المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

Baseline Cyber Security Controls

Ministry of Interior
National Cyber Security Center

2022

Table of Content

Introduction

Information is an important asset for all entities. Entities use the information to serve people, make well-informed decisions, and create new information. Information Technology helps all entities process, store and manage all information. Consequently, protecting information is considered a critical function that needs to be accomplished with devotion from all people working for the entity.

Information moves through networks which are playing a vital role in the community. Individuals depend on networks in many aspects of life. People from various professions use the networks to perform daily government, business, or industry tasks. Networks allow people to communicate, cooperate and collaborate to accomplish goals, complete projects, and achieve an entity's success. The amount of information shared among people through networks is tremendous.

The number of individuals connecting to the networks using computers and smart devices is increasing on a daily basis. Individuals use many applications, browse websites and download large amounts of information, files, media, and applications. Leveraging this wide usage of networks by individuals, many entities provide services through the digital channels that the networks enable. Entities tend to digitize and automate as many services as possible, especially after people have touched the gains of using electronic services. The number of services or applications provided through smart devices increased accordingly.

Customers can order and purchase products virtually from the comfort of their homes. Individuals conduct transactions with government entities from any location as long as they can access the network using computers or smart devices. Individuals also complete payments to businesses and government entities electronically. Moreover, employees work remotely and access their entities' networks.

The ease and comfort provided by such networks come at a cost. The Internet is the core and backbone in which all the communications, transactions, and information sharing are conducted. The Internet allows services and applications to be available to people outside the entities. The intended people are permitted access to certain paths and channels. However, criminals can use these paths to perform malicious acts and cause harmful effects and impacts. Moreover, criminals are not only attacking facilities connected and visible on the Internet. Attackers are able to make their way through private networks and then enter critical systems to cause damage and malfunctions. The risks posed by criminals and hackers have increased tremendously in recent years.

Entities are striving to handle attacker threats and confront risks. Cybersecurity professionals realize the criticality of their responsibility to protect the networks from all types of cybersecurity attacks. Cybersecurity professionals use many tools, technologies, and solutions to create layers of defense for the networks. Over the years, many cybersecurity practices, habits, and conducts have proved effective in the war against attackers. Many attacks have been thwarted when entities followed certain cybersecurity practices, habits, and conducts to defend entities' networks and Information Technology (IT) infrastructure. Cybersecurity Professionals have exerted enormous efforts to collect all cybersecurity practices, habits, and conducts and document them to promote the best cybersecurity practices.

The National Cybersecurity Center (NCSC) in the Kingdom of Bahrain has prepared the "Baseline Cybersecurity Controls" document which contains controls that promote best practices to protect information. This document addresses all private and public entities' essential and minimum high-level cybersecurity requirements. Moreover, this document's controls provide the baseline with which private and public entities can build the necessary and foundational layer of cybersecurity.

This document's controls target all private and public entities of all the critical sectors in the Kingdom's Critical National Infrastructure (CNI). Following the document's controls is mandatory for the private and public entities being part of the Kingdom's CNI. CNI entities are expected to build an essential and foundational layer of cybersecurity that protects them from a wide set of cyber-attacks and threats. Nevertheless, other entities are encouraged to follow the controls described in this document to their benefit and interest.

Domain 1 Cybersecurity Governance

The first step in governance would be to establish a clear mandate, delegation of authority, then roles and responsibilities of the cyber security function. The entity shall determine its cybersecurity objectives, stakeholders, and activities are understood and prioritized and could be maintained as a separate/dynamic document and shall be used to determine the scope of the program / determine audit scope.

Subdomain 1.1 Cybersecurity Goals

The main objective of this subdomain is to define cybersecurity goals and objectives that guide the entity during the planning and implementation phases of cybersecurity initiatives and projects.

Control 1.1.1 Cybersecurity goals and objectives must be defined and determined.

Defining cybersecurity goals and objectives help the entity set its direction. The goals aid in understanding the priorities of what to protect within the assets and from what threats. Cybersecurity goals must be effective and measurable through defining and applying appropriate measurements criteria, and metrics.

Control 1.1.2 A roadmap must be created to achieve the cybersecurity goals and objectives.

The roadmap consists of the initiatives and projects to achieve cybersecurity goals and objectives. The initiatives and projects should be defined, determined, prioritized, and identified resources needed.

Control 1.1.3 Cybersecurity goals and objectives must be reviewed periodically.

The periodic review ensures that the cybersecurity goals and objectives align with the entity's goals, laws, and regulations. The review helps identify the areas that need improvements in the goals and objectives.

Subdomain 1.2 Roles and Responsibilities

The main objective of this subdomain is to define clear responsibilities and accountability across the cybersecurity function within an entity. Also, this subdomain is intended to ensure that all cybersecurity tasks in the entity are completed effectively, securely, and consistently by a cybersecurity function (e.g., unit, department, division) to protect sensitive information and key operational services. Defining roles and responsibilities strengthens the entity's accountability and guarantees segregation of duties.

Control 1.2.1 All employees are responsible for cybersecurity.

Cybersecurity is a shared responsibility among all employees. Cybersecurity responsibility must be clearly defined in the entity; therefore, every employee should be aware of cybersecurity responsibility.

Control 1.2.2 Cybersecurity function's responsibilities must be assigned to dedicated employee(s).

Each entity should have a cybersecurity function with one or more appropriately trained employee(s) holding relevant cybersecurity certifications. When possible, the cybersecurity function should be separated from Information Technology (IT) function or the Information and Communication Technology (ICT) function. The head of the cybersecurity function reports directly to the head of the entity or delegated person.

