# Cybersecurity Guidelines for Capital Market Institutions

هيئة السوق المالية
Capital Market Authority

# Disclaimer

CMA would like to warn that this document is not an alternative to any laws or regulations applicable in the Kingdom of Saudi Arabia. In case of contradiction between this document and any of such regulations, such regulations shall prevail.Capital Market Institutions shall be responsible for applying and following the applicable laws or regulations that contribute to strengthening Cybersecurity and mitigating the impact of Cyber security threats. Also, CMA would like to highlight that this English version is a supporting document for the official reference which is Arabic version.

# Executive Summary

Through "Financial Sector Development" program, (one of the twelve Saudi Vision 2030 realization programs approved by the Council of Economic and Development Affairs), CMA seeks to make the Saudi capital market the main market in The Middle East. Moreover, CMA seeks to make it one of the key financial markets worldwide and an advanced market that attract domestic and foreign investment, so that it can play a main role in developing the economy and diversifying its sources of income. The eighth strategic goal, being strengthening stability in capital market lies under the third theme of the strategic plan "Strengthening Confidence", which consolidates participants' confidence in the market and contributes to creating an attractive investment environment that supports national economy growth. CMA works with various executive bodies to coordinate and exchange information to enhance stability in capital market and mitigate risks associated with securities transactions. Accordingly, this will strengthen security and integrity of financial information and data along with continuity of businesses of entities operating in market. In addition, the mentioned objective includes Cybersecurity Strengthening Initiative, which aims to provide a secure and transparent infrastructure and support information security to ensure stability and integrity of infrastructure.

As per Capital Market Law issued by Royal Decree No. (M/30) dated 02/06/1424 AH, this document was developed to define Cybersecurity Guidelines for Capital Market Institutions based on best practices, global and local standards that aim to mitigate risks of cyber attacks and threats against information and technology assets for Capital Market Institutions, so as to enhance electronic security stability in the capital market and reduce related risks.

# Table of Contents

# Table of Contents



# Table of Figures

# 1. Preface

## 1.1 Cybersecurity Definitions

**National Institute of Standards and Technology (NIST)** defines Cybersecurity as "The process of protecting information by preventing, detecting and responding to attacks". Similar to financial and reputational risks, cybersecurity risks can also result in high costs and affect returns, and even affect the institution's ability to innovate and gain or keep customers.

On the other hand, **International Organization for Standardization (ISO)** defines Cybersecurity or Cyberspace as "Preservation of confidentiality, integrity and availability of information in Cyberspace". In turn, "Cyberspace" is defined as "An environment resulting from interaction between people, software and services on the internet through technology devices and connected networks, which does not physically exist".

**National Cybersecurity Authority (NCA)** has issued Essential Cybersecurity Controls (ECC) as the minimum requirements of Cybersecurity that national entities must comply with. ECC aim to reduce cyber risks of various internal and external threats that affect national authorities. ECC are mandatory and all national entities, within its scope of application, shall implement requirements to achieve continued compliance. Entities shall adhere to international agreements or obligations that include Cybersecurity-related requirements when locally approved.

## 1.2 Cybersecurity Objectives

- **General objectives of Cybersecurity include:**

- **Confidentiality:** Taking necessary measures to prevent unauthorized access to sensitive and confidential information.
- **Information Integrity:** Protection against unauthorized modification or damage of information, including non-repudiation and reliability assurance.
- **Information Availability:** Ensuring access to data, information, Systems, and applications in a timely manner.

# 2. Introductiont

This document was prepared with assistance and guidance of some local and international regulatory frameworks and standards, including NCA Controls, SAMA Cybersecurity Framework, NIST, and ISO Controls.

## 2.1 Purpose

Cybersecurity Guidelines for Capital Market Institutions (Hereinafter referred to as "the Guidelines") aims to define cybersecurity controls for market institutions that help in improving Cybersecurity risk management by adopting global best practices and local Cybersecurity legislations.

## 2.2 Scope of Work

The Guidelines clarifies Cybersecurity controls for Saudi capital market institutions under the supervision of CMA.

## 2.3 Applicability

This document is considered as “guidelines” to all capital market institutions. CMA may apply this document to any entity under follow-up and supervision of CMA.

## 4.2 Review and Update

CMA shall be responsible for Guidelines’s periodic review in accordance with modifications and relevant regulatory requirements and update the same when necessary.

# 3. Guidelines Components

## 3.1 Security Domains

- **The Guidelines focuses on four main Domains:**

- Cybersecurity Governance.
- Cybersecurity Risk Management, Review and Audit.
- Operational Cybersecurity Controls.
- Third Party Cybersecurity.

- Several sub-domins for each main domin will be addressed, where security objective and main controls will be determined.

- The "Objective" describes the expected output resulting from realizing Cybersecurity controls.
- "Main Controls" contain mandatory Cybersecurity controls that should be combliant with.

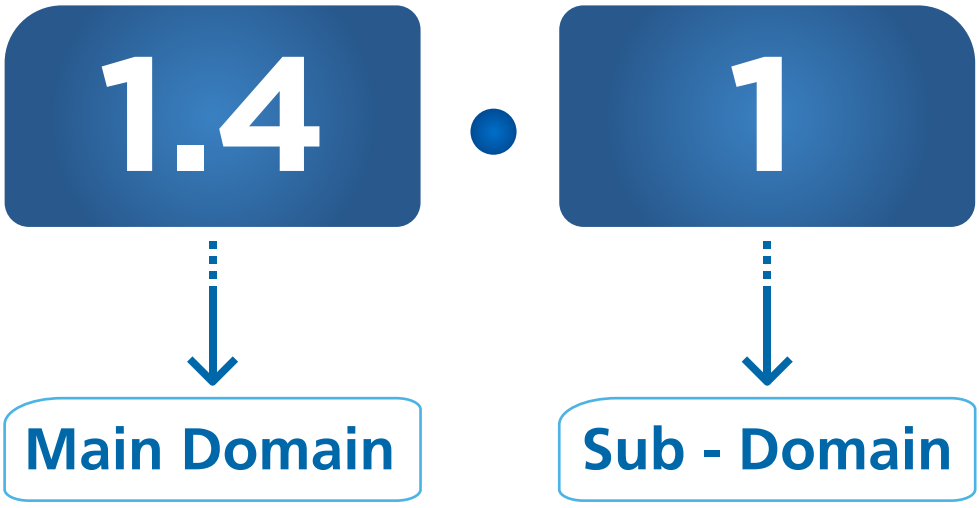


Figure 1 Numbering System

# Guidelines Components

The figure below shows general structure of the Guidelines and indicates the main Domains and sub-Domains of Cybersecurity.


Figure 2: Cybersecurity Guidelines for Capital Market Institutions

# Guidelines Components

## 3.2 Self-Assessment, Review and Audit

Implementation of the Guidelines in market institutions is subject to periodic self-assessment based on questionnaires and self-assessment forms according to a mechanism that CMA deems appropriate.

