secure location, and reviewed regularly (e.g. quarterly).
4. Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the Internet.
5. Administrative accounts should be configured to require a password change regularly.
6. Each user should authenticate using an appropriate authentication method before being granted access to applications, computers, and network devices.
7. User accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organization) or after a pre-defined period of inactivity.

f) Organizations should implement robut malware protection on exposed computers. As a minimum:

1. Malware protection software should be installed on all computers that are connected to or capable of connecting to the internet.

2. Malware protection software, including program code and malware signature files should be kept up-to-date (e.g. at least daily, either by configuring it to update automatically or through the use of centrally managed deployment).
3. Malware protection software should be configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser).
4. Malware protection software should be configured to perform regular scans of all files.
5. Malware protection software should prevent connections to malicious websites on the internet.

g) All software that runs on the organization's computers and network devices should be kept up-to-date. As a minimum:

1. Software running on computers and network devices that are connected to or capable of connecting to the internet should be supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities.
2. Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet should be installed on time (e.g. within 30 days of release or automatically when they become available from vendors).
3. Out-of-date software (i.e. software that is no longer supported) should be removed from the computer

and network devices that are connected to or capable of connecting to the internet.

4. All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner (e.g. within 14 days of release or automatically when they become available from vendors).

6. Process

6.1 Process Framework and Cycle

The process framework, shown in Figure 5 below, consists of four categories of processes: strategic management processes, core processes, enabling processes, and disruptive processes.

1. **Strategic Management Processes:** These processes create the strategic management of cyber security. The processes under this category are Disruptive Change Management, Disruptive Risk Management, Cyber Security Strategy and Policy Development, and Cyber Security Planning.
2. **Core Processes:** Core processes consist of the main processes that help implement the Cyber Security Strategy and Policy and ensure cyber security.
3. **Enabling Processes:** Enabling processes support (enable) the effective execution of other processes.
4. **Disruptive Processes:** These processes disrupt existing approaches and create better conditions for achieving cyber security.

6.2 Process Principles

The processes should be established based on the core principles mentioned in Part I. In addition, the following principles should be considered.

a) **Comprehensive implementation:** Organizations should implement Strategic Management, Core, Enabling, and Disruptive Processes. They should also provide a clear justification if a certain process is not applicable to their context.

b) **Cascaded Alignment:** All cyber security processes should align with the upper-level process. Core, Enabling, and Disruptive Processes should align with Strategic Management Processes and with an upper-level process in each category.

c) **Integration:** The processes should be integrated with other organizational processes and national governing frameworks.

d) **Embedded and updated:** The processes should be embedded into the culture and vibe of the organization and be continuously updated.

e) **Minimum Outsourcing:** Organizations should minimize the level of process outsourcing if they require external support. No process can be fully outsourced to foreign actors.

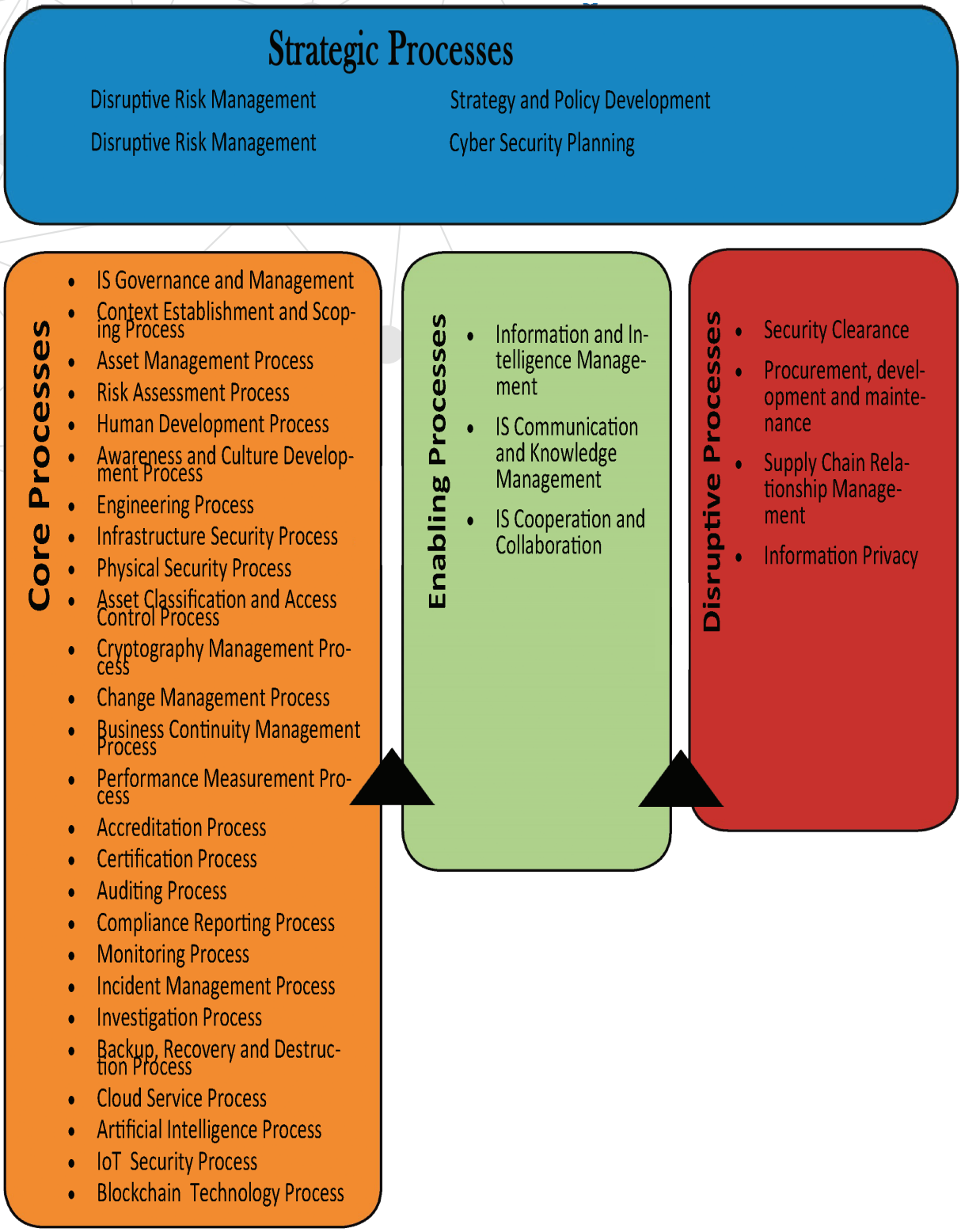


Figure 5. Process Framework

As shown in Figure 6 below, the processes create a comprehensive OPDCA cycle of an organization's cyber security. Each process mainly falls in one of the stages. Each process also includes an OPDCA cycle within it.