One of the main cybersecurity responsibilities is to assess cybersecurity risks. Some entities can assign cybersecurity risk responsibility to a dedicated risk function, but the two functions must work closely. If there is no dedicated risk function, this responsibility should be assigned to the cybersecurity function. Other responsibilities of the cybersecurity function include identifying and remediating vulnerabilities. Moreover, the cybersecurity function must create the appropriate security policies, standards, procedures, and guidelines. As well as, the cybersecurity function must perform but not be limited to monitoring systems, audits, security & applications logs.

Additionally, the cybersecurity function must improve the entity's security posture by implementing all required cybersecurity controls, as presented in this document. Promoting a security culture among all employees is one of the critical responsibilities of the cybersecurity function. Other responsibilities include but are not limited to physical security, encryption, and access control.

Control 1.2.3 The senior management must support the cybersecurity function.

The senior management shall be held accountable for the cybersecurity function. Senior management's support plays a crucial role in the success of cybersecurity function to achieve cybersecurity objectives. The management can allocate adequate funding to fulfill cybersecurity needs and requirements. In addition, the management may encourage all employees to embrace and conduct a cybersecurity culture. Senior management ensures that the cybersecurity function is empowered and strategically aligned with the entity's long-term and short-term goals. The management also provides leadership and guidance to ensure that cybersecurity does not affect operations negatively.

Subdomain 1.3 Risk Management

Risk Management is the process of identifying, assessing, and reducing risks to an acceptable level. This process is considered the basis for determining the necessary controls to treat cybersecurity risks and set up the contingency plan. Ultimately, to protect the information assets, the risks' impact, likelihood, and vulnerability have to be clearly and accurately assessed and analyzed.

Control 1.3.1 A comprehensive risk management plan must be developed.

Planning is one of the most crucial factors for the success of any process or project to ensure effectiveness and efficiency. Accordingly, the entity must initiate risk management with a comprehensive plan that includes the following:

- The criteria that are used as the base of the prioritization process in all phases of the risk management process and the ones for considering the "**Risk Appetite**".
- The scope and boundaries of risk management process of the entity. Scope and boundaries can be identified by determining the business areas and people covered.
- The overall organization of the risk management process including determining roles and responsibilities, organizational structure and charters.

Control 1.3.2 Accurate risk assessments must be performed.

As the core step of risk management, a risk assessment should be prepared carefully and accurately, especially since its results reflect the whole cybersecurity status. Furthermore, top management should review and approve the risk assessment results. The assessment results help the decision-makers determine the appropriate actions and priorities for managing risks and for implementing controls selected to protect against these risks. Risk Assessments include the following steps:

- **Assets Identification:** Identifies all information assets to be considered in the information security risk assessment and how they are connected. The information assets include data, physical assets, software assets, computing, communications services, general utilities, qualifications, skills, and experience.

- **Risk Identification**: In this step, the task is to define and extract a list of risk scenarios, risk owner (if applicable), and the consequences related to information assets and business processes through the comprehensive identification of information assets, threats, and vulnerabilities.

- **Risk Analysis:** This is to determine the likelihood of occurrence of the identified risk scenarios, consideration of the causes and sources of risk, criticality and context of the risk, impact on the entity, and existing controls.

- **Risk Evaluation:** After estimating all the components and levels of existing controls, the risk scenarios may be classified and prioritized.

Control 1.3.3 Appropriate risk treatment and mitigation plans must be determined.

After identifying, analyzing, and evaluating the risks based on the impact versus likelihood chart, a decision must be taken to respond to the risks. Responses to the risks may be any of the following:

- **Risk Mitigation**: An action taken by the entity to reduce the risk. Risk Mitigation can be performed through setting security controls that reduce the risk likelihood or/and impact. Risk Mitigation does not eliminate the risk but minimizes the impact on assets or the likelihood of the risk happening.
- **Risk Transfer**: This decision refers to reducing the impact of the risk by transferring the risk liability and responsibility to other entities. The most common example is purchasing insurance. Usually, the

management takes this decision when the risk has a high impact, but the likelihood is exceptionally low. The entity is still not protected from losses and impacts by transferring the risk because the entity is ultimately responsible for managing the risk.

- **Risk Avoidance**: The elimination of all the probabilities that may cause a given risk. Risk Avoidance is taken when plans, projects, or processes parameters are changed or eliminated. This decision is usually taken in case of several events, such as if the cost of mitigating the risk is higher than its benefit, the risk is unacceptable by the management or cannot be transferred.
- **Risk Acceptance**: Accepting the risk means that the decision-maker recognizes and accepts the given risk without taking any mitigation or elimination actions because the possible consequences and impacts of the risk can be forgiven. The decision is sometimes taken when the level of the risk is within the entity's risk appetite or when the potential loss associated with the risk is less than the cost to avoid or mitigate the risk.

Control 1.3.4 Risks should be periodically reviewed and monitored.

Risks change over time, depending on changes in the risk factors. Therefore, the entity must periodically review and monitor the risks. Changes in the risks must be identified and addressed. Reviewing the risks includes ensuring that the proposed mitigation controls and mechanisms are checked and are functioning as desired. Risk evaluation should be linked to change management processes. Risks should be re-evaluated in response to changes in products, services, internal organization structures, or regulatory requirements.

Control 1.3.5 Risks should be communicated.

This document's controls emphasize the entity's role in sharing information about risk with stakeholders and senior management through dedicated channels by the responsible persons within the risk management team.

Subdomain 1.4 Policies, Standards, Procedures and Guidelines

This subdomain ensures that all processes are well organized, governed, and documented. The term "Cybersecurity Policy" includes cybersecurity policies, standards, procedures, and guidelines for this document. Well-written policies ensure that all the goals and objectives are clear, understandable, and achievable. Appropriate procedures and guidelines support the implementation of cybersecurity requirements.