# 4. Security Domins

## 4.1 Cybersecurity Governance

Market institution's Board of Directors (BODs) shall be fully responsible for cybersecurity, and may delegate cybersecurity- related authorities to a cybersecurity committee or supervisory committee. Responsibilities of cybersecurity committee include defining cybersecurity governance, developing cybersecurity strategy for market institutions as well as defining cybersecurity policies and ensure its implementation.

### 4.1.1 Leadership and Responsibilities

**Purpose:** Defining, documenting, implementing and approving cybersecurity organizational structure, roles and responsibilities by market institution's BODs.

# Security Domins

**Main Controls:**

1. Establish a cybersecurity department separated from IT department , with taking the non-conflict of interest principle into the consideration.
2. Cybersecurity Department shall be headed by a full-time, "qualified" Saudi employee and shall be referred as "Head of Cybersecurity Department".
3. Allocate and approve an adequate budget to implement the cybersecurity tasks and functions by the market instition's BOD.
4. Review cybersecurity roles and responsibilities periodically or in case of changes.
5. Form a cybersecurity committee associated with CEO of the entity or his representative, with taking the non-conflict of interest principle into the consideration.
6. Cybersecurity Committee shall comprise of Head of Cybersecurity department and Heads of relevant departments.
7. Regulations of Cybersecurity Committee shall be prepared, documented and approved by an authorized person who clarify relevant objectives, roles and responsibilities.
8. Responsibilities of cybersecurity committee include:
    1. Monitor, review and report market institution's cybersecurity risks appetite periodically or in case of substantial change regarding risk appetite;
    2. Periodic review of cybersecurity strategy to ensure being in support of the market institution's objectives;
    3. Adopt and provide necessary support and oversight on:
        1. Cybersecurity Governance;
        2. Cybersecurity Strategy;
        3. Cybersecurity Policies;
        4. Cybersecurity Programs (such as awareness programs, data classification program, data privacy and data breach prevention);
        5. Cybersecurity Risk Management; and
        6. Cybersecurity Key Risk Indicators and KPIs.

9. Responsibilities of Market Institution's BOD include, in addition to the above-mentioned ,the following:
    1. Ensure that standards and procedures reflect cybersecurity requirements;
    2. Ensure that staff accept and comply with cybersecurity policies, and support standards and procedures when issuing and updating the same; and
    3. Ensure that cybersecurity responsibilities are included in job descriptions of relevant positions and cybersecurity positions.

# Security Domins

10 Responsibilities of Cybersecurity  Head of Cybersecurity department include:
- 1 Submit to cybersecurity committee any development and update of:
  - 1 Cybersecurity Strategy;
  - 2 Cybersecurity Policies;
  - 3 Cybersecurity Structure; and
  - 4 Cybersecurity Risk Management.
- 2 Ensure that cybersecurity standards and procedures are identified, documented, approved and implemented;
- 3 Ensure development and training of cybersecurity personnel;
- 4 Monitor cybersecurity activities (Monitor Security Operations Center);
- 5 Monitor compliance with cybersecurity policies, standards and procedures;
- 6 Oversee investigation of cybersecurity incidents;
- 7 Obtain and deal with proactive information (Threat Intelligence);
- 8 Review and audit cybersecurity program;
- 9 Effective support for other cybersecurity-related positions, including:
  - 1 Classifying systems and information;
  - 2 Defining cybersecurity controls for important projects; and
  - 3 Reviewing cybersecurity controls.
- 10 Develop and implement cybersecurity awareness programs;
- 11 Measure and report key risk indicators and KPIs on:
  - 1 Cybersecurity strategy;
  - 2 Compliance with cybersecurity policies;
  - 3 Cybersecurity standards and procedures; and
  - 4 Cybersecurity programs (Such as awareness programs and data classification program).

11 Responsibility of internal audit in market institution is to conduct a review and audit of cybersecurity controls. Such audit shall be on periodical basis with taking the non-conflict of interest principle into the consideration.

12 All market institution's personnel are responsible for complying with cybersecurity policies, standards and procedures.

## 4.1.2 Data Governance and Security

**Purpose:** To ensure that data is secured and kept confidential, available and integral.

**Main Controls:**

1. Develop and design Data Governance Program.
2. Identify data fields.
   - Data Owners
   - Data managers
   - Data Custodians
   - Data users
   - Data Dictionaries
   - Business procedures
   - Data lists
   - Report lists
   - Systems and applications
   - Policies and standards
3. Identify sensitive data elements within data fields.
4. Determine classification and mechanism of data encoding according to level of importance.
5. Identify privacy of data and information.
6. Create centralized platform for managing and controlling changes and providing access to sensitive data assets.
7. Specify mechanism to measure level of data protection.
8. Identify and implement workflow plans of governance structure and key data elements and fields.
9. Observe, monitor, and report workflow procedures.

## 4.1.3 Strategy and Policies

**Purpose:** Set out, document, implement, approve cybersecurity strategy and policies, circulate to the related parties and ensure compliance therewith.

**Main Controls:**

1. Set out, document, implement, approve and periodically update cybersecurity strategy.
2. The cybersecurity strategy shall be aligned with the overall objectives of market institution and any related regulatory requirements.
3. Cybersecurity strategy shall include the following :
   1. Importance of cybersecurity for the market institution.
   2. The expected cybersecurity state of market institution until it is able to counter cybersecurity threats.
   3. Develop a time plan to implement cybersecurity initiatives, projects and strategies.

4. Set out, document, implement and approve cybersecurity strategy and policies, circulate the same to related parties, and ensure compliance therewith.
5. Review cybersecurity policies periodically in accordance with pre-defined review plan.
6. Support cybersecurity policies with detailed security technical standards (e.g., passcode and firewall standards) to be based on local and international best practices and standards.
7. Cybersecurity policies shall include the following:
    1. Definition of Cybersecurity.
    2. The scope and objectives of the capital market institution cybersecurity.
    3. Support of senior management to cybersecurity program and objectives.
    4. Identification of cybersecurity responsibilities and roles.
    5. Indication of the reference of applicable cybersecurity standards.
    6. Cybersecurity controls shall include the following:
        1. Classifying information in a way that demonstrates its importance to a market institution.
        2. Defining ownership of all information assets.
        3. Evaluating cybersecurity risks of information assets.
        4. Making staff aware of cybersecurity.
        5. Complying with agreements as well as regulatory and contractual obligations.
        6. Reporting cybersecurity violations and suspected security vulnerabilities
        7. Appling cybersecurity requirements to Business Continuity Management.

## 4.1.4 Training and Awareness

**Purpose:** To introduce a cybersecurity program to train and educate capital market institutions employees, customers and stakeholders, with the aim of protecting capital market institution's information and technical assets.