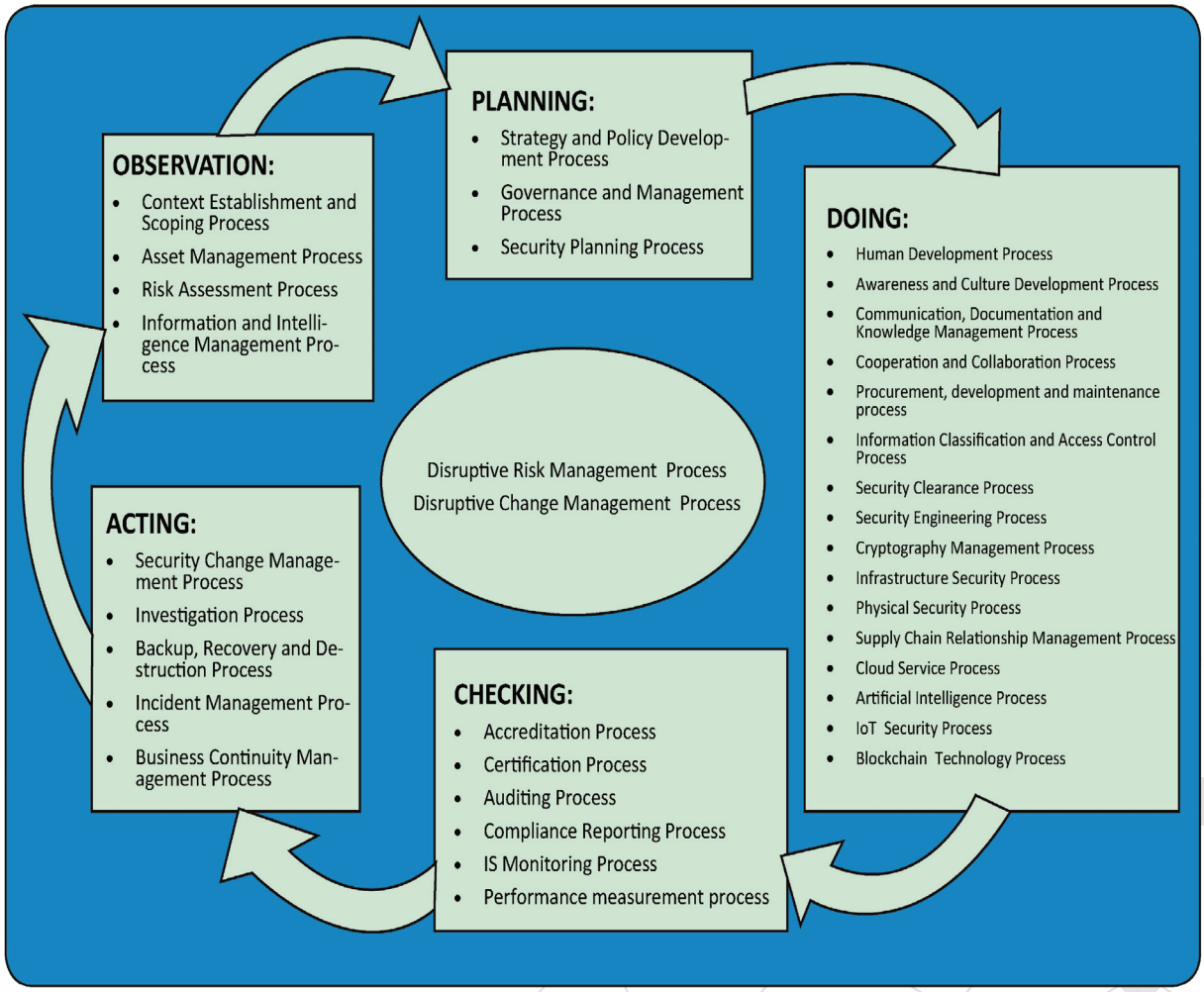


Figure 6. OPDCA Cycle of Processes

A. Strategic Management Processes

6.3 Disruptive Change Management Process

The objective of this process is to lead cyber security with a disruptive mindset to create strategic changes that realize disruptive risk management.

a) The OPDCA phases of the Disruptive Change Management Process should consider the following.

1. The Observation Phase should involve preparation, assessment, and disruptive change strategy development.
2. The Planning Phase should involve preparing a detailed plan for the change.
3. The Doing Phase should involve taking action and implementing the change management.
4. The Checking Phase should involve collecting and analyzing feedback regarding the change.
5. The Acting Phase should involve diagnosing gaps, implementing corrective actions, and managing resistance.

b) The process, including the disruptive change strategy and the plan for the change should be consulted with INSA.

c) The process owner should be the highest level of management.

6.4 Disruptive Risk Management Process

The objective of this process is to manage the cybersecurity risks of organizations with a disruptive mindset in order to transform their cyber security approach.

a) Security risk management should be the business of every staff member, including third parties associated with the organization. Risk management, particularly security risk management, should be part of day-to-day operations.

b) The process for managing security risk should be logical and systematic. Security risk management should form part of the standard management process of the organization, i.e. it should be embedded in the organization's management process.

c) Changes in the threat environment should be continuously monitored and necessary adjustments should be made to maintain an acceptable level of risk and a balance between operational needs and security.

d) The OPDCA phases of the disruptive risk management process should consider the following.

1. The Observation Phase should include processes such as context understanding, risk assessment, and intelligence management;
2. The Planning Phase should be performed based on the results of the risk assessment and intelligence management processes;
3. In the Doing Phase, risk treatment (implementation) is conducted based on the results of the planning phase;
4. In the Checking Phase, actions that evaluate and monitor the efficiency and effectiveness of the risk management system are conducted;

5. In the Acting Phase, improvement and response activities are conducted.

e) The risk management process owner should be the head of the organization's cyber security department.

f) The OPDCA phase process should be conducted in a participatory and accountable manner.

6.5 Cyber Security Strategy and Policy Development Process

This process aims to create strategic awareness, knowledge, and a st rategic system for cyber security leadership and governance.

a) Organizational (corporate) cyber security policy and strategy documents should contain issues, such as drivers, business alignment concept, mission, vision, objectives, principles, and strategies based on the National Cyber Security Framework Development Methodology.

b) Organizational cyber security policy and strategy documents should be based on the National Disruptive Risk Management, Change Management Processes, Organizational Strategic Risk Assessment, and this standard.

c) The policy and strategy should be prepared with the participation of business units and should be led by the top leadership. All employees should own the concepts of the policy and strategy. Critical external stakeholders should also be engaged.

d) The policy and strategy should be approved by the highest level of management of the organization.

e) The policy and strategy should be continuously communicated to the management and employees. All employees should be aware of the policy and strategy.

f) The policy and strategy development should never be outsourced, but local consultants may be utilized as support.

g) The policy and strategy document should be revised every 3 years, or when there are strategic changes.

h) The policy and strategy document should be informed to INSA.

6.6 Cyber Security Planning Process

The objective of this process is to develop strategic, tactical, and operational plans.

a) Organizational cyber security plans should comprise strategic, tactical, and operational plans.

b) The plans should comprise a transformational plan and a routine plan.

c) Organizational cyber security strategic plan should be:

1. based on the National Cyber Security Plan, Organizational Disruptive Risk Management Process, Change Management Process, Cyber Security Policy, and Organizational Strategic Risk Assessment;
2. developed by the top leadership of organizations and to be informed for INSA;
3. developed by the top leadership every 5 years;
4. organic and symbiotic part of organizational strategic plan;

d) The organization's cyber security tactical plan should be:
   1. based on Organizational Strategic Plan, Strategic Risk Assessment, Tactical Risk Assessment, and Cyber Security Policy;
   2. prepared by the leadership of the Cyber Security Department head, approved by the organization's top management, and consulted to INSA;
   3. developed every year;

e) The organization's cyber security operational plan should be:
   1. based on the Organizational Tactical Plan, and Organizational Operational Risk Assessment;
   2. developed by the respective units;

f) Organizational cyber security strategic, tactical, and operational plans should be developed based on the National Cyber Security Development Methodology;

g) All the plans should address critical issues such as capability building and process establishment.

h) The security plans must be updated or revised when there are changes in organizational cyber security risks and operating environment.

i) All plans should be communicated to the right people.

B. Core Processes

6.7 Cyber Security Governance and Management Process

The objective of this process is to create tactical and operational awareness and establish cyber s ecurity governance and management system.

a) The organization's cyber security governance system should be based on the National Cyber Security Governance System, the Organization's Policy, Strategic Risk Assessment, and this Standard,

b) The development and implementation of the governance system should be led by the Cyber Security Department head.

c) The governance system document(s) should be consulted to INSA.

d) The governance system should be revised every two years and whenever there is a change in the organizational governance system o r in the National Cyber Security Governance System.

e) The organizational CSMS shoul d be based on the organization's policy, tactical risk assessment, this standard, National CSMS, and international good practices.

f) The CSMS should be developed with the leadership of the Cyber Security Department head. The security committee of the organization should also be involved. The cyber

security management unit should have professional participation in the development of the system.

g) The organizational CSMS should be revised every year.

h) The organizational CSMS document (s) should be consulted to INSA.

i) Cyber security procedures and guidelines shouldb developed based on the CSMS, operational risk assessment, National Cyber Security Framework Development Methodology, and international best practices.

j) The procedures and guidelines should be developed by the respective professional units and approved by the Cyber Security Department head.

k) The procedures and guidelines should be communicated to respective stakeholders.

l) The procedures and guidelines should be revised at least once a year.