Control 1.4.1 Cybersecurity Policy must be defined and prepared.

Cybersecurity Policy is the foundation of an entity's cybersecurity program. The cybersecurity policy helps guide and shape an employee's behavior towards the acceptable use of the entity's information assets. The Cybersecurity Policy should be developed to be aligned with the requirements of NCSC and sector regulators. The Cybersecurity Policy contains best practices promoted by various local, national, and international standards. Local and International laws and regulations must be considered during the preparation of the Cybersecurity Policy. The Cybersecurity Policy should be based on the assessment of risks and Confidentiality, Integrity, and Availability (CIA) of the information assets.

Control 1.4.2 Cybersecurity Policy must be approved, issued and owned by the entity's senior management.

Senior management's approval, issuance, and ownership of the Cybersecurity Policy is critical in supporting the cybersecurity function. The approval expresses the importance of the Cybersecurity Policy and delivers a strong message to all employees to adhere to the Cybersecurity Policy and be held accountable. Failure to follow the Cybersecurity Policy may lead to disciplinary actions. The head of the department can approve procedures and guidelines instead of senior management.

Control 1.4.3 Approved Cybersecurity Policy must be communicated to and implemented by all employees.

Approved Cybersecurity Policy should be published and communicated in a relevant, accessible, and understandable form to the employees. Employees should also be instructed to carefully comprehend the entire Cybersecurity Policy to implement all the instructions and guidelines. Furthermore, employees should be informed of the point of contact in case of any issue.

All employees should be compliant with and follow the Cybersecurity Policy to ensure the success of the Cybersecurity program. Therefore, each employee is responsible for implementing Cybersecurity Policy requirements.

Control 1.4.4 Cybersecurity Policy should be regularly reviewed and updated.

The entity should regularly review and update the Cybersecurity Policy in response to rapid developments and changes in the cybersecurity field, the organizational environment, business circumstances, legal conditions, technical environment, or cybersecurity incidents and threats. For example, if a legal element related to

cybersecurity is modified, the entity should review and update Cybersecurity Policy as per the requirement after the amendment.

Subdomain 1.5 Business Continuity Management

The purpose of implementing Business Continuity Management (BCM) is to identify the impacts that might threaten the continuity of the critical operations, services, and processes. After identifying the impacts, BCM aims to ensure the availability of essential functions, services, and processes and enhance overall business resilience. BCM also includes the actions that should be taken to minimize the identified impacts resulting from cybersecurity incidents, disasters, disruptions, or network/infrastructure changes. Finally, the process of recovering the information assets from failures and disasters is documented within the Disaster Recovery Plan (DRP).

Control 1.5.1 Business Continuity Policy necessary to maintain business continuity and processes availability must be defined.

To prepare the Business Continuity Policy, the entity uses the BIA and the risk assessment to examine various threats. Failure to prepare the policy may cause serious harm to the entity's operations, services, and processes.

Control 1.5.2 A comprehensive plan must be established and built to describe the whole BCM process including the resources needed and scope of work.

Business Continuity Plan (BCP) describes how the entity can minimize the impact of cybersecurity threats and recovery actions. When disasters occur, the entity must quickly respond to protect information assets and restore critical business functions and services. Therefore, the BCP must include all steps involved in response to disasters.

Control 1.5.3 A Business Impact Analysis (BIA) must be performed to prioritize the protection and maintenance of the availability of the processes.

The BIA is a core part of the BCP. Through the BIA, the entity identifies interdependencies and requirements of systems, processes, suppliers, other departments, facilities, and supplies. Furthermore, the entity specifies IT components, systems and people. In addition, the entity identifies the people's qualifications, skills, and experience related to critical operations, services, and processes. The maximum downtime limit of the IT components, systems, and the most likely scenarios to impact them should also be identified.

Control 1.5.4 Disaster Recovery Plan (DRP) must be developed.

DRP helps entities in executing recovery actions in response to a disaster. DRP defines how to protect the entity's data that can be restored from data backup images. The frequency of data backup, including offline backup and the acceptable recovery time, must be determined in the DRP. Furthermore, DRP details the restoration process clarifying the responsibility of each employee.

Control 1.5.5 BCP and DRP must be periodically tested and reviewed.

The periodic review of BCP and DRP ensures that both are aligned with the entity's business objectives. The results of BIA should be reviewed regularly or when there is an effective change to ensure that the results are valid and updated.

The periodic tests support identifies and treats weaknesses and gaps in the BCP and DRP. Tests must be validated by business functions and should not be limited to technical and IT staff. All teams involved, including juniors and seniors, must be invited to the live testing of the BCP and DRP so that everyone is familiar with the process.

Physical copies of the BCP and DRP need to be available at the main and business continuity sites. Therefore, physical copies can be reached when a cyber-attack prevents electronic copies.

The entity should be confident that the DRP helps minimize and alleviate the effects and losses resulting from the failures and disasters. To be prepared for any failure or disaster, the entity must perform periodic testing of DRPs and backups, including restoring them.

Domain 2 Cybersecurity Training and Awareness

Employees lacking sufficient cybersecurity knowledge and skills might pose threats or vulnerabilities to the state of the entity's security. Adversaries can use vulnerabilities resulting from employee misconduct to get access to the entity's network. The purpose of this domain is to ensure that all employees are being equipped with sufficient knowledge and skillsets that contribute towards cybersecurity function efforts in protecting information assets and limit the human error that may result in security risks. The training and awareness program shall be built to promote a cybersecurity culture amongst all employees.

Subdomain 2.1 Cybersecurity Training

Control 2.1.1 All employees must be assessed on their cybersecurity knowledge and skills.

All employees must be assessed as a preliminary step to identify the gaps in employee cybersecurity knowledge and skills.