**Main Controls:**

1. Develop, approve, document, and implement a Cybersecurity Awareness Program to promote Cybersecurity awareness.
2. The Cybersecurity Awareness Program aims to provide protection against the highest cybersecurity threats and risks and to address different groups using multiple channels.
3. Cybersecurity Awareness Program shall be launched periodically.

4. Cybersecurity and Awareness Program includes protection against cyber threats, including:
   1. Cybersecurity roles and responsibilities.
   2. Information about cybersecurity incidents and threats, for example: Phishing.
   3. Secure handling of mobile devices and storage media.
   4. Secure browsing of internet.
   5. Safe use of social media
5. Evaluate Cybersecurity Awareness Program to measure its effectiveness and make recommendations for necessary improvement.
6. Provide specialized training to cybersecurity personnel in relevant functions.

## 4.1.5 HR Cybersecurity Controls

**Purpose:** Ensure that cybersecurity responsibilities of market institution's employees are covered by their employment contracts.

**Main Controls:**

1. Set out, document, implement and approve Cybersecurity controls related to HR operation.
2. Monitor effectiveness of cybersecurity controls related to HR operation, and evaluate these controls periodically.
3. HR cybersecurity controls shall include the following:
   1. Cybersecurity Responsibilities and Non-Disclosure Clauses in Employee Contracts (during employment and after termination).
   2. Conduct a cybersecurity awareness at the beginning and during the term of employment.
   3. Applicability of disciplinary measures.
   4. Security screening of staff by entities authorized to conduct such screening.
   5. Requirements for cybersecurity controls after ending/terminating the employment relationship such as:
      1. Remove access privileges
      2. Return of personal information assets (for example: Access card, mobile devices, and all online and physical information).

# 4.2 Cybersecurity Risk Management ,Review and Audit

**Risk Management is to identify, analyze, respond to, monitor and constantly review risks. To manage cybersecurity risks, Market institution shall:**

- Identifying cybersecurity risks.
- Analyzing the potential and effects of cybersecurity risks.
- Responding to cybersecurity risks.
- Monitoring process of addressing Cybersecurity risks and reviewing effectiveness of such monitoring.

**Compliance with cybersecurity controls shall be subject to periodic review and audit.**

## 4.2.1 Cybersecurity Risk Management

**Purpose:** To set, document, approve and implement Cybersecurity risk management methodology in order to protect confidentiality, integrity and availability of information and technology assets of market institution and to ensure alignment of Cybersecurity risk management methodology with market institution's risk management methodology.

**Main Controls:**

1. Set up , document, approve, implement and periodically review cybersecurity risk management methodology.
2. Cybersecurity risk management methodology aims to protect confidentiality, integrity and availability of information assets.
3. Cybersecurity risk management methodology shall be consistent with risk management methodology adopted by market institution.
4. Document Cybersecurity risk management methodology, and identify, analyze, respond to, monitor and review risks.
5. Cybersecurity risk management methodology includes information and technology assets of capital market institution including, but not limited to:

- Work procedures.
- Business applications.
- Infrastructure components.
- Employees.

# Cybersecurity Risk Management ,Review and Audit

6. Apply cybersecurity risk assessment procedures in the following stages:
   1. Early stage of the project.
   2. Before making any material change in technology infrastructure.
   3. Before obtaining third party's services.
   4. Before launching new products and technologies.
7. Set out and document cybersecurity risks in unified record including all information and technology assets of market institution.
8. Document options list of risk processing (i.e. accept, avoid, transfer or limit risks by way of implementing Cybersecurity controls).
9. Give highest priority to and closely monitor highest cybersecurity risks as well as to prepare periodic reports on procedures taken to mitigate their effects.

## 4.2.2 Cybersecurity Review and Audit

**Purpose:** Set a mechanism to review, audit and periodically evaluate cybersecurity controls related to capital market institution's information and technology assets, in order that cybersecurity controls adopted by the market institution is in accordance with its organizational policies and procedures and relevant legislative and legal requirements.

**Main Controls:**

1. Perform review and audit for cybersecurity controls periodically.
2. Document results and remarks of review and recommended procedures, and then communicate the same to the authorized person.
3. Perform Cybersecurity audit by parties independent from Cybersecurity Department according to the generally accepted auditing standards and in accordance with Market Institutions Cybersecurity Manual.
4. Review application of cybersecurity controls in accordance with the internal audit manual and plan adopted by the market institution.

# 4.3 Operation-Related Cybersecurity Controls

- The market institution shall ensure that cybersecurity controls related to operations and procedures supporting its information assets are set, documented, approved and implemented to protect information assets operations and technologies for the market institution and its employees, customers and any related third party.
- Further, compliance with operation-related cybersecurity controls shall be monitored, and evaluated for effectiveness periodically in order to determine any potential revisions for these controls.

## 4.3.1 Cybersecurity Architecture

**Purpose:** Lay out, document, approve, track and review Cybersecurity Architecture, where market institution determines its Cybersecurity requirements and processes principles of network and applications design for enhancing Cybersecurity.

**Main Controls:**

1. Set out, document, approve, implement and monitor Cybersecurity Architecture.
2. Cybersecurity Architecture shall include the following:
   1. Strategic planning and setting out cybersecurity controls according to work requirements by Cybersecurity qualified engineers.
   2. Following necessary design principles in order to develop and implement Cybersecurity controls such as Security-by-design.
   3. Review Cybersecurity Architecture periodically.

# Operation-Related Cybersecurity Controls

## 4.3.2 Infrastructure Security

**Purpose:** Set out, document, approve and implement cybersecurity controls for infrastructure, and comply with theses controls and evaluate their effectiveness within the market institution periodically.

**Main Controls:**

1. Set out, document, approve, implement and monitor cybersecurity controls for infrastructure and evaluate these criteria periodically.
2. Infrastructure cybersecurity controls include main data centers and disaster recovery centers.
3. Infrastructure cybersecurity controls shall cover all infrastructure components (e.g. operating systems, servers, virtual devices, firewalls, network devices, IDS, IPS, wireless network, external communications, databases, sharing files, computers and lab tops and tablets).
4. E-mail cybersecurity controls include the following:
    1. Anti-spam Filtering.
    2. Multi-Factor Authentication for remote and webmail access to email service.
    3. Email archiving and backup.
    4. Validation of email service domains in technological method (e.g. Sender Policy Framework).

