Ministry of Interior

National Cybersecurity Center

Financial Cybersecurity Controls

CONSULTATION

Draft v 0.1

October 2022

Introduction

As the financial sector is adopting new technologies in providing banking, insurance, money exchange, point of sales, crypto currency, and stock exchanges services to users remotely, the associated cyber security risk increased significantly. For the aim of protecting the financial sector which is one of the Critical National Infrastructure (CNI) from any cybersecurity threats and attack, the financial cybersecurity controls document is developed by NCSC to guide the financial entities to have a robust cybersecurity by following the controls mentioned in the document. All financial entities must follow the cybersecurity controls in this document.

This document will address the best practices to be implemented in seven domains which are Governance, Cybersecurity of Financial Technology, Cyber Defense, Cybersecurity Assessment, Cybersecurity of Third-Party, Cybersecurity Incident Management and Cybersecurity Audit.

CONSULTATION

Domain 1 Cybersecurity Governance

This domain aims to ensure that the entity is fully aware of cybersecurity goals and that all actions taken are in the correct direction towards the achievement of cybersecurity goals. The domain covers seven subdomains, which are Roles and Responsibilities, Cybersecurity Risk Management, Strategies, Policies and Procedures, Asset Management, Change Management, Cybersecurity Continuity Management, Cybersecurity Awareness and Training.

Subdomain 1.1 Roles and Responsibilities

This subdomain establishes the cybersecurity implementation by defining cybersecurity roles and responsibilities including the responsibilities of the board of directors and senior management and relevant stakeholders for the successful planning, implementation, and operation related to cybersecurity. Defining roles and responsibilities strengthens the entity's accountability.

Control 1.1.1 The Board of Directors is responsible for cybersecurity including ensuring sufficient budget endorsing the cybersecurity strategy and policy.

Control 1.1.2 The financial entity must identify the responsible employees for cybersecurity activities.

Control 1.1.3 A cybersecurity committee must be established to be responsible for:

- Monitoring, reviewing, and communicating the cybersecurity risk appetite periodically or when there is a major change in the risk appetite.
- Reviewing the cybersecurity strategy to ensure that it supports the financial entity's objectives.
- Approving, supporting, and monitoring cybersecurity strategy, cybersecurity policy, cybersecurity risk management process, the key risk indicators (KRIs), and key performance indicators (KPIs) for cybersecurity.
- Incident detection and response.

Control 1.1.4 The project management methodology must ensure that cybersecurity objectives are included in all projects, cybersecurity is involved in all phases of any project, and a risk assessment is performed before any project.

Control 1.1.5 Each employee must be informed of the assigned cybersecurity responsibilities.

CONSULTATION

Subdomain 1.2 Cybersecurity Risk Management

Cybersecurity 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 reduce the cybersecurity risks for the information assets, the risks' impact, likelihood, and vulnerability must be accurately identified, assessed, and analyzed. A comprehensive cybersecurity risk management plan must be developed.

Control 1.2.1 The requirements of risk management must be implemented by a committee, or any team specified by the Board of directors, based on international frameworks approved by NCSC.

Control 1.2.2 The financial entity must develop a comprehensive plan that clarifies the scope and boundaries of the cybersecurity risk management process determining the business areas, people covered in the plan and allocated recourses with consideration of risk appetite.

Control 1.2.3 The plan must identify the details of the cybersecurity risk management process including risk identification, risk analysis, risk treatment, and risk monitoring along with roles and responsibilities, organizational structure, and charters.

Control 1.2.4 The senior management must approve the plan before implementation and review the plan periodically and after a major change is made to the plan.

Control 1.2.5 The senior management must ensure implementation and effectiveness of the risk management process which includes the board of directors' review and approval of the cybersecurity risk assessment results.

Control 1.2.6 The identified risks must be communicated to relevant risk owners for their endorsement.

Control 1.2.7 The financial entity must determine appropriate cybersecurity risk treatment and mitigation plans with the tools to be used to reduce and minimize the risk likelihood and/or impact.

Control 1.2.8 The financial entity shall maintain the risk register that records risk rating, prioritize risks for treatment and identifies risks that are within the entity's risk tolerance and reviewed periodically.

Control 1.2.9 The financial entity must monitor and communicate cybersecurity risks as well as review the risk register periodically.

CONSULTATION

Subdomain 1.3 Strategies, Policies, and Procedures

This subdomain aims to ensure that all cybersecurity strategies, policies, and procedures are well organized, governed, and documented. The strategies include addressing clearly the cybersecurity goals the financial entity is willing to achieve. The policies and procedures must be defined, approved, executed, and reviewed at least once every three years to ensure achieving the financial entity's objectives.

Control 1.3.1 The cybersecurity strategy should contain: the importance and benefits of cybersecurity to the financial entity; the cybersecurity objectives to be achieved; the difficulties that may occur; the cybersecurity initiatives and projects to achieve the cybersecurity objectives.

Control 1.3.2 Cybersecurity policy and procedures must be defined, approved, communicated, and reviewed periodically.

Control 1.3.3 The board of Directors must review the cybersecurity strategy and policy periodically.

Subdomain 1.4 Asset Management

One of the core subdomains of cybersecurity governance is asset management. Identifying and maintaining the information assets is important to protect the entity's information infrastructure. Information assets include hardware, software, information systems, information services, virtualization, and information stored on-prem or in the cloud.

Control 1.4.1 The financial entity must define, approve, and implement an asset management process. The process must be monitored and measured on a regular basis.

Control 1.4.2 Automated asset discovery tools are highly recommended to be used to identify assets when they are introduced, and validated at least every two months.

Control 1.4.3 Assets must be identified, classified, prioritized, and maintained in a centralized asset inventory.

Control 1.4.4 All information stored on-premises or in the cloud must be classified based on best international practices and the classification must be reviewed at least annually.

Control 1.4.5 Asset inventory must be reviewed and updated at least annually or when major changes happen.