Control 2.1.2 Cybersecurity training needs must be identified.

The entity should identify the content and topics of the cybersecurity training based on the identified gaps and the nature of employees' jobs and tasks.

Control 2.1.3 The cybersecurity training must be periodically evaluated and reviewed.

The training must be provided and periodically evaluated to check whether it successfully improved the employees' knowledge and skills.

Control 2.1.4 Cybersecurity training must address new threats.

The entity should provide relevant and focused training to employees immediately after newly discovered cybersecurity threats that might affect cybersecurity.

Subdomain 2.2 Cybersecurity Awareness

Control 2.2.1 A cybersecurity awareness program should be developed.

The entity should develop a comprehensive plan that describes a cybersecurity awareness program. Technical personnel should create the awareness program and determine the program's scope and methodologies. The cybersecurity awareness program should be tailored to address all job levels and roles. The program ensures all employees, including top management, understand the cybersecurity policies to encourage employees to

implement the tasks within the policies' instructions and guidelines. The cybersecurity awareness program should start with a comprehensive evaluation of the current level of employee awareness. Multiple techniques can be used in the evaluation, such as surveys, quizzes, popup scenarios, and simulations. Based on this assessment, the entity can develop the program focusing on weaknesses. The program must be conducted using multiple tools, methodologies, and techniques such as workshops, emails, and campaigns.

Control 2.2.2 The cybersecurity awareness program should be periodically assessed and reviewed.

Measuring the success of the cybersecurity awareness program involves conducting assessments and periodical reviews for the program. The entity should measure whether employees' behavior, knowledge, and skills in handling information and computers have improved. For example, the entity may conduct social engineering tests for employees through simulated and organized phishing attacks. The results are used in updating and enhancing the program.

Domain 3 Cybersecurity Defense

Subdomain 3.1 Asset Management

One of the core subdomains of Cybersecurity defense is asset management because of the importance of knowing and protecting the assets owned by the entity. The entity assets may include but are not limited to hardware, software, information systems, information services, and information stored within the entity.

Control 3.1.1 Assets must be identified, classified and maintained in an inventory.

Identifying all the assets gives the entity an adequate visibility to protect the assets efficiently. Therefore, entities must identify all the assets. When possible, assets are identified automatically on a regular basis. Network scanners can provide valuable aid in identifying assets that are connected to an IP network. Network drawings or diagrams should be maintained.

All information stored in the devices, documents, and technologies must be classified when applicable based on Law No. (16) of 2014 concerning protection of state information and documents; otherwise, the classification must be based on international standards. The classification determines the sensitivity of the information to identify the protection level. The classification should be a part of the entity's Cybersecurity Policy that outlines the authority and access control.

As one of the entity procedures, the entity should automatically maintain an inventory or register of all identified assets. The entity should record asset details such as, and not limited to, asset identification (ID), asset name or description, asset function, asset classification, asset owner, asset custodian, physical asset location, license details. The inventory or register should be periodically reviewed.

Control 3.1.2 Asset owners, custodians and users must protect the entity's assets.

Asset owners should be at least assigned the following responsibilities:

- Define and regularly review classifications, access restrictions, and safeguards following applicable policies and laws.
- Designate asset custodians with the appropriate skills and tools to protect the assets. The skills can be provided through the training program.
- Identify the access privileges of the users and grant permissions.

Asset custodians must be at least assigned the following responsibilities:

- Ensure the implementation of security requirements on the assets.
- Deliver services in accordance with defined service requirements.
- Report designated asset performance and security regularly.
- Ensure all software and operating systems are updated and patched.

Asset users must be assigned the following responsibilities:

- Follow the organization's cybersecurity practices and instructions.
- Acquire the appropriate cybersecurity knowledge and skills.

Control 3.1.3 Endpoint protection must be deployed on all devices connected to the network.

Endpoint devices connected to the entity's network must be protected from attacks and threats. Endpoint protection is not limited to antivirus software. Endpoint protection must involve various functionalities such as but not limited to Anti-malware, Endpoint Detection and Response (EDR), device management and control, and host firewall.

Control 3.1.4 Cybersecurity controls must be adopted in the Software Development Life Cycle (SDLC).

The goal of the SDLC methodology is to produce software with high quality and the lowest costs in the shortest time possible. Adequate security controls must be incorporated in the SDLC to minimize security issues in the software or application.

Software development must be done in the development environment that is segregated from the testing and production environments. Segregation reduces the risk of accidental or unauthorized modifications by developers that could compromise the application's integrity or availability.

The application's source code must be reviewed and examined manually and/or automatically. The review must be conducted periodically to detect new vulnerabilities and an effective change. The source code review aims to identify any security-related weaknesses, flaws, or potential vulnerabilities in the code and detect malicious code, insecure coding practices, backdoors, and weak cryptography. Identifying the mentioned issues helps developers understand how to make the application's source code more secure.

Control 3.1.5 Assets must be disposed of securely when no longer required, through formal and clear procedures.

To minimize the risks of confidential information leakage to an unauthorized persons, formal procedures for the secure disposal of assets must be established, including the proper steps for assets disposal. While developing the procedures, the classification of information stored in the assets must be considered. A certain course of action shall be described for each category.

Subdomain 3.2 Access Control

The purpose of this subdomain is to ensure that proper controls are in place to prohibit or minimize unauthorized users from gaining access to information assets within systems, applications, and networks (collectively referred to as information processing resources).

Control 3.2.1 Requests for access to information processing resources must be reviewed in accordance with business and cybersecurity requirements and principles.