# Operation-Related Cybersecurity Controls

## 4.3.2 Infrastructure Security

5. Infrastructure Cybersecurity Controls include:
   1. Implementing cybersecurity controls (e.g. monitoring and maintaining events logs, preventing data leakage, managing access identity and privileges and remote maintenance).
   2. Separation of duties principle (supported by approved matrix of authorities).
   3. Protection of and dealing with data according to agreed classification system (including privacy of customer's data, avoiding unauthorized access and intended and unintended data leakage).
   4. Use genuine and licensed programs and safe IPs.
   5. Logical or physical segregation and segmentation of network segments safely.
   6. Protection against malware and viruses (allow a list of whitelisting applications and APT Protection).
   7. Management of update packages and patching of vulnerabilities.
   8. Protection against DDOS including:
      1. Use of Scrubbing Services.
      2. Adoption of agreed bandwidth specifications.
      3. Continuous monitoring 24/7 by SOC, Service Provider and Scrubbing Provider.
      4. Test DDOS scrubbing at least twice per year.
      5. Protect main data centers and Disaster Recovery centers from DDOS.
   9. Secure browsing and internet connectivity including restricted access to suspicious websites, storage servers and remote access websites.
   10. DNS security.
   11. Clock Synchronization with an accurate and trusted source.
   12. Conduct data backup and recovery.
   13. Restricted use of external storage media.
   14. Review compliance with Cybersecurity controls periodically.

# Operation-Related Cybersecurity Controls

## 4.3.3 Change and Projects Management

**Purpose:** Set out, document, approve and implement methodology and procedures for change and project management to ensure application of a unified, documented and approved methodology for project management and any change on information and technology assets.

**Main Controls:**

1. Set out, document, approve, implement, monitor and evaluate change management methodology periodically.
2. Change management methodology and procedures shall include the following:
    1. Cybersecurity controls to manage emergency changes to information and technology assets such as evaluating change impact and sorting, classifying and reviewing changes.
    2. Security testing, which shall include:
        1. Penetration Testing.
        2. Security Source Code Review in case of developing applications internally or externally (If the Source Code of external applications is not available, the source code review report shall be sufficient).
    3. Changes shall be approved by the authorized person.
    4. The approval of Cybersecurity Department on the market institution shall be sought before submitting changes to Change-Advisory Board for its approval.
    5. Review how far the change is acceptable after implementing relevant cybersecurity controls.
    6. Segregation of duties.
    7. Segregate of production environment from development and testing environment.
    8. Conduct emergency changes and repairs.
    9. Fallback and Rollback.
3. Set out, document, approve, implement, monitor and periodically evaluate project management methodology.
4. Project management methodology shall include cybersecurity requirements to ensure identification and addressing of cybersecurity-related risks as a part of the project.

5. Project management methodology shall include the following:
   1. Include cybersecurity objectives within the project objectives.
   2. Consider cybersecurity management as a part of project stages.
   3. Assess risks at the beginning of project in order to set out and process cybersecurity risks.
   4. Document Cybersecurity risks in project risk record and follow up these risks.
   5. Identify and assign cybersecurity responsibilities.
   6. Review cybersecurity by an independent internal or external party.
6. Project and change management methodology includes evaluating and processing vulnerabilities and reviewing configuration, shielding and patching.

## 4.3.4 Identity And Access Management

**Purpose:** Restrict access to information assets according to relevant work requirements and on a Need-to-Know or Need-to-Have basis to ensure sufficient accessibility and authorized access for users' approval.

**Main Controls:**

1. Set out, document, approve, implement and monitor access identity and privileges management policy.
2. Measure and periodically evaluate effectiveness of cybersecurity controls within access identity and privileges management policy.
3. Access identity and privileges management policy shall include the following:
   1. Access control according to work requirements (principles of Need-to Know, Need-to-Have and Least Privilege).
   2. Users Access Management.
      1. Covering all users (employees and third parties).
      2. Involving User ID verification.
      3. HR Department shall be responsible for conducting any change to employment status or position of employees.

# Operation-Related Cybersecurity Controls

4 Cybersecurity Department's approval shall be obtained in case of conducting any change to external employees or third parties.
5 Obtain official and certified approval for user access according to work requirements (i.e. principles of Need-to-Know and Need-to-Have to avoid unauthorized access and intended and unintended data leakage).
6 Process any emergency changes to access privileges in a timely manner.
7 Review user access privileges and profiles periodically.
8 Review the submitted, approved and processed user access applications and process related cancelation applications.
3 User Access Management shall be automated.
4 Provide uniform systems for access identity and privileges management.
5 Multi-Factor Authentication for access to sensitive systems and accounts.
6 Management controls of high and sensitive privileges and access management include:
1 Restricted and customized use of remote access and accounts with high and sensitive privileges; especially:
1 Use Multi-Factor Authentication mechanism for all remote access operations.
2 Use Multi-Factor Authentication mechanism for accounts with high and sensitive privileges on sensitive systems according to risk assessment.
2 Conduct periodic review for users with important and sensitive accounts and remote access accounts.
3 Accountability in case of violations.
4 Use of important and sensitive systems accounts includes:
1 Restriction and monitoring.
2 Maintaining password confidentiality
3 Changing passwords periodically.

# Operation-Related Cybersecurity Controls

## 4.3.5 Information and Technology Assets Management

**Purpose:** Set out, document, approve, implement, circulate and monitor information and technology assets management in order to obtain accurate, unified and updated asset record, to support market institution in getting an accurate and detailed inventory.

**Main Controls:**

1. Set out, document, approve, implement, monitor and periodically evaluate information and technology assets management.
2. Information and technology asset management includes, but not limited to:
   1. Unified record including information and technology assets during their full lifecycles.
   2. Ownership of Information and technology assets.
   3. Classification, labeling and handling of information and technology assets.
   4. Maintaining backup of assets records and keeping them in safe place.
3. Set out, document, approve, implement, circulate and periodically evaluate acceptable use policy.

## 4.3.6 Safe Disposal

**Purpose:** Dispose of market institution's information assets safely when they are no longer needed, to ensure protecting market institution's business, customers and sensitive information from disclosure, unauthorized disclosure upon disposal thereof.

**Main Controls:**

1. Set out, document, approve and implement safe disposal criteria and procedures.
2. Safe disposal standards cover digital and hard copies and reuse of assets.
3. Monitor compliance with safe disposal standards and procedures.
4. Measure and periodically evaluate effectiveness of Cybersecurity controls on safe disposal.
5. Dispose of information assets when they are no longer needed according to the relevant legislative and legal requirements and in line with data privacy regulations to avoid unauthorized access and intended and unintended leakage.
6. Destroy sensitive information using certain technologies to make information not recoverable (e.g. Secure Wiping and Degaussing).
7. Ensure that third-party service providers comply with safe disposal standards and procedures, and measure and evaluate this effectiveness periodically.

# Operation-Related Cybersecurity Controls

## 4.3.7 Cybersecurity Incident Management

**Purpose:** Set out, document, approve and implement cybersecurity incident management process in line with incident management procedures followed by market institution, with the aim to determine, respond to and overcome cybersecurity incidents as well as to measure and periodically evaluate effectiveness of this process to ensure identification and processing of cybersecurity incidents in a timely manner and limit potential adverse negative impacts on market institution.