6.8 Context Establishment and Scoping Process

The objective of this process is to understand the context of organizations and identify the scope of implementation.

a) Organizations should determine external and internal issues that are relevant to their purpose and affect their ability to achieve the intended outcome(s) of their CSMS.

b) Organizations should understand the needs and expectations of interested parties. It should determine:

   1. interested parties that are relevant to the CSMS; and
   2. the requirements of these interested parties about information security;

c) Organizations should determine the scope of the CSMS,

including its boundaries and applicability. When determining this scope, the organization should consider:

1. the external and internal issues referred to in 6.8, a (above);
2. the requirements referred to in 6.8, b (above); and
3. interfaces and dependencies between activities performed by the organizations and those performed by other organizations;

d) The context and scop e should be documented and consulted with INSA.

e) The organization should establish, implement, maintain, and continually improve its CSMS, in accordance with the requirements of this standard.

6.9 Cyber Security Change Management Process

The objective of this process is to properly manage and formally approve any cyber security changes before the changes are applied on the organizational assets.

a) Organizations must have a formal security change management process in place to make changes that are important to mitigate identified vulnerabilities.

b) Organizations should ensure that their change management process includes:

1. a policy that identifies which changes need to go through the formal change management process;
2. documenting the changes to be implemented;
3. the formal approval process of the change request;
4. maintaining and auditing logs of all changes;

5. conducting vulnerability management activities when significant changes have been made to the system;
6. testing and implementing the approved changes;
7. updating the relevant cyber security documentation;
8. notifying users about the changes that have been implemented as soon as possible after the change is applied;
9. continually educating users about changes;

c) Organizations must ensure that both routine and urgent changes are handled as follows.
   1. The change management process, as defined in the relevant cyber security documentation, is as followed.
   2. The proposed chang e is approved by the relevant authority.
   3. Any proposed change that could impact the security of a system is submitted to the accreditation authority for approval.
   4. All associated cyber security documentation is updated to reflect the change.

d) The change management process must define appropriate actions to be followed before and after urgent changes are implemented.

e) When a configuration change impacts the security of an asset and is subsequently assessed as having changed the overall security risk for the system, the asset must undergo reaccreditation.

6.10 Asset Management Process

The objective of this process is to identify organizational assets and define appropriate protection responsibilities.

a) Assets associated with information and information processing facilities must be identified and an inventory of these assets shall be drawn up and maintained.

b) Assets maintained in the inventory should be owned by a responsible body.

c) Policy and procedure for the acceptable use of assets should be identified, documented, and implemented.

d) All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract, or agreement.

6.11 Cyber Security Risk Assessment Process

The objective of the process is to continuously develop a risk profile that can be used as intelligence that drives all other processes.

a) The risk assessment process should be based on the National Cyber Security Risk Assessment Framework.

b) The risk assessment profile should comprise issues such as objectives, vulnerabilities, threats, strengths, and opportunities.

c) The risk assessment should comprise strategic, tactical (managerial), and operational (technical) assessments.

d) The strategic risk assessment should focus on organizational strategic risks. This risk assessment should be based on the national strategic risk assessment profile and sectorial strategic risk assessment profile. The

assessment should incorporate SGOC analysis with PESTLE in it. It should be led by the top leadership and revised annually.

e) The tactical risk assessment should focus on managerial risks. This risk assessment should be based on the organizational strategic assessment and sectorial tactica l risk assessment. It should be conducted by the security committee of the organization and can be based on the BMIS model. It should be revised every six months.

f) The operation risk assessment should focus on technical risks. This risk assessment should be based on the organizational strategic risk assessment, organizational managerial risk assessment, and national technical risk profile. This assessment can be based on the ISO 27001 standard. This risk assessment should be updated every three months.

g) 80% of the risks should be taken from the national and sectorial common risk profile and 20% of the risks should be identified based on the context.

h) The risk assessment profile should be multi-purpose.

i) The risk assessment should be mission-oriented and conducted inside out.

j) The risk assessment should be based on cyber security intelligence.

k) The risk assessment should be continuously updated based on information, intelligence, and incidents.

l) The risk assessment should identify the root risks and root strengths.

m) All the risk assessments should be communicated to the right body.

n) Organizations should inform all the risk assessments on time for INSA.

6.12 Cyber Security Human Development Process

The objective of this process is to build the capability of cyber security managers and professionals, enabling them to conduct the organization's cyber security tasks properly.

a) The recruitment, job assignment, development, and growth (promotion) of cyber security professionals and managers should be based on gap analysis, the National Cyber Security Career Paths, and the National Cyber Security Personnel Clearance Scheme.

b) All security positions should have job descriptions based on the national information security job descriptions outlined in the National Cyber Security Career Paths.

c) Organizations should ensure that security personnel possess the necessary competence through appropriate education, training, or experience. Where applicable, organizations should conduct human development programs to acquire the necessary competence.

d) Human development should be done by preparing a strategic, tactical, and operational plan. The strategic plan should be based on the national cyber security human development plan and strategic organizational information security plan.

e) The development of cyber security professionals and managers should comprise of initial tipping point transformation training and continual trainings.

f) Organizations should allocate a minimum number of professionals and managers for a job.

g) Organizations should allocate sufficient resources to build the capacity of cyber security professionals and managers.

h) The human development plans should be reported to INSA.

6.13 Cyber Security Awareness and Culture Development Process

The objective of this process is to continuously create cyber security awareness and develop a cyber security culture in organizations.

a) Organizations must provide sufficient information and security awareness training to all staff, including third parties, to ensure they are aware of security, and meet the requirements of this standard.

b) Organizations should implement a program that fosters a culture of information security resilience based on the National Cyber Security Culture Development Framework and strategic risk assessment. This program should be consulted with INSA.

c) Awareness and training should be tailored to the roles and responsibilities of employees and given continually.

d) The awareness and training program should be based on the National Cyber Security Culture Development Framework, risk assessment, and employees' learning styles.

e) All cyber security incidents should be analyzed and used for awareness and training.

f) The awareness and training program should enable employees to understand their roles and responsibilities, fulfill their security responsibilities, understand and meet security requirements . The program shoul d inform and regularly remind individuals about their security responsibilities, issues, and concerns.

g) Awareness and training should be provided whenever there is a change in role or assignment.

h) Organizations must provide training on their cyber security policies and procedures, and the secure operation

of their systems for all users before granting unsupervised access of the systems.

i) Organizations should ensure that individuals with specific security duties receive appropriate and up-to-date training.

j) Organizations should communicate and make available their information security policies and procedures to all staff, including contractors.

6.14 Cyber Security Engineering Process

The objective of this process is to effectively direct and manage organizations` cyber security engineering projects and major activities to build national cyber security engineering capabilities.

a) The cyber security engineering of organizations should be based on the National Cyber Security Engineering Architecture.

b) Organizational security system should be integrated to the National Cyber Security System.

c) Organizations should have cyber security engineering strategic and tactical plans based on their high-level security requirement and national security engineering plans.

d) Organizations should inform the security engineering plans to INSA before One year.

e) Any information system engineering function (project) should have an equivalent cyber security engineering function. The cyber security engineering function should be informed to INSA.

f) The requirement analysis document (RAD) and the design of the organization' s information system should

be audited and evaluated by INSA before the systems are procured or developed. Information systems that are not certified by INSA should not be deployed. In addition to the evaluation, INSA should monitor and be involved throughout the whole Process of big and mega ICT projects. Organizations should create a conducive situation for this.

g) The whole security engineering function for systems (assets) that have an EXTREME business impact should be done in a centralized and planned way by INSA.