No user should be granted access to information processing resources unless a request is provided, reviewed, approved, implemented, and verified. The same applies to processes and systems accessing information processing resources to accomplish certain tasks. When accumulated, the requests help the entity identify or record all users, systems, and processes that need access to the information processing resources. The entity must know all users, systems, and processes accessing the information processing resources. Detected access from an unknown user, system, or process must be denied.

The relevant personnel must review all new access requests. To be approved, access requests must follow business and cybersecurity requirements that involve some crucial principles in protecting information processing resources from any possible unauthorized access. One of such principles is the "Need to Know" principle which requires the entity to restrict and control role-based access to information processing resources. Access is granted only to users whose job duties, roles, and responsibilities involve the need to access and use data or information. Otherwise, the request should be rejected, and access should not be granted. Conflicting roles (e.g., Requestor and Approver roles) must be considered and shall be segregated to ensure that no individual has access to control all phases of an operation/process.

Another principle is the "least privilege" principle, so the user can only do the necessary activities based on the user's role and duties. Giving a user, system, or process the ability to perform unnecessary actions increases the risks to information processing resources. Accounts with more privileges enable attackers to access more information processing resources or perform activities beyond those available to accounts with less privileges. The entity must limit the number of employees with privileged accounts. Moreover, the usage of privileged accounts must be monitored.

Control 3.2.2 Authentication, Authorization, and Accountability (AAA) must be performed when granting users, systems or processes access to information processing resources.

Authentication is the process of checking whether someone or something is claiming the correct identity. Authentication must be applied by requesting and verifying the user's credentials to access information processing resources.

Authorization is the process of determining whether a user, system or process is allowed to access information processing resources or perform certain actions. The authorization process is mandatory to determine whether the verified user, system, or process has permission to access or use the information processing resources.

Accountability is the process of ensuring that a user, system, or process is held responsible by observing and tracing back actions and events that occurred. Accountability should be applied to all authorized users, systems, or processes.

Control 3.2.3 The necessary measures for the authentication and authorization processes must be implemented.

All users of information processing resources must be assigned a unique identifier (user-ID) to ensure accountability while accessing information processing resources. Any action performed after getting access can be traced to that user. If the entity detects that the user has performed any suspicious or harmful activities, the entity must investigate the incident and take appropriate actions.

Attackers use techniques to guess user account credentials by using a list of possible credentials in the login process. The entity must lock out the account after a certain number of failed login attempts.

Control 3.2.4 Multi-Factor Authentication (MFA) must be implemented for information processing resources

Multi-factor authentication (MFA) is a method where two or more factors or credentials must be used to complete the authentication process. Factors can be: (i) something the user knows (e.g., complex password/PIN); (ii) something the user has (e.g., device/card); (iii) something the user is (e.g., voice/fingerprint); (iv) something the user does (e.g., talk/signature); (v) somewhere the user in (e.g., location). MFA adds a layer of security, making access to information processing resources harder for attackers. If one of the factors or credentials is compromised (e.g., a password is leaked), the account cannot be breached without further credentials.

Control 3.2.5 Privileges and access rights of user accounts must be reviewed periodically and when there is a change in user's duties, position or department.

Periodic review and re-evaluation of all privileges and access rights should be performed to all user accounts to ensure appropriate access rights or privileges are given. When the user's position or duties change; or leave the entity, the account must be reviewed accordingly.

Control 3.2.6 Teleworking should be done based on identified cybersecurity practices based on this document and/or other international standards.

Each entity must implement all cybersecurity practices for teleworking based on the cybersecurity controls presented in this document and/or other international standards.

Control 3.2.7 Email messages must be protected using email filtering solutions and authenticated by enforcing Domain-based Message Authentication, Reporting, and Conformance (DMARC) on inbound and outbound emails.

Email messages filtering involves scanning, analyzing, and categorizing email messages. Authenticating email messages can be ensured by enforcing DMARC standard, an email authentication method that helps prevent attackers from spoofing the organization and domain of the entity.

Subdomain 3.3 Vulnerability Management and Penetration Testing

The purpose of this subdomain is to ensure that proper controls are in place to decrease the number of undetected exploits or ignored vulnerabilities within systems, applications, and networks (collectively referred to as information processing resources).

Control 3.3.1 Periodic vulnerability assessments must be conducted to detect weaknesses within information processing resources.

A vulnerability is a weakness or error in a system or device's design, including code, architecture, implementation, flow, etc. Threat actors exploit vulnerabilities to access information processing resources and conduct malicious activities. Therefore, the entity must conduct periodic vulnerability assessments at least every three months. Vulnerability assessment is the process of defining, identifying, classifying, and prioritizing vulnerabilities within information processing resources. The entity may use an automated testing tool such as vulnerability scanner tools.

Control 3.3.2 Vulnerability assessments must be conducted before deploying a new system to the network or any effective infrastructure changes.

Besides the periodic vulnerability assessments, the entity must conduct the same process before any effective changes are made in the infrastructure, application flow, network, user segment type etc. (e.g., adding new services, installing new equipment). The purpose is to identify weaknesses and/or risks within the information processing resources that might result in compromise of information processing resources by threat actors.

Control 3.3.3 Detected vulnerabilities must be addressed, and proper corrective action must be performed based on vulnerabilities classifications and priorities.

After vulnerability assessment, proper corrective actions must be performed to treat the discovered vulnerabilities. Most critical vulnerabilities must be given top priority. Some vulnerabilities cannot be treated immediately, such as a critical application running on an unsupported operating system and is not compatible with updated operating systems. Senior management should be made aware of the risks associated with using applications with vulnerabilities.

One example of corrective actions is patch management which aims to apply updates to the software to treat the discovered vulnerabilities before being exploited by attackers. Patches shall be tested in an isolated test environment before being applied in production.