Control 1.4.6 All assets must be labeled with a unique identifier physically or tagged electronically in accordance with their asset classification. Therefore, all users are aware of the ownership and classification of the information.

CONSULTATION

Control 1.4.7 Asset details must be recorded such as, but not limited to, asset identifier, asset name or description, asset function, asset classification, asset owner, asset custodian, asset users, physical asset location, license details, and asset severity.

Control 1.4.8 Assets maintenance details must be recorded.

Control 1.4.9 Asset owners, custodians, and users must protect the finance entity's assets.

Control 1.4.10 The re-classification of assets must be done either in terms of degrading or upgrading the classification.

Control 1.4.11 Since reclassification involves a change in access control, appropriate precautions/security controls must be considered against information disclosure.

Control 1.4.12 All assets must be sufficiently protected against loss, theft, unauthorized access, and/or unauthorized disclosure in line with the classification level.

Control 1.4.13 Appropriate controls must be in place to ensure the security of the information asset during its transmission over different channels. The level of controls must be in line with the classification of assets being transmitted.

Control 1.4.14 The recipient of the information must treat it in accordance with the information classification established by its originator.

Control 1.4.15 To minimize the risk of confidential information leakage to unauthorized persons, formal procedures for the secure disposal of information and assets must be established, including the proper steps for asset disposal.

Control 1.4.16 The entity must ensure compliance with the secure disposal formal procedures.

Control 1.4.17 The financial entity must ensure that breached assets are fully recovered and safe to use.

Subdomain 1.5 Change Management

This subdomain is aimed to ensure the change management process is a structured procedure in which the finance entity is well-prepared, organized, and can implement changes with minimum number of difficulties.

Control 1.5.1 A change management process must be established to ensure that changes to information assets are assessed, tested, reviewed, and approved before implementation. The compliance with change management process must be monitored.

Control 1.5.2 The change management process should set the cybersecurity requirements related to controlling changes of information assets including cloud computing assets, which include the impact, classification, and review of changes.

CONSULTATION

Control 1.5.3 A risk and impact analysis of the change to an information asset must be conducted before implementation to analyze the implications of the change.

Control 1.5.4 All changes must be tested in a testing environment based on test plans approved by business and IT management. Test results must be accepted and signed off before the changes are deployed to a production environment.

Control 1.5.5 Before implementing the change, a backup (including offline backup) must be performed, and a rollback plan must be developed.

Control 1.5.6 Procedures must be defined for assessing, approving, and implementing urgent or emergency changes that need to be implemented without following the standard change management process.

Subdomain 1.6 Cybersecurity Continuity Management

Business Continuity Management (BCM) is an act of anticipating and minimizing impacts that might affect mission-critical operations, services, functions, and processes of the financial entity and ensuring their availability to enhance overall business resilience. BCM also includes efforts to recover the information assets.

Control 1.6.1 A comprehensive plan must be established and built to describe the whole BCM process including the resources needed and the scope of work. The plan must be approved by the Board of Directors.

Control 1.6.2 The plan must include all steps involved in response to disasters to protect the information assets and restore critical business functions and services.

Control 1.6.3 A business impact analysis must be performed that covers the estimated losses to prioritize the protection and ensure the availability of services.

Control 1.6.4 The results of business impact analysis must be reviewed regularly or when there is an effective change.

Control 1.6.5 The finance entity must ensure that the required resources to deliver essential services and business functions are adequate to maintain availability in a disaster.

Control 1.6.6 A disaster recovery (DR) plan must be developed which determines the frequency of data backup including offline backup, the acceptable recovery time, the responsible employees to

CONSULTATION

handle the recovery process steps, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Control 1.6.7 DR plan must include alternative out-of-band communication methods and details of their use in case of unavailability of the original method.

Control 1.6.8 The plans for business continuity and disaster recovery must be reviewed at least annually or after a major change to identify any weaknesses or gaps.

Control 1.6.9 A test plan must be developed to test the plans of business continuity and disaster recovery. The plan should include the test scope and objectives, test scenarios and the details related to the test activities performed.

Control 1.6.10 Testing the plans must involve all teams and not be limited to cybersecurity or IT staff. The testing must include as many aspects of disaster recovery, including restoring from offline backups and the use of out-of-band communication.

Control 1.6.11 Physical copies of the plans must be available at the main site and at the DR site to be reached when a cyber-attack prevents access to electronic copies.

Subdomain 1.7 Cybersecurity Awareness and Training

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. This subdomain ensures that all employees are equipped with sufficient knowledge and skillsets that contribute towards efforts in protecting information assets and limiting human error that may result in security risks and insider threats. The training and awareness program shall be built to promote a cybersecurity culture amongst all employees.

Control 1.7.1 The cybersecurity awareness program must be defined, approved, conducted, and reviewed periodically to promote cybersecurity awareness among employees, third parties and customers of the financial entity.

Control 1.7.2 An assessment should be completed for all employees who will be able to access IT systems, including new employees, to identify the level of their cybersecurity knowledge and skills.

Control 1.7.3 Based on the assessment, topics for cybersecurity training and awareness content must be identified, taking into consideration the employees' job levels and roles.

Control 1.7.4 The cybersecurity training program must be developed and conducted based on the identified topics. Some of the training can be provided as part of the orientation program.

CONSULTATION

Control 1.7.5 Employees of the financial entity must be trained to acquire the skills and knowledge required to securely operate and protect information assets and systems.

Control 1.7.6 The cybersecurity training and awareness program must be annually evaluated and reviewed to check whether it successfully improved the employees' knowledge and skills.

Control 1.7.7 The cybersecurity training and awareness program must address newly discovered cybersecurity threats.

Domain 2 Cybersecurity of Financial Technology

The involvement of technologies in the financial sector has many advantages, but a large number of cybersecurity threats may arise. This domain targets financial systems and is intended to provide the required cybersecurity measures to be considered when acquisition, developing and managing financial systems.

Subdomain 2.1 Cybersecurity of Critical Financial Systems

This subdomain aims to protect critical financial systems that provide financial services and transactions of funds such as payment systems and Automated Teller Machines (ATMs).