•**Note:** ***Refer to Annex A for Business Impact Leveling Guidance.***

6.15 Infrastructure Security Process

The objective of this process is to secure the infrastructures of organizations.

a) Organizations must document and implement operational procedures and measures to ensure assets, respective activities, and tasks are managed securely and consistently, in accordance with the required security level.

b) Organizations must have control measures in place based on business owner requirements and assessed risks to control acces s to all assets, including information, ICT systems, networks (including remote access), infra-structures, and applications.

c) Organizations must have security measures in place during all stages of ICT system development, as well as when new ICT system s are implemented into the operational environment. Such measures must match the assessed

security risk of the assets contained within, or passing across, ICT networks, infrastructures, and applications.

d) Organizations must ensure that their cyber security measures for all assets; information processes, ICT systems, and infrastructure adhere to any legislative or regulatory obligations under which the organization operates.

e) Organizations which have industrial control systems (Supervisory Control and Data Acquisition systems) should implement the necessary controls based on risk assessment.

6.16 Physical Security Process

The objective of this process is to ensure the physical security of organizations.

a) Organizations must ensure they fully integrate protective physical security early in planning, selecting, designing, constructing, and modifying their facilities.

b) Organizations must implement physical security measures that minimizes or remove the risk of information and information systems being made inoperable or inaccessible, or being accessed, used, or removed without appropriate authorization.

c) Organizations must establish clear direction on physical security by developing and implementing their physical security policy, and addressing their physical security requirements within their security plan.

d) Organizations must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The governmen t may direct organizations to implement heightened security levels.

e) Organizations should select the physical location of their data center and critical infrastructures based on international standards and best practices.

f) Organizations must ensure that any proposed physical security measure or activity does not breach relevant employees' work health and safety obligations.

6.17 Asset Classification and Access Control Pro cess

The objective of this process is to accurately classify organizations' assets and implement appropriate access control mechanisms for a classified asset.

a) Organizations should assure that information assets are valued, handled, shared, and protected in line with the National Cyber Security Classification Standard and related guidelines.

b) Organizations must prepare and implement policies and procedures for the security classification and protective control of assets that match their value, importance, and sensitivity.

c) Organizations must classify their assets based on the Assets Classi fication Guidance presented in Annex B.

d) Organizations should ensure that assets are assigned the appropriate level of classification. If an asset has not been classified, it should not be released until a classification has been applied.

e) Organizational access control rules must align with organizations' business requirements, asset classification, and legal obligations.

f) Personnel seeking access to a system need to have a genuine business requirement and the access right to

access the system as verified by their security clearance or authorized body of organizations.

g) Third parties should be provided access to a system based on genuine business requirements, and the access right should be verified by an authorized body of organizations. They should comply with this standard before they get access. They should be monitored during access, and privileges should be removed once the activities are finalized.

6.18 Cryptography Management Process

This process aims to implement proper cryptographic security measures for classified information.

a) Organizations should use secure cryptographic systems which are approved by INSA when applying cryptographi security measures. Organizations are recommended to use the National PKI Infrastructure.

b) Organizations should use the following cryptographic systems for classified information according to the classification level.

1. For TOP SECRET information: use highly secure proprietary algorithms and protocols that exceeds the security level of international crypto standards and are new to the research field;

2. For SECRET information: use secure innovatively extended proprietary algorithms and protocols with security level higher than international crypto standards;

3. For CONFIDENTIAL information: use extended secure proprietary algorithms and protocols with security level equivalent to international crypto standards.

6.19 Business Continuity Management Process

The objective of this process is to ensure the continued availability of critical services and assets of organizations during cyber security attacks and natural disasters.

a) Organizations must establish a business continuity management (BCM) program.

b) Organizations should develop a governance system establishing authorities and responsibilities for a BCM program, and for the development and approval of business continuity plans.

c) Organizations should evaluate their overall level of preparedness, and make provision for the continuous review, testing, and auditing of business continuity plans.

d) Cyber security continuity should be embedded in organizations' business continuity management systems.

1. Organizations should determine their requirements for cyber security and the continuity of cyber security management in adverse situations, e.g. during a crisis or disaster;
2. Organizations should establish, document, implement, and maintain processes, procedures, and controls to ensure the required level of continuity for cyber security during adverse situations;
3. Organizations must verify the established and implemented cyber security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.

e) Organizations should implement information processing facilities with redundancy, cost-effectively and sufficiently, to meet availability requirements.

6.20 Performance Measurement Process

The objective of this process is to define appropriate metrics and measure the performance of information security personnel and the effectiveness of the CSMS.

a) Organizations should measure the performance of the information security capabilities and the effectiveness of the CSMS. Organizations should determine:
   1. what needs to be monitored and measured, including information security capabilities, processes, and controls;
   2. the methods and metrics for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results, and certify that the selected methods produce comparable and reproducible results to be considered valid;
   3. when the monitoring and measuring must be performed;
   4. who must monitor and measure;
   5. when the results from monitoring and measurement must be analyzed and evaluated; and
   6. Who must analyze and evaluate these results.

b) Organizations should take corrective actions based on the performance measurement results.

c) Organizations should retain appropriate documented information as evidence of the monitoring and measurement results.

6.21 Audit Process

The objective of this process is to assess and evaluate the actual implementation and effectiveness of CSMS of organizations.

a) Organizations must undertake an annual security audit against the mandatory national and organizational cyber security frameworks.

b) The auditor should comprise internal, external, and regulatory assessors.

   1. Internal audit should be conducted by internal auditing team that should be certified by INSA;
   2. Third-party audits are external security assessments that should be conducted by an external auditor certified by INSA;
   3. A regulatory auditor (INSA) is an independent body auditing governmental organizations and key private organizations.

c) The audit should be conducted based on the National Auditing and Evaluation Methodology.

d) Organizations should ensure that auditors conducting audits are not the system owner or accreditation authority.

e) Audits for SECRET and lower level systems can be undertaken by organizations' internal auditing team and Registered Cyber Security Auditors.

f) Audits for TOP SECRET assets must be undertaken by INSA.

g) Cyber security audit reports should be compressive of compliance status and recommendations.

h) The audit report must be accessible to the respective authority bodies.

6.22 Accreditation Process

The objective of accreditation is to formally recognize and accept the residual security risk to a system and the information it processes, stores, or communicates. Accreditation is awarded when the accreditation authority accepts the residual security risk relating to the operation of the system and gives formal approval for the system to operate. If the accreditation authority does not accept the residual security risk, it can place restrictions on the use of the system until required changes are made to the system or reaccreditation is taken place.

a) Organizations must ensure that their systems is awarded accreditation before the systems are used to process, store or communicate sensitive or classified information. System owners should obtain and maintain accreditation for the security of the system.

b) Organizations must develop an accreditation procedure.

c) Organizations must ensure that all systems are awarded accreditation before connecting them via a gateway.

d) Organizations should ensure that information security monitoring activities are conducted on accredited systems.

e) Before beginning the accreditation process, the system owner should inform the certification and accreditation authorities of their intent to seek certification and accreditation for the system.

f) If information is processed, stored, or communicated by a system not under an organization's control, the organization must ensure that the non–organization system has appropriate security measures in place to protect the organization's information.

1. Organizations should review an accreditation report

when determining whether the non–organization system has appropriate security measures in place to protect the organization's information;

2. Organizations must ensure that security requirements are documented in either contract provisions or a memorandum of understanding.

g) A system that processes, stores or communicates TOP SECRET, SECRET, or CONFIDENTIAL information must be accredited for such classified information.

h) Organizations must ensure that the interval between accreditations of systems does not exceed two years.

i) All systems must be certified as part of the accreditation process; unless the accreditation authority is satisfied that if the system is not immediately operational, it would have a devastating and potentially long-lasting effect on operations.

1. The accreditation authority must accept the residual security risk relating to the operation of a system in order to award accreditation.

j) An organization's accreditation authority must be at least a senior executive with an appropriate level of understanding of the security risks they are accepting on behalf of the organization.

k) For multinational and multi-organization systems, the accreditation authorities should be determined by a formal agreement between the parties involved.

l) For TOP SECRET systems, the accreditation authority must be INSA.

m) Cyber security auditing and evaluation systems should be accredited by INSA.