Control 3.3.4 Periodic penetration testing must be conducted to detect weaknesses in information processing resources.

After vulnerability assessment, penetration testing must be performed annually and conducted either manually or automatically using software applications. First, the testers or assessors gather information about the target then identify possible access points. Next, a cyber-attack is simulated, and the search for weaknesses within the information processing resources starts.

Penetration testing shows technical weaknesses and indicates defects in adherence to the Cybersecurity Policy and the employees' cybersecurity awareness. Penetration testing helps in identifying how the entity detects and responds to cyberattacks. Hence, application developers can identify the weaknesses in their codes, and system administrators can identify the weaknesses in their systems. The weaknesses discovered encourage system administrators and application developers to enhance their cybersecurity knowledge and education. The scope of penetration testing must be defined and approved by the senior management. The scope involves the systems, locations, techniques, and tools used in the test. The entity should plan on the type of penetration testing, whether external or internal.

Control 3.3.5 Identified weaknesses in information processing resources must be treated.

The identified weaknesses must be prioritized, and a remediation plan must be developed to treat the weaknesses.

Subdomain 3.4 Encryption

The purpose of this subdomain is to ensure the proper and efficient use of encryption to protect systems, applications, and networks (collectively referred to as information processing resources).

Control 3.4.1 All data and information on all levels must be encrypted in transit and at rest based on NCSC recommendations and requirements.

Stored and transmitted information and data must be protected using encryption. Unauthorized users are not able to read the encrypted information. Information in transit may travel through the public network infrastructure, making encryption necessary.

Control 3.4.2 Encryption keys must be managed and protected during the lifecycles.

Unprotected encryption keys might lead to the exposure of sensitive information. To create strong and reliable encryption keys, which must belong and be rotated frequently. Furthermore, the employee responsible for creating and managing the keys must not access the protected data. Moreover, using the same encryption key for different applications should be avoided. Finally, the encryption keys must be stored in a secure manner, such as Hardware Security Module (HSM), to safeguard the keys.

Subdomain 3.5 Physical Security

The purpose of this subdomain is to ensure the protection of all Information Technology (IT)/Operational Technology (OT) assets, including systems, applications, and networks (collectively referred to as information processing resources), from unauthorized physical access, loss, theft, and damage.

Control 3.5.1 IT/OT Information processing resources must be physically secure to prevent unauthorized physical access, damage and interference.

IT/OT equipment and devices could be installed in locations that are accessed by different people, including offices, conference rooms, server rooms/data centers, disaster recovery centers, and security surveillance centers. The availability of the information processing resources can be at risk of theft, destruction or manipulation with their settings.

Therefore, measures must be implemented to protect all IT/OT assets based on their criticality and location. Entrance and exit management systems with MFA, lockable doors and partitions, physical access management

systems, access control devices, lockable cabinets or security containers, protection of power equipment and cabling, UPS (uninterruptable power supply) and others may be installed to protect all IT/OT assets. The records of the entrance and exit management systems must be protected. The keys to doors, cabinets, and containers must be kept safe.

Control 3.5.2 IT/OT Information processing resources must be physically secure from environmental threats.

Depending on the outcome of risk assessment, adequate measures and procedures must be implemented to address and respond to environmental threats including fire, floods, earthquakes, and others. The entity must control and monitor water leakage, humidity, and temperature levels in the equipment locations. Moreover, the entity must install a fire detection and suppression systems. Information processing facilities must provide power supply from multiple sources like UPS, power generator etc. Building Management Systems (BMS) should be utilized for monitoring and alerts based on the criticality and entity size. When possible, IT/OT assets should be monitored remotely and regularly.

Control 3.5.3 Appropriate security measures must be implemented to protect against the risks of using portable and mobile devices.

Portable and mobile devices must be used carefully when connected to the entity's network. Before allowing the network connection, the devices should be authenticated and authorized. Portable and mobile devices must be disabled when lost or stolen. Backup including offline backup for the data stored on portable or mobile devices must be maintained. Access to sensitive information must be restricted. Endpoint protection solutions must be applied to portable and mobile devices. Avoiding storing classified information in portable and mobile devices is highly recommended. However, if there is a justified business need, classified information should be wiped remotely when necessary.

Subdomain 3.6 Social Media Cybersecurity

This subdomain aims to ensure the protection of social media accounts used to represent the entity.

Control 3.6.1 Proper measures must be in place to protect social media accounts.

Specific employee(s) should be assigned the responsibility of managing each social media account representing the entity. Accounts must be protected by using secure passwords following the recommended password management best practices and multi-factor authentication (MFA) to designated emails or phone numbers authorized by the entity. Communication of confidential information must be avoided while working on these accounts.

Control 3.6.2 Social media accounts must have verification badges.

Verification badges show people that the accounts are authentic and help in building trust between the entity owning the verified account and other platform users. Hence, the users ensure confidential interaction with the verified accounts.

Control 3.6.3 Email addresses must be provided by the entity to use for social media accounts registration and operational purposes.

The entity must provide the team managing social media accounts with approved email addresses to be used during the entire process of account registration. In addition, the email address must be used for later continuous operating of the social media account. Using emails not provided by the entity is prohibited.

Domain 4 Log Management & Cybersecurity Incident

Subdomain 4.1 Logs Management

This subdomain aims to ensure necessary controls are in place to activate, protect, and maintain the cybersecurity event logs within networks, systems, and applications. In addition, this subdomain ensures that monitoring is conducted to required events within the information processing resources in order to identify any cybersecurity threats or incidents.

Control 4.1.1 Cybersecurity event logs within the information processing resources must be activated.