Control 2.1.1 Customer data must be protected by securing communications channels using strong cryptographic technologies.

Control 2.1.2 Transaction-signing must be implemented for authorizing high-risk activities such as but not limited to changes to sensitive customer data (e.g., address, email, and phone), high value funds transfers, and revision of funds transfer limits.

Control 2.1.3 Access to services that the financial system provides must require strong authentication techniques.

Control 2.1.4 The biometrics-related data (e.g., face, iris or palm images, voice patterns, etc.) and authentication credentials must be strongly encrypted at rest and in transit and be stored in a form that prevents reverse engineering.

Control 2.1.5 When implementing time-based One-Time Passwords (OTPs), the validity period must be as short as practicable to lower the risk of using stolen OTPs.

Control 2.1.6 Mobile applications provided by the financial entity to customers must be through official mobile application stores or other secure delivery channels.

CONSULTATION

Control 2.1.7 The financial entity must raise the awareness of protection against phishing and alert customers of any phishing campaigns targeting the financial entity.

Control 2.1.8 Real-time fraud monitoring systems must be implemented to identify and block suspicious or fraudulent online transactions.

Subdomain 2.2 Financial System Acquisition, Development, and Management

The objective of this subdomain is to ensure that the security requirements are considered during the acquisition, development, and management of financial systems.

Control 2.2.1 The entity must evaluate the purchase of any financial systems by documenting the information security requirements and must keep in consideration the relevant standards, wherever available and applicable.

Control 2.2.2 The financial entity must develop a procedure for vendor evaluation and selection to ensure the vendor is qualified and able to meet security requirements.

Control 2.2.3 The financial entity must test newly enhanced or purchased systems before integrating into the entity.

Control 2.2.4 The financial entity should properly plan the installation of new software/applications to minimize disruption and to ensure that the information security issues are adequately covered.

Control 2.2.5 The financial entity should ensure that acquisition and approval of system/application software is centralized.

Control 2.2.6 The license of the software, activation keys, and serial numbers should be obtained from the vendor and retained in a durable and retrievable form by the IT directorate.

Control 2.2.7 All errors, faults, security incidents, and problems with application software must be logged via the IT service desk / IT department and reported to the respective team for handling and closure.

Control 2.2.8 The support maintenance contract with the vendor should contain a non-disclosure agreement (NDA). The support maintenance contract should clearly state that no data should be moved or stored outside the finance entity except logs during investigations and with proper approval from senior management.

Control 2.2.9 The financial entity must ensure that the vendor does troubleshooting/maintenance under the supervision of authorized persons from the entity.

CONSULTATION

Control 2.2.10 The entity must consider the upgrades and patches procedures to resolve software bugs. The patches can only be applied, with the following precautions.

- Verify that the patches are necessary and come from an authorized source, normally the software developers.
- Patched versions of the software should always be tested before release for live use.
- A rollback/fallback plan shall be developed before the implementation of production systems in the event of an unsuccessful deployment.
- Apply patches only with proper authorization and system documentation.
- All patches shall be tested in the test environment before deploying in production and tests are logged and approved.

Control 2.2.11 A framework must be established to manage system development life cycle (SDLC). The framework must define the processes, procedures, and controls in each phase of the life cycle.

Control 2.2.12 The financial entity must ensure the segregation of duties during the system development life cycle.

Control 2.2.13 Developers must be trained to have the required knowledge and skills to apply secure coding and other security standards for software development.

Control 2.2.14 Procedures must be developed to ensure the review and testing for third party and open-source software.

Control 2.2.15 Software bugs or vulnerabilities must be mitigated as much as possible by adopting standards on secure coding, source code review and application security testing.

Control 2.2.16 The secure coding and source code review standards must cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling.

Control 2.2.17 For third party and open-source software, updates and reported vulnerabilities must be tracked.

Control 2.2.18 All discovered issues in the software must be tracked. Major issues must be remediated before production deployment.

Control 2.2.19 A configuration management process must be implemented to maintain accurate information of the hardware and software.

CONSULTATION

Control 2.2.20 Configuration information about hardware and software must be reviewed and verified on a regular basis to ensure it is accurate and up to date.

Domain 3 Cyber Defense

The scope of this domain is to address the effective cybersecurity defense processes to ensure their effectiveness in protecting networks, systems, applications, and IT services of the entity. The domain defines and describes many processes in six subdomains: Identity and Access Management, Cybersecurity of Communication, Email Protection, Cryptography, Physical and Environmental Security and Social Media Cybersecurity.

Subdomain 3.1 Identity and Access Management

This subdomain is describing how to prohibit or minimize unauthorized users, systems, and processes from gaining access to information assets.

Control 3.1.1 Identity and Access Management (IAM) cybersecurity requirements including user registration and revoking procedures must be defined, documented, approved, and implemented.

Control 3.1.2 The implementation of the IAM cybersecurity requirements must be reviewed periodically.

Control 3.1.3 Default operating system accounts must be disabled, renamed, and have their passphrase changed where possible.

Control 3.1.4 Device access control tools must be used to prevent the connection of unauthorized devices to workstations and servers through external interfaces.

Control 3.1.5 Root account access must only be granted as part of an special task as defined in existing policy and following senior management approval.

Control 3.1.6 Root accounts can be only used due to change management or any emergency occurrence such as disaster recovery, incident handling plan, and business continuity plan.

Control 3.1.7 Access to the financial entity's networks, systems, and applications by unknown users, systems, or processes must be monitored and restricted.

Control 3.1.8 The financial entity should develop a policy and process for accessing the local administrator account.

CONSULTATION

Control 3.1.9 Access to server consoles and operating systems must be limited to respective administrator personnel only. All administrator accounts shall comply with the access control requirements.

Control 3.1.10 The built-in administrator account is the original administrative account of the server and/or domain. Only selected system administrator personnel are to know this account's credentials. Where possible, use a split password process for the administrator account and assign the rights to specific personnel.