6.23 Certification Process

The objective of the certification process is to ensure that the audit for a system was conducted in an appropriate manner and to a sufficiently high standard. Its outcome is a certificate to the system owner acknowledging that the system has been appropriately audited and that the controls identified by the system owner have been implemented effectively.

a) All systems must undergo an audit as part of the certification process.

b) The certification authority must accept the effectiveness of controls for the system in order to award certification.

c) Following the audit, the certification authority should produce a certification report for th e accreditation authority containing an assessment of th e residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.

d) For SECRET or below systems, the certification authority is the organization`s Internal Auditing Team or there may be an authorized certification authority external to the organization.

e) For TOP SECRET systems, the certification authority should be INSA.

f) For multinationa l and multi-organization systems, the certification authority is determined by a formal agreement between the partie s involved.

g) For commercial providers of gateway services intended for use by multiple organizations across the government, INSA performs the role of the certification authority as an independent third party.

h) Organizations must ensure that commercial or government–provided gateway services intended for use by multiple organizations have got a Gateway Certification from INSA annually.

6.24 Compliance Reporting Process

The objective of this process is to enable organizations and other concerned bodies to understand the organization's cyber security compliance with internal and external applicable security directives and requirements.

a) Organizations should comply with legal and contractual requirements to avoid breaches of legal, statutory, regulatory, or contractual obligations related to cyber security and any security requirements.

b) Organizations should conduct cyber security reviews to ensure that security requirements and controls are implemented in accordanc e with the organizational policies and procedures.

c) Organizations should provide compliance reports on the execution of the security plans to respective authorities.

d) Organizations must report their compliance with the mandatory requirements to the relevant portfolio Minister, or equivalent authority applicable for them.

e) The compliance reports must contain a declaration of compliance by the organization head, and state any areas of non-compliance, including details on measures taken to lessen identified risks.

f) Organizations must send a copy of their annual reports on compliance with the mandatory requirements to INSA.

g) Organizations must recommend any non-compliance with mandatory requirements to INSA, and to the head of any

organization whose personnel, and assets may be affected by the non-compliance.

h) Using organizations' compliance reports, and building upon current security audits, INSA will annually report the cyber security status across government organizations.

6.25 Cyber Security Monitoring Process

The objective of this process is to monitor the security of organizations' i nformation system and to properly manage vulnerabilities.

a) Organizations should implement cyber security monitoring systems.

b) Organizations should monitor their information system during operational hours.

c) Organizations should prepare and implement a vulnerability management strategy and process that includes:

1. conducting vulnerability assessments on systems throughout their life cycle to identify vulnerabilities;
2. analyzing identified vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost, and existing security controls;
3. using a risk-based approach to prioritize the implementation of identified mitigations or treatments;
4. Monitoring new information regarding new or updated vulnerabilities in operating systems, software, and devices as well as other system components that may adversely impact the security of a system.

d) Organizational systems vulnerability assessment should be conducted by suitably skilled personnel independent

of the targeted system owner or by an independent third party.

e) Organizations should conduct vulnerability assessments on systems before deployment. This includes conducting assessments during the system design and development stages, and after any significant change to the system.

f) Organizations must analyze their system vulnerability to determine their potential impact on organizations and identify appropriate mitigations.

g) Organizations must mitigate identified vulnerabilities as soon as possible.

6.26 Cyber Security Incident Management Process

The objective of this process is to detect and properly manage cyber security incidents in organizations.

a) Organizations should have tools and procedures in place, for detecting and managing potential cyber security incidents, including:
   1. countermeasures against malicious code;
   2. intrusion detection;
   3. incident handling;
   4. system integrity checking;
   5. vulnerability assessments;

b) The incident management procedure should include mechanisms to monitor and quantify the types, volumes, and costs of cyber security incidents.

c) Organizations should use the results of the security risk assessment to determine the appropriate balance of resources allocated to the prevention and detection of cyber security incidents.

d) Organizations must prepare an incident reporting procedure and direct all employees and third parties to report cyber security incidents, suspicious events, and any observed or suspected security weaknesses to the security department of th e organizations as soon as possible.

e) Organizations should deal with the violation of cyber security policies and procedures by personnel through a formal disciplinary process.

f) Organizations must report cyber security incidents to Ethio-CER^{2}T through the Cyber Security Department head.

g) Organizations that outsource their information technology services and functions must ensure that their service provider informs them and cooperate for investigation when a cyber-security incident occurs.

h) Organizations must notify of an y suspected loss or compromise of TOP SECRET for INSA.

i) Organizations must detail cyber security incident responsibilities and procedures for each system in their relevant policies and procedures.

j) Organizations must treat any data spill as a cyber-security incident and should conduct the following:

1. Organizations must document procedures for dealing with data spills.

2. The procedures must require all personnel with access to systems to report any data spillage and access to any data which they are not authorized to access.

3. When a data spill occurs, organizations must report the details of the data spill to the information owner and Ethio-CER^{2}T.

k) When information is introduced onto a system not accredited to handle the information:

1. personnel must not delete the information until advice is sought from the Security Department;
2. personnel should not copy, print or email the information;
3. organizations should segregate the affected system from the network;

l) Organizations allowing intrusion activity to continue undecontrolled conditions to scope the intrusion or seek further information or evidence should inform their accreditation authority and seek legal advice.

m) Organizations should ensure that any requests for Ethio-CER^{2}T assistance are made as soon as possible after the cyber security incident is detected and that no actions, that could affect the integrity of the evidence, are carried out before the involvement of Ethio-CER^{2}T.

n) Organizations should perform a post-incident analysis of successful intrusions, storing network traffic for at least seven days after the incident.

6.27 Investigation Process

The objective of this process is to investigate cyber security attacks in a proper manner.

a) A cyber-attack investigation should be conducted by INSA and authorized legal investigators. Legal investigation should be initiated by the proper legal authorities.

b) Organizations must ensure that investigators are appropriately trained and certified, and they have

procedures for investigating and reporting security incidents and taking corrective action.

c) Organizations should:

1. transfer a copy of raw audit trails (evidences) onto media for secure archiving, as well as securing manual log records for retention;

2. ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation;

d) Organizations must report any incident that has an EXTREME business impact to INSA.

e) Organizations should report incidents suspected of constituting criminal offenses to the appropriate law enforcement authority.

6.28 Backup, Recovery, and Destruction Process

The objective of this process is to minimize the loss of assets and securely destroy those that should be removed.

a) Organizations should have backup, recovery, and destruction policies and procedures.

b) Organizations should take backup copies of assets regularly in accordance with their backup policy.

c) Event logs recording administrator and user activities, exceptions, faults, and information security events should be produced, kept, and regularly reviewed.

d) Logging facilities and log information should be protected against tampering and unauthorized access.

e) Organizations should retain or store event logs at least for one month.

f) Recovery and destruction shoul d be conducted by certified investigators.

g) If organizations want to sell used computers or any devices that were used to process and/or store classified information, they should remove or destroy the hard disks and any components used to process and/or store classified information.

h) Any device used to process and/or store SECRET assets and/or TOP SECRET assets should not be sold or transferred to a third party unless approved by INSA.