**Main Controls:**

1. Develop, document, approve and implement cybersecurity Incident Management Process and align the same with Incident Management Procedures followed by the market institution.
2. Disaster recovery plan includes different scenarios of cybersecurity incidents.
3. 3. Measure and periodically evaluate effectiveness of cybersecurity controls under Cybersecurity incident management process.
4. Cybersecurity incident management controls shall include:
    1. A team in charge of cybersecurity incident management.
    2. Provision of well-qualified employees and trainers.
    3. Restricted area for Cybersecurity Emergency Response Team (CERT).
    4. Setting response plan for security incidents and escalation mechanisms.
    5. Classifying of Cybersecurity incidents.
    6. Addressing Cybersecurity incidents in a timely manner, following-up, and monitoring the progress made.
    7. Protecting related evidence and records.
    8. Criminal analysis of cybersecurity incidents.
    9. Maintaining cybersecurity incidents record.

# Operation-Related Cybersecurity Controls

5. Coordinating with CMA before any media action concerning the security incident.
6. Report National Cybersecurity Authority of CMA immediately after occurrence/detection of any incident.
7. Provide official report on security incident to CMA after resuming operation including the following details:
    1. Name of Cybersecurity incident.
    2. Classification of Cybersecurity incident (mild or severe).
    3. Date and time of Cybersecurity incident.
    4. Date and time when the Cybersecurity incident is detected.
    5. Information assets affected.
    6. Technical details of Cybersecurity incident.
    7. Analysis of reasons and motivations.
    8. Taken and planned remedial procedures.
    9. Description of damage caused (e.g. data loss, services failure, unauthorized modification and intended and unintended data leakage and the number of affected customers).
    10. Total cost estimated for the Cybersecurity incident.
    11. Estimated cost for corrective procedures.
    12. The report shall be sent to following mail: Cyber.Incident@cma.org.sa

# Operation-Related Cybersecurity Controls

## 4.3.8 Cybersecurity Event Logs Management

**Purpose:** Define, document, approve and implement security event logs management to analyze security registration and deal with cybersecurity events. The efficiency of this process shall be periodically measured and evaluated to ensure identification of suspicious events related to information assets and response thereto in a timely manner.

**Main Controls:**

1. Define, document, approve and implement security event logs management process.
2. Measure and periodically evaluate the effectiveness of cybersecurity controls related to security event logs management process.
3. Define, document, approve and implement control standards for cybersecurity event logs to support that process.
4. Identify event standards to be monitored based on classification of information assets or risk profile.
5. Monitor cybersecurity event logs for accounts with high and sensitive privileges and remote login accounts.
6. Retention period for cybersecurity event logs must be 12 months at least.
7. Event logs management shall include the following:
   1. Form a teamwork in charge of security control (Security Operation Center "SOC").
   2. Well-trained and qualified citizen employees.
   3. A restricted area dedicated for SOC related activities.
   4. Resources required for constant monitor of security events for 24 hours a day, seven days a week (24/7).
   5. Retrieving the source code and detecting malware.
   6. Detecting suspicious security events and addressing them.
   7. Using solutions to analyze network packages.
   8. Protecting cybersecurity event records.
   9. Periodical monitoring of compliance with cybersecurity standards for applications and infrastructure.
   10. Using automated and central analysis of security logs and linking events and patterns (e.g. Security information and event management and cybersecurity monitor "SEIM").
   11. Reporting cybersecurity incidents.
   12. Conducting a periodic and independent test to verify SOC effectiveness (For example: Red Team).

8. In case of any major cybersecurity incident:
   1. A crisis management team comprising an employee of market institution's board of directors, representatives of executive management and qualified persons shall be formed to deal with incidents.
   2. Disclosure of cybersecurity incidents shall be made according to certain standards and shall include stakeholders.
   3. An improvement and development plan shall be developed after the end of crisis. In addition, necessary measures shall be taken and relevant recommendations shall be made based on the report.
   4. Ensure that the incident has ended with all supporting documents explaining how the incident ended, the lessons learned and any additional investigations and post-crisis reviews and reports needed.

## 4.3.9 Cybersecurity Threat Management

**Purpose:** Set out, document, approve and implement Cybersecurity Threats Management process, aiming to identify, evaluate and understand risks threating market institution's technical and information assets by using reliable multiple sources and measure and evaluate effectiveness of this process.

**Main Controls:**

1. Define, document, approve and implement Cybersecurity Threats Management process.
2. Periodically measure and evaluate effectiveness of Cybersecurity Threats Management process.
3. Cybersecurity Threats Management process shall include the following:
   1. Using the internal sources, such as access and applications control, infrastructure records, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), security tools and SEIM in addition to the supporting department (such as Legal and Audit, Technical Support, Criminal Investigation, Anti-fraud and Compliance and Risk Departments).
   2. Utilizing reliable external sources that are related to threat intelligence, such as government entities and security service providers.
   3. Develop a certain methodology to periodically analyze threats-related information.
   4. Details related to certain threats, such as work method, actors, motivations and threats type.
   5. Sharing the relevant threat intelligence with the concerned entities.

# Operation-Related Cybersecurity Controls

## 4.3.10 Applications Protection

**Purpose:** Set out, document, approve and implement applications cybersecurity controls, monitor compliance with these standards and periodically measure and evaluate effectiveness of these controls.

**Main Controls:**

1. Define, document, approve and implement applications cybersecurity controls.
2. Monitor compliance with cybersecurity controls to protect applications.
3. Periodically measure and evaluate effectiveness of applications cybersecurity controls.
4. Follow the adopted methodology on Software Development Life Cycle upon development of applications.
5. Applications Cybersecurity controls shall include the following:
    1. Adoption of Applications' Secure Coding Standards.
    2. Applicable cybersecurity controls (Configuration Parameters) and events to be monitored and retained (including system and data access), Identity Management, Access privileges).
    3. Using reliable and approved sources and libraries.
    4. Using Multi-tier Architecture Principle, Multi-Factor Authentication, Web Application Firewall and secure protocols.
    5. Conducting penetration testing for all external (Online) services annually at minimum.
    6. Application integration security.
    7. Acceptable Use Policy
    8. Segregation of Duties supported by the approved matrix of authorities.
    9. Protecting and dealing with data according to the classification system adopted (including client data privacy, prevent unauthorized access, intended or unintended data leakage).
    10. Manage vulnerability, updates package and security patching.
    11. Backups and data recovery procedures.
    12. Periodic review of compliance with cybersecurity controls.

# Operation-Related Cybersecurity Controls

## 4.3.11 Encryption

**Purpose:** Set out, document, approve and implement encryption solutions for market institution to ensure prevention of unauthorized access to, and integration of sensitive information.