Control 3.1.11 Administrators are not permitted to share their account information with anyone.

Control 3.1.12 Access to networks, systems, and applications by systems and employees including teleworkers must be:

- Requested, reviewed, approved, implemented, and verified in accordance with business needs and cybersecurity requirements including the access control policy.
- Reviewed by the owners or administrators of networks, systems, and applications and access must only be granted after having appropriate approval.
- Maintained to help the financial entity in identifying and recording all access rights granted to the networks, systems, and applications.

Control 3.1.13 The access to networks, systems, and applications must be restricted and granted based on identity and access control principles including:

- Need-to-Know Principle: granting access to users whose job duties, roles, and responsibilities involve the need to access and use data or information in accordance with the "Need-to-Know" principle. Otherwise, the request must be rejected, and access must not be granted.
- Least Privilege Principle: assigning a user, system, or process with the least privileges needed to do the necessary activities/actions based on the user's role and duties.
- Segregation of Duties Principle: The entity must consider the conflicting roles (e.g., Requestor and approver roles or checker and maker roles) and shall segregate them to ensure that no individual has access to control all phases of an operation/process.

Control 3.1.14 Administrative access shall be granted to respective personnel after having proper business justification and a need-to-know basis.

CONSULTATION

Control 3.1.15 The financial entity must ensure a separate account is created per user of networks, systems, and applications by assigning a unique identifier (User ID) linked to the user account. Any action performed should then be attributable to that single user.

Control 3.1.16 The financial entity must maintain the approved unique user's ID using an appropriate solution.

Control 3.1.17 The financial entity must prohibit sharing the same accounts across multiple users. Employees must not use other user accounts to gain access to the entity's networks, systems, and applications.

Control 3.1.18 The financial entity must consider Privileged Access Management (PAM) solution to manage privileged access to information systems.

Control 3.1.19 The usage of privileged accounts must be limited to specific employees and privileged account activities must be logged and monitored regularly.

Control 3.1.20 Users must not use privileged accounts as personal accounts for daily tasks such as reading emails and web browsing.

Control 3.1.21 Privileges and access rights of user accounts must be reviewed and re-evaluated periodically and in response to a change in a user's duties, position, or department. Access rights of users must be revoked while there is job relocation, termination, or separation from the entity.

Control 3.1.22 Authentication, Authorization, and Accountability (AAA) must be performed when granting users, systems, or processes access to financial entity's networks, systems, and applications. The necessary measures for AAA must be implemented.

- Authentication must be applied by requesting and verifying the user's credentials before accessing the networks, systems, and applications to ensure the claimed identity is the correct identity.
- The authorization process must be performed to determine whether a verified user, system, or process has permission to access networks, systems, and applications or perform certain actions. The access must not be granted until the completion of an authorization process.
- Accountability must be applied to ensure that a user, system, or process is held responsible by observing and tracing back actions and events that occurred.

CONSULTATION

Control 3.1.23 Multi-Factor Authentication (MFA) must be used for all types of access in financial systems, and unique passwords must be utilized for such critical systems.

Control 3.1.24 MFA must be implemented to add a layer of security by making access to networks, systems, and applications harder for attackers. In which, compromising one of the factors requires the compromise of other factors to breach an account.

Control 3.1.25 MFA 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).

Control 3.1.26 Multi-factor authentication must be deployed at login for online financial services and mobile applications.

Control 3.1.27 The default password/passphrase of financial systems and devices must be changed.

Control 3.1.28 Passwords/passphrases that are set or reset on users' behalf must be randomly generated and must be changed after first access by the user.

Control 3.1.29 After resetting user's account password/passphrase:

- Users must provide sufficient evidence to verify their identity.
- Providing passwords/passphrases to users must be through a secure communications channel.

Control 3.1.30 All passwords/passphrases stored in financial system databases must be encrypted.

Control 3.1.31 Passwords/passphrases must be changed in these cases:

- Passwords/passphrases are directly compromised or suspected of being compromised.
- Passwords/passphrases are found in databases of an online stored data breach.
- Passwords/passphrases appear to be stored in the clear on a network or transferred in the clear across a network.
- The retention period has passed without changing the password/passphrase.

Control 3.1.32 The financial entity must enable a rule to limit the number of failed logins permitted on a user account before it is locked, and if a user is frequently locked out due to failed login attempts then passwords/passphrases will be reset after investigation.

CONSULTATION

Control 3.1.33 Authentication methods using legacy protocols must be disabled whenever it is possible, to prevent cyberattacks from exploiting vulnerabilities in legacy authentication protocols and methods.

Control 3.1.34 Warning banners should appear prior to system login which specify requirements for accessing the system and penalties for improper use

Control 3.1.35 All non-essential users, groups, and service accounts must be removed where possible.

Control 3.1.36 User accounts must be permanently disabled upon retirement/termination of an employee after receipt of the user clearance form.

Control 3.1.37 Service accounts used by services must only be used for the purpose of accessing system resources. Only system administrator personnel are permitted to know service account credentials.

Control 3.1.38 If server access is required for security audit purposes, access should be granted to required areas only.

Control 3.1.39 For security and maintenance purposes, only authorized personnel may monitor equipment, systems, servers, and network traffic.

Control 3.1.40 Using Bring Your Own Device (BYOD) to access a financial entity's network, information, or services must be approved by top management after considering securing devices and connections in addition to limiting what users can access.

Control 3.1.41 Teleworking must be conducted based on best cybersecurity practices.

Subdomain 3.2 Cybersecurity of Communication

The objective of cybersecurity in the communication subdomain is to assure network protection against all threats and risks. The cybersecurity controls of this subdomain can be implemented at either gateway or perimeter level.

Control 3.2.1 Network security requirements must be considered from the planning and design stage of the network architecture.

Control 3.2.2 Network architecture high-level diagram (HLD), Low-level diagram (LLD) must be documented and approved by the senior management.