6.29 Cloud Security Process

The objective of this process is to secure cloud-based infrastructure and manage communication between cloud service providers and users.

a) Organizations should develop procedures and processes to manage cyber security risks associated with cloud service.

b) The security posture of Cloud Service Providers must be assessed to determine compliance with organizational security requirements before the organization host outside of their environment.

c) When using cloud storage for backups, organizations should have to verify the location of the cloud storage to ensure it is in a separate geographical location.

d) Service level agreements and contracts with cloud service providers must be reviewed, understood, and accepted before sign-up to the services.

e) The organizational data must be removed from cloud service after the service agreement closed up by any reason.

f) Classified data stored in cloud service must be encrypted at rest and in transit based on CMCSRS encryption requirements. The encryption keys must be held by the organization.

g) Organizational access control and management of user accounts should be applied to cloud services.

h) The cloud service customer should agree with the cloud service provider on an appropriate allocation of cyber security roles and responsibilities, and confirm that it can fulfill its allocated roles and responsibilities.

i) The cloud service customer should identify and inventory assets stored in the cloud computing environment and label them in accordance with the cyber security asset classification standard and adopted labeling procedures.

j) Organizations should establish a process of acquisition, use, management, and exit from cloud services based on their cyber security requirements.

k) The governmental and key private organizations must use locally licensed cloud service providers.

l) The cloud service provider should design cloud infrastructure securely based on the service model and deployment model based on national cyber security engineering architecture and in line with secure cloud computing and related guidelines.

m) An outsource d cloud service register should contain the following for each service:

1. cloud service provider's name;
2. cloud service's name;
3. purpose for using the cloud service;
4. sensitivity or classification of data involved;

5. due date for the next security assessment of the cloud service;
6. contractual arrangements for the cloud service;
7. point of contact for users of the cloud service;
8. 24/7 contact details for the cloud service provider.

n) Organizations outsourced SECRET and TOP SECRET assets should only use community or private clouds.

o) Cloud service providers and their cloud services undergo a security assessment by INSA at least every two years.

p) Security requirements associated with a service provider must be documented in contractual arrangements and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.

q) Cloud service customer and cloud service provider service level agreement should include the following measures as a minimum but not limited to:
   1. The requirement for service providers to report cyber security incidents to a designated point of contact as soon as possible after they occur or are discovered;
   2. The right to verify compliance with security requirements is documented;
   3. Notification by service providers, when there is significant changes;
   4. Types of assets and their ownership;
   5. The geographical location where the data will be processed, stored and communicated;
   6. Access to all logs relating to an organization's information and services;

7. The storage of assets in a portable manner that allows for backups, service migration, and service decommissioning without any loss of asset;

8. A minimum notice period of one month for the cessation of any services by a service provider.

r) Organizations that outsource their information technology services must ensure that their service provider informs them and cooperate with the investigation when a cyber-security incident occurs.

6.30 Artificial Intelligence Process

The objective of this process is to secure artificial intelligence technology systems and products in organizations. Use AI as an integral part cyber security solutions to automate the capability of vulnerability management, risk analysis, mitigation, and response.

a) Organizations should use AI for cyber defenses to proactively detect and mitigate threats that require a speed of response far greate r than human decision-making allows.

b) AI systems must function in a robust, secure, and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.

c) Organizations should implement AI security solutions to identify, predict, respond, and learn about potential cyber security threats with supervisor of human.

d) Organizations must take a risk-based approach before adopting AI technology.

e) AI systems should respect the dignity, privacy, diversity, and autonomy of individuals.

f) Organizations must ensure that AI systems respect and uphold privacy rights and data protection to ensure the security of data.

g) Organizations should identify potential security vulnerabilities, and implement resilience measure s that are proportionate to the magnitude of potential risk.

h) AI systems should be monitored and tested to ensure that they continue to meet requirements without compromising the ethics and governance of Organizations.

i) Organizations should develop policies and procedures for governing and managing secure of AI technology.

j) Organizations using AI in decision-making should ensure that the decision-making process is explainable, transparent, and fair.

k) Organizations should establish appropriate data collection, sharing, management, handling, and storage policy and procedure for AI.

6.31 IoT Security Process

The objective of this process is to secure the IoT and reduce their security risk through protecting the IoT system service, and device creation, deployment, installation, use, procurement, and managing continuous vulnerabilities in vendors, operators, and end-users.

a) Organizations should have a secure IOT infrastructure. As minimum:

1. default credentials for any IoT device/component must be changed, and the organization's password standard must be followed when changing credentials;

2. enable minimum services and features required to perform an operation when building and configuring new IoT devices/components; If a service or feature is not needed, disable it or, even better, uninstall it.

b) There should be an initial inventory of IoT devices/components and their configuration specifications.

c) Network and host logs for the IoT device/component and its associated environment must be collected, stored, and reviewed regularly.

d) All data must be collected, stored, processed, and transferred securely.

e) Provision devices and systems with unique identities and credentials should:

1. assign unique identities to all devices and on-premises or in-cloud systems;
2. assign unique and cryptographic credentials;
3. create mechanisms to facilitate the generation, distribution, rotation, and revocation of credentials;
4. create mechanisms to securely manage access to IoT services and resources;

f) Organizations must have authentication and access control mechanisms. As a minimum, they should:

1. establish clear trust boundaries based on the threat model and enforce access controls on all access outside those boundaries;
2. identify and mitigate issues with entry points that are vulnerable to forging or spoofing identities and unauthorized escalation of privileges;
3. consider deployment of services that authenticate

identities without hard-coding passwords, tokens, or other secrets;

4. use tamper-proof device hardware, and disable any unused hardware interfaces physically and/or at the firmware or operating system layer if the threat model includes potential physical access to devices by unauthorized actors;
5. enforce resource consumption limits and practice throttling to protect the availability of shared resources;

g) Organizations should deploy security auditing and monitoring mechanisms, As a minimum, they should:
   1. continuously collect and report activity metrics and logs from across IoT ecosystem;
   2. monitor on-device and related off-device activities, such as network traffic and entry points, process execution, and system interactions, for any unexpected behavior;
   3. use logs to further monitor events and troubleshoot issues;
   4. maintain and regularly exercise a security incident response plan, along with containment and recovery mechanisms;
   5. keep a record of security actions taken by the user, role, or service;

h) Organizations should minimize the attack surface of IoT ecosystem. As a minimum, they should:
   1. identify and eliminate unused entry points on devices, field gateways, and backend systems;

2. disable unused device sensors, actuators, services, and/or their unused functions;
3. disable unused functionality or insecure-by-default configurations;
4. use the least possible number of dependencies, such as third-party libraries and network services;
5. employ secure-by-default configurations across organizational IoT ecosystem;
6. only add well-maintained dependencies and establish a mechanism to keep them up to date;
7. regularly review and identify attack surface minimization opportunities that IoT ecosystem evolves;

i) The development of IoT products, and services should be based on the CMCSRS procurement process.

j) Procurement of IoT devices should be approved by INSA.

6.32 Block chain Technology Process

The objective of this process is to secure block chain technology products, platforms, and services, as well as to enhance block chain cyber security solutions.

a) Organizations should define and establish a business process and/or procedure for the block chain solution and their use cases.

b) All participating organizations on the permission blockchain shall define, document, implement, agree, and follow unified security policies in relation to blockchain-based services.

1. All organizations should agree on the relevant security policies, standards, and best practices to follow and comply with in relation to blockchains.
2. The unified security policies should include, but not be limited to, access control policy, cryptography policy, network, and communication security policy.
3. Organizations should establish and maintain relevant documentation such as processes, procedures, templates, records, plans, logs, and/or guidelines.
4. The unified security policies should be communicated to all users of the participating organizations on the blockchain platform.
5. The unified security policies should be reviewed at planned intervals, or in case a significant change occurs, on the relevant blockchain-based service and accordingly, they must be updated and approved by INSA.

c) All organizations should establish and agree on a process to define the data type to be stored on the blockchain along with the data owner's responsibilities.

d) Organizations should define, design, plan, and implement an Identity Access Management (IAM) solution for the permission blockchain-based service in line with the users' on-boarding and off-boarding processes

e) The Blockchain-based service access should cover at least the following privileges in line with the least privilege principle.
   1. read access to the blockchain;
   2. publish new transactions on the blockchain;
   3. the relevant account/identity is created, approved, enabled, modified, disabled, and removed as per Access Control Policy in relation to the blockchain;

4. access control can further be restricted to users' identities or credentials to provide content privacy of transactions;
5. periodically review the relevant account/identity along with its granted/assigned permissions/privileges and any access audit logs/reports;
6. continuous monitoring, oversight, and auditing of users' access to the blockchain-based service;
7. In case of any access violations and/or malicious transactions, generate an incident report in line with the approved Information Security Incident Management Policy.

f) All organizations should establish and agree on the architecture and procedure for the Hardware Security Module (HSM) implementation for securing the blockchain identity keys.

g) Access to smart contracts lifecycles management should be defined, controlled, logged, and monitored on a continuous basis, including the relevant processes and/or applications that any smart contract will be collaborating with.

h) Organizations shall establish a process for testing, analyzing, and auditing smart contract codes by INSA.

i) The smart contracts should be tested and audited against legal considerations, security vulnerabilities, bugs, and flaws by INSA.

j) Organizations shall establish a process and/or procedure for testing, monitoring, and evaluating the publication rate of a block and accordingly adjust influencing factors of the respective rate if required.

k) Organizations should manage cyber security risks in a blockchain network using cyber security frameworks, assurance services, and best practices to reduce risks against attacks and fraud.

l) Blockchain service providers, systems, and product developers must be licensed by INSA.