**Main Controls:**

1. Define, document, approve and implement encryption standards.
2. Monitor compliance with encryption standards.
3. Periodically measure and evaluate effectiveness of encryption cybersecurity controls.
4. Encryption standard shall include the following:
    1. General review of approved encryption solutions and restrictions thereof (Technically and organizationally).
    2. Cases to which the approved encryption solutions shall apply.
    3. Managing encryption keys, including managing their life cycle, as well as archiving and recovering them.
    4. Encrypting data during transfer and storage based on their classification and according to the relevant best practices, standards and legislative and regulatory requirements.

## 4.3.12 Vulnerabilities Management

**Purpose:** Set out, document, approve and implement a Security Vulnerabilities Management process to detect and counter effects of vulnerabilities in the applications and infrastructure, and measure and evaluate effectiveness and impact of this process periodically.

**Main Controls:**

1. Set out, document, approve and implement vulnerabilities management process.
2. Measure and evaluate effectiveness of vulnerabilities management process periodically.
3. The vulnerabilities management process shall include:
    1. All information and technical assets;
    2. Periodic vulnerability scan;
    3. Classifying security vulnerabilities;
    4. Setting timelines to patch vulnerabilities, based on their classification;
    5. Setting priorities for classified information and technology assets;
    6. Managing security patching and implementation methods;
    7. Communicating and cooperating with trusted sources regarding new and patched vulnerabilities alerts.

# Operation-Related Cybersecurity Controls

## 4.3.13 E-Trading Services

**Purpose:** Set out, document, approve, implement and monitor cybersecurity controls on e-trading services, and periodically measure and evaluate effectiveness of these controls, with the aim of ensuring confidentiality of customer information.

**Main Controls:**

1. Set out, document, approve and implement cybersecurity controls of e-trading services.
2. Monitor compliance with e-trading services cybersecurity controls.
3. Measure and evaluate effectiveness of e-trading services' cybersecurity controls periodically.
4. E-Trading Services Cybersecurity Controls shall include the following:
    1. E-services protection, including social media.
    2. E-trading protection via smart devices and mobile through:
        1. Using genuine and trusted application stores and websites;
        2. Preventive measures to detect and close fake applications and websites;
        3. Using "Sandboxing";
        4. Using "Non-Caching" techniques;
        5. Using communication technologies to avoid "Man-in-the-Middle" attacks;
        6. Using multi-factor identity verification:
            1. The multi-factor identity verification method shall be used during registration by customer for using e-trading services;
            2. The multi-factor identity verification method shall be applied to all available e-trading services to customers;
            3. Protect security codes with a password;
            4. Block customer access option after entering 3 consecutive incorrect passwords or invalid "PIN";
            5. Conduct and activate multi-factor identity verification requests through different communication channels;
            6. Apply the multi-factor identity verification method to the following processes:
                1. Log in;
                2. Reset password.
        7. Ensure continuity and availability of e-trading services;
        8. The agreement between the market institution and customer shall include setting of roles, responsibilities and obligations of both the market institution and customer regarding cybersecurity requirements;
        9. CMA shall be notified upon initiating a new e-trading service.

3. **Instant notification via SMS:**
   1. No "SMS" shall contain sensitive data (such as customer's national ID number, and investment portfolio number);
   2. SMS notice shall be sent to customer's phone number when a new multi-factor identity verification is requested;
   3. SMS notice shall be sent to customer's phone number when initiating any trading, subscription or redemption transaction

## 4.3.14 Physical Security

**Purpose:** Physical protection of all facilities of the Market Institution to prevent unauthorized physical access and ensure protection of the Market institution.

**Main Controls:**

1. Set out, document, approve, and implement physical security controls.
2. Measure, monitor effectiveness, and periodically evaluate physical security controls.
3. Ensure that trading services are protected against service disruption due to power outage.
4. Monitor fire alarms on an ongoing basis, test them regularly, and maintain them according to manufacturer specifications.
5. Mitigate the impact of natural disasters.
6. The physical security process includes, but not limited to, the following:
   1. Physical entry controls (including visitor security);
   2. Surveillance and monitoring (using "CCTV" systems, sensors, etc.);
   3. Protecting data centers, data rooms and power supplies for crucial facilities;
   4. Protection against environmental hazards;
   5. Protect information assets during their life cycle (including transportation, safe disposal, avoid unauthorized access and intentional or unintentional data leakage);
   6. Train personnel on use of fire extinguishers and other safety equipment.

# Operation-Related Cybersecurity Controls

## 4.3.15 Business Continuity Management

**Purpose:**Set out, document, approve and implement business continuity policy, strategy and plans based on assessment of Cybersecurity risks and Business Impact Analysis (BIA), and to monitor compliance with these specific controls, measure effectiveness of its impact and evaluate it periodically to ensure effectiveness and readiness of the disaster recovery plans and work teams in the event of an accident, as well as to review them periodically.

**Main Controls:**

1. Set out, document, approve and update a business continuity policy and communicate the same to stakeholders inside and outside the market institution.
2. Review business continuity policy on an annual basis or when significant changes occur.
3. Identify standards, legislation and regulations to be observed on development of business continuity policy.
4. Conduct BIA, through which all key processes and services can be identified for market institution's business.
5. Conduct BIA on an annual basis to identify scope of Business Continuity Management Program and to confirm business priorities and resources.
6. Prepare a Business Continuity Management Strategy that clarifies business recovery requirements and is consistent with time required and expected to restore the capacity for work specified and approved in BIA.
7. Establish a Crisis Management Team, comprising representatives of the board of directors, executive management and employees qualified to deal with accidents that affect business continuity.
8. The business continuity plan includes clear and specific steps that shall be taken in the event of crises or emergencies, contact details of all officers in charge, in addition to regular testing of the plan to know how far it represents the reality.
9. Test Business Continuity Management and Disaster Recovery Plans periodically or after every material change to ensure being suitable, updated and compatible with business continuity objectives.
10. Ensure that employees entrusted with developing Business Continuity Management Programs are trained and qualified and have the necessary experience to deal with management of such plans and programs.
11. Provide general training and awareness required for all employees regarding Business Continuity Management.

# Operation-Related Cybersecurity Controls

## 4.3.16 Use of Personal Devices "BYOD"

**Purpose:**Define Cybersecurity standards and controls for use of smart devices (such as smartphones, tablets and laptops) for business purposes, in order to ensure confidentiality and protection of market institution information.

**Main Controls:**

1. Set, document, approve and apply a BYOD cybersecurity policy.
2. Monitor compliance with the BYOD cybersecurity policy.
3. Measure effectiveness of BYOD cybersecurity controls, and evaluate them periodically.
4. BYOD cybersecurity policy shall include the following:
    1. User responsibilities including training and raising awareness.
    2. Indication of restrictions imposed, and consequences to which employees shall be subject when applying cybersecurity controls to their personal devices; for example in cases such as using devices with modified (cracked) software (rooting or cracking tools "Jailbreaking"), termination of employment, or loss of personal device.
    3. Separate market data and information from personal information (Containerization):
    4. Rule of use of genuine mobile applications related to market institution or general use.
    5. Use of Mobile Device Management (MDM) to apply remote access controls, encryption mechanisms and deletion of data and information stored on the personal device remotely.