CONSULTATION

Control 3.2.3 Required level of flexibility must be considered, keeping in view the future expansion of business (due to growth) and bandwidth requirements for the desired response time, at the time of designing the network.

Control 3.2.4 Network diagrams and configuration records must be secured and access should be restricted.

Control 3.2.5 Any network architecture change must be reflected in the diagrams and configuration records and must adhere to a well-planned change management process.

Control 3.2.6 Only necessary traffic is allowed in the financial entity's network, other traffic must be blocked.

Control 3.2.7 Systems that are classified as sensitive and critical or identified as vulnerable during the risk assessment must be run in an isolated network with proper access controls and restrictions.

Control 3.2.8 Information like system names, network topology, network device types, and internal user ID's must be not reachable by unauthorized users.

Control 3.2.9 All outbound traffic from the financial entity to other networks and vice-versa must pass through a parameter security device based on NCSC's recommendations such as a firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), etc.

Control 3.2.10 All incoming and outgoing network traffic must be subject to malware scanning at the gateway.

Control 3.2.11 The financial entity's networks must be segmented and segregated logically or physically based on information classification and risk assessment.

Control 3.2.12 Screening all the web requests from the internal network for inappropriate content or/and malicious code using a content filtering solution.

Control 3.2.13 The financial entity's security devices should consider the access control requirements.

Control 3.2.14 Configuration of security devices must meet business needs and be reviewed regularly to avoid misconfiguration.

Control 3.2.15 Network devices and their configuration must be compatible with cybersecurity requirements.

Control 3.2.16 Routers and switches must be configured in such a way that the risks of compromise of these vital networking components are reduced. This includes disabling unnecessary services.

CONSULTATION

Control 3.2.17 Redundant provisions must be made for critical network components to ensure the continuous availability of the network.

Control 3.2.18 Only authorized administrators are allowed to configure network devices.

Control 3.2.19 The financial entity must identify and shut down unused network ports.

Control 3.2.20 Unauthorized devices connecting to the financial entity's network must be restricted.

Control 3.2.21 The financial entity's network must be scanned regularly to monitor and identify network changes.

Control 3.2.22 Any change in the configuration of network security devices must follow a proper change management process.

Control 3.2.23 The configurations of network security devices and information systems used by the financial entity must be backed-up regularly.

Control 3.2.24 IP telephony infrastructure (video conferencing units, handsets, software, and servers) must be hardened. Authentication and authorization must be used for all actions on IP telephony networks such as registering a new IP phone and accessing voicemail.

Control 3.2.25 The firewall must be configured and monitored in order to maintain a secure network based on best practices such as backing up the configuration and examining firewall logs.

Control 3.2.26 Firewall security policies must be reviewed every three months or whenever major changes are incorporated in the network or firewall configuration. Firewall rules should be audited for vulnerabilities, conflicts, or for those which are no longer in use.

Control 3.2.27 A Web Application Firewall (WAF) must be used to filter HTTP(S) traffic.

Control 3.2.28 The network security systems and solutions must be upgraded with the necessary modules to assure optimal firewall performance. The firewall administrator must be aware of any hardware and software bugs, as well as firewall software upgrades that are issued by the vendor.

Control 3.2.29 The financial entity must ensure that the person configuring the security systems and solutions is different from the approver.

Control 3.2.30 All Internet activities must be controlled and pass through the financial entity's security gateway devices.

CONSULTATION

Control 3.2.31 If internet access for customers or visitors will be provided, the financial entity must ensure network segregation and restrict the entity's network systems and devices' network visibility, or reachability and a registration solution must be deployed.

Control 3.2.32 The financial entity visitors' internet access must be reviewed every year and restricted if internet access is no longer required.

Control 3.2.33 Any remote access to the financial entity's network must use secure connections such as a Virtual Private Network (VPN).

Control 3.2.34 Devices accessing the wireless network must be restricted, and visitors' or guests' wireless access points must be isolated from the financial entity's network.

Control 3.2.35 The highest and most effective encryption standard must be applied to protect the wireless network.

Control 3.2.36 All usage of the Internet, network, VPN, and wireless by users or systems must be logged and monitored.

Subdomain 3.3 Email Protection

This subdomain ensures that proper controls are in place to minimize the risks associated with email services, servers, and applications.

Control 3.3.1 Email accounts belonging to the financial entity's domain must be assigned only to entity's employees.

Control 3.3.2 A Secure Email Gateway (SEG) must be used to protect the financial entity from email attacks.

Control 3.3.3 All emails must be automatically scanned for viruses and spam. The findings and infections must be blocked or quarantined depending on the severity level. The email server administrator has the right to reject any recovery of Infected/Quarantined emails that might compromise the system or network. Suspicious emails and URLs must be blacklisted.

Control 3.3.4 All files including compressed files sent as attachments in the incoming and outgoing mail (SMTP traffic) must be scanned, any detected malware must be cleaned automatically, and the infected file must be deleted otherwise the folder must be quarantined.

Control 3.3.5 Email messages must be protected using email filtering solutions and authenticated by enforcing Domain-based Message Authentication, Reporting, and Conformance (DMARC),

CONSULTATION

Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) on inbound and outbound emails.

Control 3.3.6 Unnecessary and unauthorized browser or email client plugins should be limited and controlled to decrease the chances of any risk generated from these plugins. A log of all information related to approved plugins used must be maintained, protected, and reviewed.

Control 3.3.7 Third-party emailing platforms must not be used for sending official emails.

Control 3.3.8 Emails must be archived and backed-up as per the email backup policy and based on the severity of the emails.

Subdomain 3.4 Cryptography

This subdomain aims to guarantee that encryption is used correctly and efficiently to safeguard networks, systems, and applications. Encryption in a cloud environment will be covered in domain 5. Cybersecurity of Cloud Environment.