C. Enabling Processes

6.33 Information and Intelligence Management Process

The objective of this process is to create situation awareness and visibility to influence stakeholders at a strategic, tactical, and operational level and to have information superiority.

a) The scope of the intelligence should cover all issues, such as assets, vulnerabilities, threats, threat actors, threat sources, attack process, attack, and their impacts. It should cover tactical and operational intelligence types.

b) The information and intelligence to be managed should be timely, correct, interoperable, and have integrity.

c) This process should be triggered whenever there is a change of state in the internal and external environment.

d) The process should have sub-processes such as surveillance (observation), analyzing the information and planning its management, further analysis, and utilization of the intelligence, monitoring the impact of the intelligence, and improving the outcome. The whole process should be based on the National Cyber Security Intelligence Management Scheme.

e) The information and intelligence gathered should be utilized in its highest level for risk profile building, early warning, learning lessons, creating awareness, deterring threats, and so on.

f) The environment and infrastructure that enables this process should be established.

    1. Employees should be encouraged to provide information security information and intelligence.

2. Minimal technologies that provide visibility should be deployed.

3. There should be a system to monitor the external environment.

g) There should be a Team (which can be part of the Cyber Security Team) that gathers information and conducts analysis and reports to the Cyber Security Department head. The Information Security Monitoring Team can play this role based on the organization's context.

h) Organizations should report the intelligence to INSA.

i) After gathering all the intelligence, INSA develops intelligence and distributes them to the right authorities.

j) All the intelligence should be distributed to the National Cyber Command.

k) The organization should share its intelligence in a secure manner based on National Cyber Security Intelligence Management Scheme.

l) The intelligence and information gathered should be classified, labeled, and retained based on the National Cyber Security Classification Standard.

m) Intelligence will be classified and declassified based on the National Cyber Security Classification Standard.

n) This process cannot be outsourced to foreign actors. An organization that conducts outsourced services should follow the requirement.

o) The organization should have a threat warning level based on the National Cyber Security Intelligence Management Scheme.

p) INSA must develop national cyber defense statistics every year.

6.34 Cyber Security Communication, Documentation, and Knowledge Management Process

The objective of this process is to properly manage cyber security communication, documentation, and knowledge.

a) The organization should determine the need for internal and external communications relevant to the organization's information security including:
   1. on what to communicate;
   2. when to communicate;
   3. with whom to communicate;
   4. who must communicate; and
   5. the processes by which communication must be effected;

b) All Cyber security issues should be communicated to the right people at the right time.

c) The organization's information security leadership, governance, and management system should have:
   1. documented information required by this standard; and
   2. Documented information determined by the organization as being necessary for the effectiveness of the CSMS.

d) When creating and updating documented information, the organization should apply appropriate identification and description, format and media, and review and approval.

e) Documented information required by the organization's information security leadership, governance, and management system should be controlled to ensure:

1. it is available and suitable for use, where and when it is needed; and
2. it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

f) All information security knowledge should be documented, stored, and shared with the right personnel and organizations.

6.35 Cyber Security Cooperation and Collaboration Process

The objective of this process is to create collaborated and coordinated efforts on cyber security at national and sectorial levels.

a) The organization should create collaboration with organizations in it s sectorial and at national levels.

b) Organizations should sign a code of conduct when conducting cooperation with other organizations.

c) Organizations should share information security information, intelligence, knowledge, and experience for authorized bodies when they need it.

d) Disruptive Processes

6.36 Information Privacy Process

The objective of this process is to secure individual information and ensure compliance with legal and regulatory requirements for information privacy.

a) Organizations should develop information privacy policies aligned with the National Information Privacy Act and Directive.

b) The organizational cyber security management system should not compromise the privacy of individuals.

c) Organization collection, processing, storing, and sharing of personal information should be managed securely.

d) The organization should have an agreement with the individual regarding their information usage by the organization;

e) Organizational information privacy should protect individual's sensitive data including but not limited to:

1. personal social identity;
2. race or ethnicity;
3. personal financial;
4. Genetic or biometric data;
5. physical or mental health or condition;
6. sexuality life;
7. political opinion;
8. religion;
9. other personal information that requires caution will be included;

f) The organization should conduct information privacy audits to determine the level of compliance with relevant legislation and internal policies.

g) The organization should apply Controls for handling personally identifiable information.

h) The organization should establish an awareness program to make staff and external parties (e.g. customers, clients, and suppliers) aware of the importance of information privacy.

6.37 Security Clearance Process

The objective of this process is to ensure that personnel can be trusted to access a classified asset.

a) Personnel shoul d get security clearance and briefing before being granted access to a classified asset.

b) Organizations should brief individuals on the access privileges and prohibitions attached to their security clearance level before giving access, or when required in the security clearance renewal cycle.

c) Access to the classified asset should be dependent upon the granting of the required security clearance.

d) Authorization, security clearance, and briefings should be documented.

e) Security clearance should be revised based on the National Cyber Security Personnel Clearance Scheme.

f) Under strict circumstances, access to systems may be granted to personnel who lack the appropriate security clearance based on the National Cyber Security Personnel Clearance Scheme.

g) Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearance based on National Cyber Security Personnel Clearance Scheme.

h) Emergency access to systems processing, storing, or communicating TOP SECRE T assets is not permitted.

i) When personnel are granted access to a system under the provisions of temporary access they need to be closely supervised or have their access controlled in such a way that they only have access to information they require to undertake their duties.

j) Organizations should have a policy which addresses personnel security issues before, during, and after employment.

k) Organizations must ensure that employees, contractors, and temporary staff who require ongoing access to information and resources are eligible to have access; have had their identity established; are suitable to have access, and are willing to comply with the Government's policies, standards, protocols and guidelines that safeguard the organization's asset from threat.

l) Organizations must, as part of their risk management approach, identify designated security assessment positions (DSAPs) within their organization that require access to CONFIDENTIAL, SECRET, and TOP SECRET assets. They must maintain a DSAP register.

m) Organizational security vetting should be conducted based on the National Cyber Security Personnel Clearance Scheme.

n) Organizations must have in place personnel security aftercare arrangements, including the requirement for individuals holding security clearances to identify any significant change in personal circumstances that may impact their continuing suitability to access security classified resources.

6.38 Procurement, Development, and Maintenance Process

The objective of this process is to ensure cyber security is considered during the procurement, development, and maintenance of cyber security and selected ICT products and services.

a) All procurement, development, and maintenance of

information security products and services should be based on the engineering process.

b) All procurement, development, and maintenance should align with the corresponding requirements of this standard.

c) Organizations should include information security related requirements in the requirements for new asset procurement or development and enhancements to an existing asset.

d) Procurement of cyber security systems, products, and services should be approved by INSA.

e) Organizations should sign an agreement with their vendors which mandate the vendors to provide long time update and maintenance of the product, and service.

f) Cyber security products and classified ICT assets developed by local governmental organizations or private companies should be evaluated and certified by the INSA before they are made available on the market.

g) Information security and classified ICT services which are provided by local governmental organizations or private companies should be evaluated and certified by the INSA before they are made available on the market.

h) Certified information security and classified ICT products which are developed and made available by local governmental organizations or private companies should not be procured from foreign suppliers unless there is an exceptional case approved by INSA.

i) Certified information security and classified ICT services which are available from local governmental organizations and private companies should not be outsourced from foreign supplier s unless there is an exceptional case approved by INSA.

j) Organizations which procure information security products from foreign companies should require the companies to transfer knowledge and should sign a knowledge transfer agreement to build national capability to develop the products, unless it is allowed by INSA.

k) Organizations which procure information security and classified ICT products from foreign companies should require the companies to make the products open in order to add required additional features as necessary.