# 4.4 Cybersecurity for Third Parties and Suppliers

- **When dealing with a third party, the market institution shall ensure that the same level of Cybersecurity protection is applied to the said third party, as is the case in the market institution.**

- **Relevant Cybersecurity requirements shall be set out and regulated between the market institution and third parties, and shall be then documented, approved, applied and monitored. Third parties are defined in the Guidelines as the outsourcing services providers, external services providers, cloud Computing suppliers, sellers, suppliers and governmental entities etc.**

## 4.4.1 Contracts and Suppliers Management

**Purpose:**Set out, document, approve, apply and monitor Cybersecurity controls regarding management of Contracts and Suppliers.

**Main Controls:**

1. Set out, document, approve, apply and circulate Cybersecurity controls related to management of contracts and suppliers.
2. Monitor compliance with Contracts and Suppliers Management process.
3. Measure and periodically evaluate effectiveness of Cybersecurity controls related to management of contracts and suppliers.
4. Contracts and Suppliers Management process shall include:
   1. inclusion of the minimum cybersecurity controls that shall be applied in all cases.
   2. Authority to conduct periodic cybersecurity audit and review.
5. Contracts Management process shall include:
   1. Evaluate Cybersecurity risks as a part of signing contracts with third party (e.g. Outsourcing and Managed Services).
   2. Define Cybersecurity controls as a part of bidding.
   3. Evaluate responses of potential suppliers according to cybersecurity controls adopted.
   4. Test the agreed cybersecurity controls (Risks-Based Testing).
   5. Identify communication and escalation procedures in case of cybersecurity incident.
   6. Lay down Non-Disclosure Clauses.
   7. Safe disposal by the third party of market institution's data upon the end of contractual relationship.
6. Suppliers Management Process includes preparing, reviewing and evaluating periodic reports for cybersecurity controls agreed upon in the relevant agreements (SLA).

# Cybersecurity for Third Parties and Suppliers

## 4.4.2 Outsourcing

**Purpose:**Set out, document, approve, apply and monitor cybersecurity controls set forth in outsourcing policy and process, and measure and evaluate effectiveness of the prescribed cybersecurity controls.

**Main Controls:**

1. Set out, document, approve and apply cybersecurity controls set forth in outsourcing policy and process and circulate the same across the market institution.
2. Measure and periodically evaluate cybersecurity controls related to outsourcing policy and process.
3. Outsourcing includes engagement of Cybersecurity Department and evaluating Cybersecurity risks.
4. Compliance with related national laws and regulations.
5. Outsourcing is limited to providing security operations monitoring services for service providers within KSA.

## 4.4.3 Cloud Computing

**Purpose:**Set out, document, approve, apply and monitor cybersecurity controls related to cloud computing and hosting services, and measure and evaluate effectiveness of these cybersecurity controls.

**Main Controls:**

1. Set out, document, approve and apply cybersecurity controls related to Cloud Computing Policy organizing cloud computing and hosting services and circulate the same across the market institution.
2. Monitor compliance with Cloud Computing Policy.
3. Measure and periodically evaluate cybersecurity controls related to Cloud Computing Policy organizing cloud computing and hosting services.
4. Cybersecurity controls related to Cloud Computing Policy shall include:
   1. Approval of cloud computing services, which include:
      1. Conduct cybersecurity risk assessment of cloud computing services provider.
      2. Conclude a contract laying down cybersecurity controls before using cloud-computing services.
   2. Conduct data classification before hosting.
   3. Data hosting location, i.e. to use cloud-computing services within KSA.
   4. Data use restrictions, which prevent cloud computing service provider from using data of market institution for other purposes.
   5. Protection; Cloud Computing Service Provider shall apply and monitor cybersecurity controls as defined in risk assessment in order to protect confidentiality, integrity and availability of market institution's data.
   6. Segregation of data; to properly separate market institution's data from other data maintained by the cloud computing service provider, in order for the cloud computing service provider to be capable of identifying market institution's data and distinguishing them from other data at all times.
   7. Business Continuity; to meet business continuity requirements according to business continuity policy adopted by the market institution.
   8. The market institution shall have the right to conduct cybersecurity review, audit and inspection of the cloud computing service provider.
   9. Termination, which includes:
      1. The market institution shall have the right to termination.
      2. The market institution shall have the right to recover its data from the cloud computing service provider, upon termination, in an appropriate and usable form.
      3. The market institution shall have the right to request deletion of its data by cloud computing service provider, upon termination, in an unrecoverable way.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Access management**

The process of granting authorized users the right to use the service and denying it to unauthorized users.

**Advanced Persistent Threats (APT)**

Protection from advanced threats that use hidden methods aimed at illegal access to technical systems and networks and trying to stay in them as long as possible by avoiding detection and protection systems. These methods usually use Malware Day-Zero viruses and malware that are not previously known to achieve their goal.

**Application Whitelisting**

A list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which use blacklists to prevent known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

**Asset**

Anything tangible or intangible that has value to an organization. There are various types of assets; and some of them include tangible items such as persons, machinery, utilities, patents, software and services. The term asset may include intangible items such as: information and properties (mental image, reputation or skills and knowledge).

**Assurance**

Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (١) functionality that performs correctly, (٢) sufficient protection against unintentional errors (by users or software), and (٣) sufficient resistance to intentional penetration or by-pass.

**Attack**

Any kind of malicious activity that attempts to illegally collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Audit**
Independent review and examination of records and activities to assess the adequacy of cybersecurity controls, to ensure compliance with established policies and operational procedures as well as relevant legislative and regulatory requirements.

**Availability**
Ensuring timely and reliable access to and use of information, data, systems and applications.

**BOD**
Board of Directors.

**Bring Your Own Device (BYOD)**
BYOD refers to personally owned computing devices, such as laptops, tablets or smartphones that employees and operators are permitted to use at their place of work.

**Business applications**
Any application used by employees to perform various business functions in the entity.

**Business Continuity**
The organization's ability to continue provision of IT and business services at determined and pre-accepted levels after occurrence of disruption event.

**Business impact analysis (BIA)**
Determine important activities and priorities of institution, in addition to determining extent of reliability between various activities, minimum resources needed for recovery, and extent of the impact that business interruption can cause.

**Capital Market Institutions**
Financial institutions licensed by and fall under supervision and control of CMA

**Change Advisory Board**
The board which provides support to change management team through introducing required changes and help in change evaluation and prioritization.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Change management**
Identifying and introducing required changes with regard to control of business systems/information.