Control 3.4.1 Information and data on all levels must be encrypted in transit and at rest based on information classification and best practices, which includes:

- Data stored on end-user devices including BYOD
- Data stored on removable media
- Data in transit including communications through online transactions
- Data transmitted across third-party network
- Sensitive/critical or confidential data transported in computer-readable storage media
- Sensitive/critical or confidential data delivered through any network communication over wired or wireless network

Control 3.4.2 The strength of the encryption technique to be employed must be determined based on data classification. The more Sensitive/critical or confidential the data, the stronger encryption technique is to be employed.

Control 3.4.3 All encryption operations for key management (key generation, storage, etc.) should take place in a secure environment.

Control 3.4.4 Encryption keys must be managed and protected during their lifecycles.

Control 3.4.5 Encryption keys must be generated by the latest means (algorithms and standards), which will yield keys that are difficult to compromise.

CONSULTATION

Control 3.4.6 Encryption keys are the most Sensitive/critical or confidential type of information, and access to such keys must be strictly limited to authorized personnel only.

Control 3.4.7 Unless the exception of the senior management is obtained based on risk assessment, encryption keys must not be revealed to any third parties.

Control 3.4.8 It is highly recommended that no single person has full access to any single encryption key, which can be achieved by separation of duties in such a way that two people must be present for an important activity or by "key splitting".

Control 3.4.9 When the number of keys is high, it is recommended to use Key Management System (KMS).

Control 3.4.10 All keys must be maintained by the head of cybersecurity for emergency cases.

Control 3.4.11 While storing encrypted data, the encryption keys and other encryption material are used to encrypt:

- Must not be stored on the same media as the encrypted data
- Must be stored in an encrypted form including the master keys
- Master Key must be handled with dual responsibility with split knowledge
- Master Keys must be stored in tamper-proof modules such as Hardware Security Module (HSM)
- Master Keys must not be transmitted over the network

Control 3.4.12 Encryption keys must be discarded while the key's life is expired or found to be compromised by using the key management lifecycle.

Subdomain 3.5 Physical and Environmental Security

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

Control 3.5.1 Infrastructure and security devices such as firewalls, servers, routers, and switches must be physically located in access-controlled and environmentally protected facilities to prevent unauthorized physical access, damage, and interference.

Control 3.5.2 Measures must be implemented to protect all information assets based on their classification and location.

Control 3.5.3 Information assets must be monitored remotely and regularly including using CCTV cameras to monitor the access to critical financial system such as ATMs.

CONSULTATION

Control 3.5.4 The financial entity must ensure that ATMs have adequate measures to avoid skimming attacks based on the best practices and standards.

Control 3.5.5 Access to facilities such as data center/server rooms or areas where sensitive information is kept must be restricted using an access control system with multi-factor authentication to prevent any unauthorized physical access.

Control 3.5.6 Facilities must provide power supplies from multiple sources like Uninterruptible Power Supplies (UPS), and power generators, etc.

Control 3.5.7 The records of the entrance and exit management systems must be protected. The keys to doors, cabinets, and containers in the data center must be kept safe.

Control 3.5.8 Power going to computer systems should be through UPS. It should be ensured that the UPS is always in working condition.

Control 3.5.9 Financial information systems and devices must be physically secure from environmental threats. Adequate measures and procedures must be implemented to address and respond to environmental threats including fire, floods, earthquakes, and others.

Control 3.5.10 The financial entity must control and monitor water leakage, humidity, and temperature levels in the equipment locations.

Control 3.5.11 The financial entity must install fire detection and suppression systems.

Control 3.5.12 Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications.

Control 3.5.13 Data center financial checklists must be logged, reviewed, and maintained daily.

Control 3.5.14 No equipment/media shall be taken off-premises without prior authorization that must be recorded in an easily retrievable location such as the asset register.

Control 3.5.15 Routers must be placed in a room, free of electrostatic or magnetic interference and must have controls for temperature and humidity.

Control 3.5.16 Visitors are not allowed to access authorized facilities without proper approval and all visits must be recorded in a register and the record retained for a period specified in a data retention policy.

Subdomain 3.6 Social Media Cybersecurity

Social media applications can create several cybersecurity risks to entities when used in an inappropriate or unsafe manner. Due to their popularity, social media applications are a common way for an adversary to gather information on entities and their employees. When sensitive information is posted to social media, it has the

CONSULTATION

potential to harm the public and the entities' interests. Therefore, financial entities are required to follow the controls in this subdomain to protect their social media accounts.

Control 3.6.1 Employees must be trained in the secure use of the financial entity's social media accounts.

Control 3.6.2 Only authorized employees have access to the financial entity's social media accounts.

Control 3.6.3 Social media accounts must not be configured to automatically sign in.

Control 3.6.4 The financial entity's social media accounts must not be accessed on untrusted devices.

Control 3.6.5 Employees managing the financial entity's social media accounts must not share access credentials with anyone.

Control 3.6.6 MFA must be implemented for access to the financial entity's social media accounts with a complex password/passphrase.

Control 3.6.7 Employees managing social media accounts must use their official work email address to log in to the social media accounts.

Control 3.6.8 If asked to set up security questions to recover social media accounts, the employee must not provide answers that could be easily obtained from public sources of information. The answers to the security questions must be securely recorded with the account credentials.

Control 3.6.9 Employees managing social media accounts must not post sensitive information.

Control 3.6.10 Access to social media accounts must be revoked immediately when there is no longer a requirement for access.

Control 3.6.11 Social media account credentials must be reset upon personal re-positioning, transfer, or termination.

Control 3.6.12 All employees must not share confidential entity's information over social media and be aware of the harms of sharing such information.

Control 3.6.13 The financial entity should use social media control tools and techniques to control content over social media like brand protection services.

Control 3.6.14 Procedure must be created for managing the social media accounts. The procedure should include managing multi-users for a single account and specifying the roles for writing and approving the posts.

CONSULTATION

Domain 4 Cybersecurity Assessment

Cybersecurity Assessment is a process that enables the discovery of cybersecurity weaknesses in a system. It is very crucial as the attackers usually exploit a weakness in a system to perform an attack and breach the entity's system. This domain aims to guide the financial entities in performing vulnerability assessment and penetration testing.