Activating Cybersecurity event logs within networks, systems and applications is very important. Cybersecurity event logs of the information processing resources record the operation, user access history, communication history, and other essential information. Machine Learning/Artificial Intelligence solutions can help to detect and react to abnormal activities. The application (email, web, intranet, etc..) logs should contain the actual client IP address for each request logged.

Control 4.1.2 Clock synchronization over all networks, systems and applications must be enabled with an accurate time source.

Events must be recorded with time stamps indicating the exact time events have occurred. The timestamps help the entity identify the sequence of events and the relations between events. Without accurately synchronized timestamps, the entity cannot find out which event occurred before the other.

Control 4.1.3 Cybersecurity events must be monitored.

Monitoring cybersecurity events should be applied to help identify whether there are any cybersecurity threats or incidents. The logs of critical systems, remote access controls and privilege accounts should be monitored at least. Log monitoring can happen through a centralized system. One of the solutions that can be used is Security Information and Event Management (SIEM). Additionally, solutions like EDR, Network Detection and Response (NDR), and User and Entity Behavior Analytics (UEBA) can be implemented to work in tandem with SIEM for better detection and response.

Control 4.1.4 Cybersecurity event logs must be protected and maintained for an appropriate period as per the sector regulator and business needs and criticality of the logs.

Event logs must be protected from unauthorized access, modification, or deletion. The logs must be available for any investigation efforts, especially after cyberattacks. The logs must be maintained for an appropriate period as per the business requirements, sector regulations and criticality of the logs.

Subdomain 4.2 Incident Management

The purpose of this subdomain is to ensure that all cybersecurity incidents are being timely identified, detected, and effectively handled and managed to avoid or reduce the impact on the operations of the entity.

Control 4.2.1 A cybersecurity incident response plan must be developed and maintained.

The cybersecurity incident response plan shall provide a clear course of action for the incident response expected from all the employees within the entity. Furthermore, the plan ensures the entity's management commitments and the severity ratings of incidents. The plan should stipulate the formation of a cybersecurity incident management team to be the point of contact for cybersecurity incidents. Clear procedures must be devised and include handling, escalation, and reporting cybersecurity incidents. The incident management process and plan should be defined based on the requirements of NCSC and the sector regulator.

Control 4.2.2 All attainable means must be used to detect cybersecurity incidents.

Cybersecurity incidents must be detected based on data sources. The logs of existing systems can be considered as the source from which data can be extracted, collected, and analyzed to detect cybersecurity threats or incidents. For example, cybersecurity event logs show that an unauthorized user or process has gained access to the information processing resources. The logs may also show some malicious behaviors performed by attackers on the information processing resources. If a cybersecurity incident occurs, the logs provide the necessary information for investigation efforts to identify the causes of the incident and help in mitigating future occurrences.

Control 4.2.3 All employees must report any suspected cybersecurity event or activity.

All employees must be informed about their responsibility to report any suspected cybersecurity event or activity. The employees must be provided with a clear reporting procedure defining the report's contents, including the point of contact and communication method.

Control 4.2.4 Clear procedures must be used to classify cybersecurity incidents.

Not all cybersecurity incidents are similar. The impact and magnitude of incidents are different on the entity. Therefore, the entity must respond differently to cybersecurity incidents. Based on NCSC and/or sector regulator guidelines, the entity must classify cybersecurity incidents to determine the priorities, handling, escalation, and reporting procedures.

Control 4.2.5 The NCSC and the sector regulator must be informed when a medium or high classified cybersecurity incident has occurred and identified or suspected.

The entity should inform the sector regulator and the NCSC about medium or high classified incidents to ensure timely identification, detection, effective management, and handling of cybersecurity incidents.

Control 4.2.6 The impact of cybersecurity incidents must be contained.

To prevent the spread of damage due to a cybersecurity incident, the entity must take the appropriate actions. In some incidents the entity may isolate and remove any infected systems from the network. The entity may need to scan the infected systems for recovery efforts and remove the infection. In some situations, removing the infection is impossible, a backup may be required, or the system may be rebuilt.

Control 4.2.7 evidence associated with cybersecurity incidents must be collected, retained, preserved and protected.

The entity must collect evidence related to cybersecurity incidents. A copy of the evidence must be analyzed to identify the causes and effects of cybersecurity incidents. Furthermore, evidence can help in identifying weaknesses in the information processing resources. Evidence may also be used in the legal system. The entity must protect the evidence from any loss or tampering.

Control 4.2.8 A comprehensive formal cybersecurity incident report must be prepared.

The entity's management must be aware of cybersecurity incidents. The management must receive formal incident reports. Incident reports must contain the following:

- Title of the incident
- Classification of the incident
- Date and time when the incident occurred and detected
- Attack duration
- Information processing resources involved
- Technical details
- Root-cause analysis
- Indicators of Compromise (IOCs)
- Corrective activities performed and planned
- Description of the impact (loss of data, disruption of services, unauthorized modification of data, (un)intended data leakage, number of customers impacted)
- Total estimated cost of the incident
- Estimated cost of corrective actions.

Control 4.2.9 A knowledge base containing cyber incident Response Playbooks and cyber monitoring use-cases must be created.

The information contained in the knowledge base provides a reference for incident analysis. The knowledge base may contain but is not limited to text documents, spreadsheets, and databases. The information within the knowledge base can be used to explain alerts, log entries, and error codes.

Domain 5 Third-Party and Cloud Cybersecurity

Subdomain 5.1 Third-Party Cybersecurity

The purpose of this subdomain is to ensure the protection of systems, applications, and networks (collectively referred to as information processing resources) from risks associated with third parties.

Control 5.1.1 Security requirements must be addressed in the agreement with the third-party.