**Chief Executive Officer**
The executive official having the authority to take key decisions within the organization.

**Closed Circuit Television (CCTV)**
is the use of video cameras to transmit signals to a specific place into a limited set of monitors.

**Cloud computing**
A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of IT resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing allows users to access IT-based services through cloud computing network without need to have knowledge or control of IT supporting infrastructure.

**Confidentiality**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Cybersecurity Committee**
It aims to help capital market institution to obtain good practices of cybersecurity, established by CMA.

**Cybersecurity Controls**
Administrative, operational and technical controls (measures or counter-measures) stipulated in information system for protecting confidentiality, integrity and availability of system and its information.

**Cybersecurity Governance**
A set of responsibilities and practices performed by BOD and Executive Management, with a view to provide strategic guidance of cybersecurity and to ensure achievement of its goals, and to ensure cybersecurity risks are appropriately managed and enterprise's resources are properly utilized.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Cybersecurity Outreach Program**

A program that explains code of conduct suitable for safe use of IT systems. The program contains cybersecurity policies and procedures to be followed.

**Cybersecurity policy**

A set of established standards to provide security services. These standards determine activities of data processing utilities to be conducted to preserve security status of systems and data.

**Cybersecurity Resilience**

The enterprise's overall ability to withstand and recover from cybersecurity events and adverse conditions.

**Cybersecurity risks**

The risks that prejudice organization's business (including the organization's mission, mental image or reputation) or organization's assets, individuals, other organizations or the state, due to possibility of unauthorized access and/or use or disclosure, or disruption, modification or destruction of information and/or information systems.

**Cybersecurity**

A set of security tools, policies, concepts, guarantees, guidelines, risk management approach, procedures, training courses, best practices, guarantee and technologies that can be used to protect information assets of capital market institution against internal and external threats.

**Data classification**

Determine data sensitivity level during its creation, modification, enhancement, storage or transfer. Thereafter, Data classification locates the need for controlling or securing the data, and indicates its value in terms of commercial assets.

**Effectiveness of Cybersecurity Controls**

Measuring authenticity of execution (how far control is exercised in alignment with security plan) and how far security plan meets organizational needs according to existing risk tolerance.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Encryption**

The rules that include principles, methods and tools for storing, transferring data or information in a specific manner, in order to hide its meaningful content, prevent unauthorized access or undiscovered modification, in such a way that no irrelevant person can read and process the same.

**Enterprise risk management**

The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.

**Forensic evidence**

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

**Identity Management**

The process of controlling information about users on computers, including information that authenticates the identity of a user and systems and/or actions authorized. It also includes information about the user and how and by whom that information can be accessed and modified.

**Incident**

Security breach of violating cybersecurity policies, acceptable use policies, cybersecurity practices, controls or requirements.

**Incident management plan**

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information systems(s).

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Integrity**

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Intrusion detection system (IDS)**

IDS operate on hardware or software that collects information from different regions within a computer or network to identify and analyze potential security breaches that include all attempts of infiltration (attacks from outside organizations) and misuse (attacks from within organizations).

**Intrusion Prevention System (IPS)**

System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

**Jailbreaking**

A privilege escalation of the device, for the purpose of removing software restrictions imposed by software manufacturer, often leads to unlimited privileges on the device.

**Key Performance Indicators (KPI)**

A type of performance level measurement tools that evaluates success of an activity or organization towards achievement of specific goals.

**Likelihood**

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

**Malware**

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Mobile Device Management (MDM)**
is an industry term for management of mobile devices.

**Multi-Factor Authentication (MFA)**
Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

**Intrusion Prevention System (IPS)**
System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

**NIST**
National Institute of Standards and Technology www.nist.gov.

**Official documentation**
Written documentation approved by the senior management and communicated to relevant stakeholders.

**Patch**
An Update of operating systems, applications, or any other programs that are specially developed to correct specific problems in the program, including vulnerabilities.

**Penetration Test**
Test a computer system, network, website application, or smart phone application to find out vulnerabilities that the attacker could exploit.

**Personal devices**
Devices that are not owned or issued by the institution, such as smartphones.

**Personal identification number (PIN)**
A password consisting only of decimal digits.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Physical security**

Physical protection for facilities hosting information assets from intended and unintended security events.

**Portable storage device**

Portable device / flash drives (such as floppy disks, CDs, USB flash drives, external hard disk, and other flash memory cards/ drives that contain nonvolatile memory), as well as computing and portable communication devices with the capacity of storing information (for example: laptop, PDA, cell phones, digital cameras, and voice recorders).

**Authorites matrix**

Matrix defines rights and permissions a particular job requires in order to access information. The matrix identifies each user's roles and tasks, and the affected systems.

**Privileged Accounts**

An information system account with approved authorizations of a privileged user to perform security-related functions that ordinary users are not permitted to perform.

**Official documentation**

Written documentation approved by the senior management and communicated to relevant stakeholders.

**Risk register**

A sheet used as reference for all determined risks. It includes additional information about each risk separately, for example: risk category, risk owner and mitigation measures.

**Sandboxing**

A restricted, controlled execution environment that prevents potentially malicious software from accessing any system resources except those for which the software is authorized.

**Secure Coding Standards**

The practice of developing computer software and applications in a way that guards against the accidental introduction of security vulnerabilities related to software and applications.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Security information and event management (SIEM)**

A system that manages, analyzes data of security events logs in the real time, to provide control of threats, analyze results of interrelated rules of event logs, prepare reports about log data and incident response.

**Security Operations Center (SOC)**

A dedicated site (and team) where security-related data of enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. In most cases, SOC is allocated for inspection, investigation and potential response to security breach indicators. SOC works closely through security-related classified information, and disseminates the same in other areas in the organization (Such as Cybersecurity functions, incident management team, IT service providers).

**Sensitive Information**

Information where the loss, misuse, or unauthorized access or modification could adversely affect the organizational matters or the privacy of individuals. In addition, sensitive information is also information that is sensitive in accordance with the regulatory data classification policy.

**Service Level Agreement**

An agreement between two parties, where one party is the customer and the other is service provider, which clarifies services that must be rendered by the service provider and criteria that must be met to render the service.

**Software Development Life Cycle (SDLC)**

SDLC describes the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

**Threat**

Any circumstance or event related to information system, with the potential to adversely affect capital market institution's business (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

# Appendices

## Terms and Definitions

The below table illustrates some terms and their definitions contained herein:

**Threat Intelligence**

An organized information about recent, current and potential attacks that may pose cybersecurity threat to an organization.

**Vulnerabilities Management**

Periodic practice of identifying, evaluating and treating security vulnerabilities.

**Vulnerability**

A weakness found in computer system, programs or applications, a set of procedures, or anything that makes cybersecurity triggered by a threat.