Subdomain 4.1 Vulnerability Management

Vulnerability is a weakness or flaw in hardware or software like a system or device's design, including code, architecture, implementation, flow, etc. Threat actors exploit vulnerabilities to gain unauthorized access to networks, systems, and applications and conduct malicious activities. This domain includes the proper controls to reduce the number of undetected flaws or ignored vulnerabilities within systems, applications, and networks.

Control 4.1.1 Vulnerability assessments (VAs) must be conducted for financial technologies at least once a month.

Control 4.1.2 The financial entity must use automated tools such as a vulnerability management solution.

Control 4.1.3 VAs must be conducted before deploying a new system to the network or any major infrastructure changes.

Control 4.1.4 Detected vulnerabilities must be addressed, and corrective action must be performed based on vulnerability classifications and priorities.

Control 4.1.5 The financial entity must identify, prioritize, and treat weaknesses in networks, systems, and applications in accordance with the remediation plan.

Control 4.1.6 A patch management process and supporting patch management procedures must be developed and implemented.

Control 4.1.7 A software register, including versions and patch histories of financial devices applications, drivers, operating systems, and firmware for workstations, servers, mobile devices, and network devices must be maintained and regularly audited.

Control 4.1.8 When support for a device, application, or operating system has been ended by the vendor or manufacturer, the financial entity must update or replace them with supported versions.

CONSULTATION

Subdomain 4.2 Penetration Testing

This subdomain aims to ensure cybersecurity controls are in place to address the Penetration Testing (PT) of the financial entity's systems, applications, and network devices to check the robustness of their implemented cybersecurity controls.

Control 4.2.1 The PT must be conducted at least twice a year, and once there is an upgrade in the infrastructure or software in use either manually or automatically.

Control 4.2.2 At least one of the two PTs a year must be performed by an independent third party and that third party must change at least every two years.

Control 4.2.3 The financial entity must ensure that the penetration testers are qualified, experienced, and certified by a reputable certification body for providing PT services.

Control 4.2.4 The PT scope must be defined and approved by the senior management. The scope involves but is not limited to systems, locations, techniques, and tools used in the test and verified vendor.

Control 4.2.5 The PT must be performed on either the production environment or an exact replica of the production environment.

Control 4.2.6 The financial entity should conduct external and internal PTs.

Control 4.2.7 The financial entity must identify, prioritize, and treat weaknesses that are identified during PT in information processing resources.

CONSULTATION

Domain 5 Cybersecurity of Third-Parties

Dealing with a third-party brings many threats and risks to the entity especially when third-party is allowed to access the networks, applications, and systems of the entity. To protect the entity from third-party misconduct, this domain lists cybersecurity controls starting from selecting a third party until the termination of the third-party contract. This domain includes two subdomains, which are Third-Party Management and Cloud Computing.

Subdomain 5.1 Third Party Management

The objective of this subdomain is to establish controls to ensure that access by a third party is appropriate and will not allow them to carry out any unauthorized activity and follow and abide by the requirements set forth by the financial entity. Security requirements must be addressed in the agreement with the third party.

Control 5.1.1 The financial entity must conduct a detailed feasibility study to identify, analyze, and mitigate any potential cybersecurity risks associated with a third-party agreement or outsourcing a service.

Control 5.1.2 Third-party contracts shall include confidentiality, integrity, and availability, and should be consistent in all respects with the financial entity's information security policies, procedures, and standards.

Control 5.1.3 Third-party access must be monitored and reviewed. The financial entity must take appropriate action in response to any suspicious activity performed by the third party.

Control 5.1.4 Third-party and outsourcing contracts shall include clear terms for a Non-Disclosure Agreement (NDA) in case a contract is terminated or transferred to another service provider.

Control 5.1.5 The financial entity must know and agree to the involvement of subcontracted suppliers. The roles and responsibilities of both the lead and sub-contracted suppliers shall be documented, as applicable.

Control 5.1.6 Support and maintenance contracts and agreements for the financial entity's devices, systems and applications should be signed at least partially by the manufacturer company if possible.

Control 5.1.7 Outsourcing contracts shall include the Service Level Agreement (SLA) to be provided, the level of availability in the event of a disaster and after termination the customer data must be retrieved.

CONSULTATION

Control 5.1.8 The financial entity must ensure that the outsourcing service provider encrypts the customers' confidential information and stores it separately from other client data.

Control 5.1.9 Financial entity must ensure compliance with the terms of the outsourcing contract and the compliance with cybersecurity controls, policies, and procedures issued by NCSC and sector regulator.

Subdomain 5.2 Cloud Computing

The main objective of this subdomain is to ensure that proper controls are in place to protect the cloud environment of the financial entity. Entities are allowed to use more than one cloud computing service provider.

Control 5.2.1 All assets in cloud computing must be identified, and an inventory of all assets must be created and maintained.

Control 5.2.2 The financial entity must maintain logical, conceptual, and network connection diagrams for the entity's account.

Control 5.2.3 Cloud computing network segmentation and segregation must be implemented.

Control 5.2.4 Access to cloud computing for accounts and users must be role-based considering need-to-know and least privilege principles.

Control 5.2.5 The financial entity must ensure MFA is implemented for all types of access.

Control 5.2.6 The financial entity must restrict cloud computing accounts console access to only authorized IPs/subnets/connections.

Control 5.2.7 All the information stored in cloud computing must be classified based on international best practices.

Control 5.2.8 Only required system functions and network protocols can be enabled on the cloud computing services. Unnecessary functions and network protocols must be disabled.

Control 5.2.9 All security-related service packs, patches, and hotfixes must be tested and applied to all services in the cloud on time.

Control 5.2.10 Backup must be taken for services in cloud computing including taking offline backup for critical servers and storage.

CONSULTATION

Control 5.2.11 All data and information must be encrypted at rest and in transit when using cloud computing services including the outsourced cloud services. The encryption keys must be kept secure and under the financial entity's control.

Control 5.2.12 The financial entity must ensure the logical segregation of entity's data at the outsourcing service provider's platform.