6.39 Supply Chain Relationship Management Process

The objective of this process is to manage cyber security breaches due to supply chains.

a) Organizations must ensure their product and/or service supplier complies with the requirements of this standard and other national cyber security regulations.

b) Organizations should prepare and implement a Supply Chain Relationship Management Policy and Procedure.

c) When outsourcing any part of an asset, there should be a security agreement that guarantees the fulfillment of the national cyber security standards and regulations.

d) Based on the requirements of this standard, cyber security requirements for mitigating the risks associated with suppliers' access to the organizations' assets should be agreed with the supplier and documented.

e) All relevant information security requirements should be established and agreed with each supplie rthat may access, process, store, communicate, or provide technology or service.

f) Organizations should regularly monitor, review and audit

the security compliance of their suppliers.

g) Based on the review and audit findings, organizations should manage changes and improve existing supply chain information security policies, procedures and controls, and countermeasures.

7. Stakeholders

7.1 Address Stakeholders' Security Requirements

a) The organization should identify their national and international stakeholders.

b) The organization should identify and address the security requirements and concerns of its stakeholders. Stakeholders include, but not limited to

1. **Customers –** require secure service and secure storage and processing of their information.
2. **Partners and Third parties –** organizations that have business relationships require their partners to process and store their information securely.
3. **National regulatory organization (INSA) –** required to implement security regulations such as standards.
4. **International regulatory organizations (e.g. ISO) –** require organizations, which accept their regulations, to effectively implement their regulations (e.g. standard).
5. **Competitors –** competent organizations may launch an attack to steal information or to affect the effective operation of the organization.
6. **Opponents –** who need to exploit or compromise the information system of the organization can be considered as stakeholders with negative interests.

8. Mission

The cyber security program should create an enabling situation for the organization to achieve its mission.

References

1. Commonwealth of Australia, 2012. Protective Security Policy Framework: Securing Government business.
2. Commonwealth of Australia, 2013. Protective security governance guidelines: Business impact levels.
3. ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems -Requirements.
4. UK Government, 2014. Cyber Essentials Scheme: Requirements for basic technical protection from cyber-attacks.

Annex A: Business Impact Leveling Guidance

The guidance given below is indicative to assist organizations in developing their own business impact level. The impact level is grouped in to national level economic, political and social impacts.

Level 1 (Low-medium)	Level 2 (High)	Level 3 (Extreme)
Could be expected to cause low to medium damage to the National interest by:	Could be expected to cause high damage to the National interest by:	Could be expected to cause extreme damage to the National interest by:
National Economic Impacts		
Impacts on Finance		
Causing low to medium financial damage to a major Ethiopian or Ethiopia-based organization or company, or financially disadvantaging a limited number of Ethiopian organizations or companies	Causing high financial damage to a major Ethiopian or Ethiopia-based organization or company, or disadvantaging several Ethiopian organizations or companies	Causing extreme financial damage to a major Ethiopian or Ethiopia-based organization or company, or disadvantaging several major Ethiopian organizations or companies
Impacts on Materials		
resulting low to medium and short-term material damage to national finances or economic interests	resulting high and short-term material damage to national finances or economic interests	causing high to extreme and long-term damage to the Ethiopian economy
Impacts on International Trade or Commerce		
causing low to medium- and short-term damage to international trade or commerce, with the potential to reduce economic growth in Ethiopia	causing high and short-term damage to international trade or commerce, with the potential to directly and noticeably reducing economic growth in Ethiopia	causing high to extreme and long-term damage to global trade or commerce, leading to prolonged reduction of economic growth in Ethiopia

Impacts on National Infrastructure		
Causing low to medium damage on significant national infrastructure	Highly damaging or disrupting significant national infrastructure	shutting down or extremely disrupting significant national infrastructure
National Political Impacts		
Impacts on Government Policies and Strategies		
cause low to medium hindrance on the development or operation of government policies and strategies	highly impedes the development or operation of government policies and strategies	extremely impedes the development or operation of major government policies and strategies
Impacts on International Negotiations and Diplomacy		
causing low to medium disadvantage on Ethiopia in international negotiations or strategy	highly disadvantaging Ethiopia in international negotiations or strategy	extremely disadvantaging Ethiopia in major international negotiations or strategy
causing low to medium- and short-term damage or disruption to diplomatic relations	causing high damage or disruption to diplomatic relations, or raising international tension	causing extreme damage to diplomatic relations especially with friendly governments, or directly provoking international conflict
Impacts of Public Confidence		
resulting in low to medium loss of confidence in government	resulting in high loss of confidence in government or temporarily damaging the internal stability of Ethiopia or friendly countries	extremely threatening the internal stability leading to widespread instability or collapse of internal political stability of Ethiopia or friendly countries
Impacts on Crime Prevention		
hindering the detection, impeding the investigation, or facilitating the commission of low to medium-level crime	hindering the detection, impeding the investigation of, or facilitating the commission of a high-level crime	causing major, long-term impairment to the ability to investigate extremely organized crime undertaken by an organized crime group

Impacts on Defence Operations		
causing low to medium damage to the non-operational effectiveness or security of Ethiopian or allied forces without causing risk to life	causing high damage to the non-operational or operational effectiveness or security of Ethiopian or allied forces that could result in risk to life	resulting in extreme damage to the operational effectiveness or security of Ethiopian or allied forces
Impacts on Intelligence Operations		
causing low to medium damage to Ethiopian or allied intelligence capability	causing high damage to Ethiopian or allied intelligence capability	causing extreme damage to Ethiopian or allied intelligence capability, or to the effectiveness of extremely valuable security or intelligence operations
National Social Impacts		
Impacts on Human Life		
endangering individuals - the compromise of information could lead to serious harm or potentially life-threatening injury to an individual	endangering small groups of individuals - the compromise of information could lead to serious harm or potentially life-threatening injuries to a small group of individuals	leading directly to widespread loss of life – the compromise of information could reasonably be expected to lead to the death of a large number of people
Impact on National Culture and Values		
resulting low to medium adverse effect on the culture and values of the society	resulting highly adverse effect on the culture and values of the society	resulting extremely adverse effect on the culture and values of the society
Impacts of Public Psychology (Psychological Warfare)		
Causing low to medium psychological impact on the society.	Causing high psychological impact on the society.	Causing extreme psychological impact on the society.

Annex B: Asset Classification Guidance

Organizations must follow the following four levels of classification while classifying their assets:

1. **TOP SECRET:** this is the most sensitive asset requiring the highest levels of protection from the most serious threats. If this asset is publicly disclosed without proper authorization, it would cause "exceptionally grave damage" to national security. For example, a compromise could cause widespread loss of life or else threaten the security or economic well-being of the country or friendly nations.
2. **SECRET:** This is a very sensitive asset that requires heightened protective measures to defend against determined and highly capable threat actors. Its unauthorized disclosure would cause "serious damage" to national security. For example, a compromise could seriously damage military capabilities, international relations, or the investigation of serious organized crime.
3. **CONFIDENTIAL:** this is a sensitive asset that requires protective measures to defend against threat actors. It would "damage" national security if publicly disclosed without the proper authorization.
4. **PUBLIC:** There may be occasions when it is necessary to indicate that a document does not carry sensitive information. In these cases, the term PUBLIC should be used.

+251-11-371-71-14
Fax: +251-11-3-20-40-37
P.O.BOX: 124498
contact@insa.gov.et
www.facebook.com/INSA.ETHIOPIA
www.insa.gov.et
Addis Ababa
Ethiopia