The third-party may be allowed to access, process, and store the entity's information. Therefore, the security requirements that the third-party must follow have to be clarified. The requirements must be included in the formal agreement between the entity and the third party as well as other documentation such as the request for proposals (RFP). The third party must also sign a non-disclosure agreement (NDA) with the clause of data privacy. The entity must accurately define the scope of the information and information systems that the third party may access. The third-party must not use the information for unrelated purposes and not share, forward, or utilize it without the entity's prior approval. The third-party must use privileged accounts to access systems based on the contractual scope and never use root accounts

Control 5.1.2 Risks related to changes proposed by the third-party must be managed and assessed.

Major changes proposed by the third-party such as new systems, applications or procedures, must be assessed to identify related risks. To manage the changes and treat risks, risk assessments shall be conducted. The risk assessment should also cover matters related to data privacy.

Control 5.1.3 Services and deliverables provided by the third-party must be monitored, audited and reviewed.

The entity must monitor the third-party activities and ensure that all provided services and deliverables comply with all security requirements clarified in the formal agreement.

Subdomain 5.2 Cloud Cybersecurity

The purpose of this subdomain is to ensure that all risks associated with cloud computing and services are **identified, controlled, and mitigated to protect information processing resources.**

Control 5.2.1 Risks of using cloud services must be evaluated.

Moving to the cloud is perceived as a major change for an entity. All risks associated with using cloud services must be identified and reported as part of the risk assessment process. Then, the entity must build all required controls to prevent threats to the information processing resources.

Control 5.2.2 Access to cloud resources must be controlled.

Attackers or unauthorized users must not gain access to any sensitive data or other cloud resources. Authorization and authentication must be applied. Multi-factor authentication (MFA) must be enabled. Access to cloud resources must be with the least privilege. Users should get limited privileges to accomplish tasks. For more information, refer to subdomain 3.2 Access Control.

Control 5.2.3 Data must be encrypted before transferring to cloud storage.

Data must be encrypted to be in an unreadable form in case attackers' attempts to breach the cloud service were successful. For more information, refer to subdomain 3.5 Encryption.

Control 5.2.4 Cloud services must be monitored, and logs must be managed.

Logs must be monitored, processed, and analyzed based on NCSC requirements and guidelines. Logs are helpful in incident investigation. For more information, refer to subdomain 4.1 Monitoring and Logs Management.

Domain 6 Cybersecurity for Operational Technology (OT) and Internet of Things (IoT)

This domain aims to ensure the cybersecurity of Operational Technology (OT) and the Internet of Things (IoT) to protect information processing resources.

Control 6.1 Network segmentation must be implemented to separate the OT or IoT network from other networks.

Implementing network segmentation best practices can create better defense and visibility, enhance access controls, limit lateral movement, improve network performance, protect critical systems and isolate untrusted networks.

When operations personnel who manage OT lack cybersecurity experience or training, cybersecurity function should ensure close coordination to achieve a successful network segmentation. Data diodes systems solution may be used. Some entities are able to have a specialized OT Cyber Security Engineer reporting to the CISO to design, implement and manage cybersecurity controls.

Control 6.2 OT and IoT network must be monitored and the event logs must be activated.

Logs must be collected and analyzed. Log analysis helps for event correlation and cybersecurity incident investigations. Security Information and Event Management (SIEM) solution may be used as a cybersecurity log management. For more information, refer to subdomain 4.1 Monitoring and Logs Management.

Control 6.3 Default passwords must be changed on all OT and IoT devices.

Default passwords are easy to guess, allowing the attackers to access the OT and IoT devices without any difficulties. Accordingly, the entity must change these default passwords to passphrases that are stronger and more secure.

Control 6.4 Security updates and patches for all OT and IoT devices must be tested and implemented.

Attackers can exploit unpatched vulnerabilities. Hence, security updates and patches should be implemented to all OT and IoT devices based on risk assessment. The patches should be prioritized and then tested in the testing environment before being implemented into production. When available, the entity may implement already tested and certified patches by Original Equipment Manufacturers (OEM)s. The entity shall implement

the patches from the highest priority to the lowest priority. The frequency of the patching should be based on a documented risk assessment or approved 'tolerated risks' register.

Control 6.5 Backup for data and configuration must be maintained.

Threats may cause disruption to operations or loss of data. To ensure proactivity about the data's security, backups, including offline backup, should be executed. The entity must maintain a backup copy of both data and configuration for successful backups.

Control 6.6 Unnecessary services, ports, protocols must be disabled.

The entity must perform a network scan to identify running services, open ports, and supported protocols. Some ports may have been opened after installing the software. Unneeded open ports must be shut. The same applies to outdated and unnecessary services and protocols that must be stopped.

Domain 7 Internal and External Audit

This domain aims to maximize the effectiveness of cybersecurity requirements of the entity by conducting internal and external audits to ensure compliance with established policies, operational procedures, and relevant standard, legal, and technical requirements.

Control 7.1 The entity must have an adequate auditing team to carry out the internal audit process.

The auditing team must apply the internal audit process to ensure that the cybersecurity requirements are effectively implemented and maintained.

Control 7.2 The entity must plan for internal audit requirements.

An audit plan must be precise to guarantee a successful internal audit process. The plan includes assigning the responsibility of the internal audit to the audit team members and defining internal audit requirements. The plan must be reviewed at least annually.

Control 7.3 The internal audit process must be conducted at least annually.

The internal audit must be conducted at least annually to ensure compliance of the information processing resources.

Control 7.4 The external audit must be coordinated with NCSC and sector regulators.

The external audit should be performed with the coordination between the NCSC and the sector regulator. The entity has to cooperate with the auditor to fulfill audit requirements that do not involve sensitive or confidential information. If the auditor identifies any non-compliance, an action must be taken based on cybersecurity law, sector regulations and/or entity's internal regulations.

-End of the Document-