Control 5.2.13 Data stored in cloud storage must be locked in a retention period to prevent deletion or modification such as implementing Write Once Read Many (WORM) or immutable storage.

Control 5.2.14 Remote users must connect to cloud computing securely and data must be decommissioned properly when not in need anymore.

Control 5.2.15 All cloud services logs should be recorded in a centralized location and actively monitored for suspicious activities and unauthorized access.

Control 5.2.16 Vulnerability assessment, penetration testing, and risk assessment activities for cloud services should be performed at the same frequency as self-hosted services.

Control 5.2.17 The financial entity must ensure that the outsourcing cloud service provider does not have the right to release entity's data and information.

Control 5.2.18 The financial entity utilizing cloud services as part of financial services should be complied with the financial cybersecurity controls.

CONSULTATION

Domain 6 Cybersecurity Incident Management

Cybersecurity-related incidents may occur even when cybersecurity controls are implemented. However, the cybersecurity controls mentioned in this domain are critical to minimizing the impact of current and future incidents. This domain contains two subdomains which are Log Management and Incident Management.

Subdomain 6.1 Log Management

The purpose of this subdomain is 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 networks, systems, and applications to identify any suspicious behavior which may lead to cybersecurity incidents.

Control 6.1.1 A log management process must be established to collect, process, review, and retain system logs.

Control 6.1.2 All recorded logs and events must be actively reviewed and monitored, and must be protected from unauthorized access, modification, and deletion.

Control 6.1.3 Logging and alerting must be implemented to detect any suspicious event or cybersecurity incidents, attempted intrusions, and unusual usage patterns.

Control 6.1.4 System time for all information processing systems must be synchronized regularly. Logs should be created and stored in Coordinated Universal Time (UTC).

Control 6.1.5 Logging of security auditing events must show successful and unsuccessful events, including inappropriate access events.

Control 6.1.6 Security audit logs must include at a minimum the user ID, date, time, and events.

Control 6.1.7 Only authorized administrators are allowed to access the logs. System administrators' activities must be regularly audited, such as the use of privileged accounts.

Control 6.1.8 The financial entity must implement a Security Information and Event Management "SIEM" system with a log retention period 5 years or longer.

Control 6.1.9 Event logs must be backed up and available for investigation purposes and maintained based on business requirements and financial sector regulation.

Control 6.1.10 Event logs must be retained and kept active based on NCSC requirements and recommendations.

CONSULTATION

Control 6.1.11 In case of manual review of logs, a weekly log review report must be generated to be shared with the senior management.

Subdomain 6.2 Incident Management

This subdomain aims to identify appropriate processes and resources to effectively respond to cybersecurity incidents and threats within an acceptable timeframe to avoid and reduce interruption in business continuity and operations in the financial entity.

Control 6.2.1 A cybersecurity incident response plan should be implemented and maintained to isolate cyber threats and resume affected services. The plan should include:

- The board and senior management commitment and severity ratings of incidents.
- Address employees' responsibilities and actions for cybersecurity incidents.
- Require the establishment of a cybersecurity incident handling team.
- The clear procedure that must be developed including cybersecurity incident handling, escalation, and reporting.

Control 6.2.2 The financial entity should regularly test and review the incident response plan to validate the effectiveness, identify gaps, and address gaps.

Control 6.2.3 The financial entity should provide training to the incident handling team members. Training should cover past incidents, lessons learned, the financial entity's current threat landscape, and new threats and attack trends worldwide.

Control 6.2.4 The financial entity should assess and classify cybersecurity incidents to determine the priorities, handling, escalation, and reporting procedure.

Control 6.2.5 The financial entity must document and retain all cybersecurity incident records and reports.

Control 6.2.6 All employees within the financial entity 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 6.2.7 The NCSC and the financial sector regulator must be informed immediately when a medium or high classified cybersecurity incident has occurred and identified or suspected based on National Cybersecurity Incident Response Plan.

Control 6.2.8 In the case of incident detected, the financial entity must activate the containment process to prevent any further damage.

CONSULTATION

Control 6.2.9 Evidence related to cybersecurity incidents must be collected and protected from any loss or tampering before the containment process. Evidence should be retained for a period 5 years or longer.

Control 6.2.10 The financial entity should contain the impact of cybersecurity incidents by scanning infected systems and removing the infections. A live system backup is required to preserve evidence due to the system's rebuilding condition.

Control 6.2.11 The financial entity management must provide a comprehensive cybersecurity incident report for each confirmed incident. The report should include:

- Date and time when the incident occurred and was detected
- Root-cause analysis
- Indicators of Compromise (IOCs)
- Description of the Impact (loss of data, disruption of services, unauthorized modification of data, (un)intended data leakage, number of customers impacted)
- Unique reference for the incident
- Classification of the incident
- Attack duration
- Information processing resources involved
- Technical details
- Corrective activities performed and planned
- The total estimated cost of the incident
- The estimated cost of corrective actions
- Key Findings
- Lesson Learned from the Incident

Control 6.2.12 A centralized cybersecurity incident repository should be maintained by the financial entity and reviewed periodically.

CONSULTATION

Domain 7 Cybersecurity Audit

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

Control 7.1 The financial entity must assign adequate auditors to carry out the internal audit process and ensure the cybersecurity requirements are effectively implemented and maintained.

Control 7.2 The internal audit process should include an audit plan, responsibilities, and requirements which should be conducted and reviewed at least annually.

Control 7.3 The internal report should be shared with the board of directors or audit committee and the financial entity's departments to get endorsement and an action plan with a target date.

Control 7.4 The external audit should be performed in coordination between the NCSC and the financial sector regulator.

Control 7.5 The financial entity must cooperate with the external auditors to fulfill the external audit requirements that do not involve sensitive or confidential information.

Control 7.6 A follow-up audit will be conducted to close the audit finding accordingly.

Control 7.7 The financial entity must perform the necessary corrective action in case of any non-compliance identified.

CONSULTATION