Suruhanjaya Sekuriti
Securities Commission
Malaysia

GUIDELINES ON TECHNOLOGY RISK MANAGEMENT

SC-GL/2-2023 (R1-2024)

Issued: 1 August 2023
Revised: 19 August 2024

GUIDELINES ON TECHNOLOGY RISK MANAGEMENT

Effective Date upon 1st Issuance	19 August 2024

LIST OF REVISIONS

Revision Series	Revision Date	Effective Date	Series Number
1st Revision	19 August 2024	19 August 2024	SC-GL/2-2023 (R1-2024)

CONTENTS

PART A: GENERAL

Chapter 1

INTRODUCTION

1.01 The *Guidelines on Technology Risk Management* (Guidelines) are issued by the Securities Commission (SC) pursuant to section 377 of the *Capital Markets and Services Act 2007* (CMSA).

1.02 Digital revolution has enabled a new era of connectivity, convenience and innovation. Consequently, there are more capital market entities leveraging technologies to carry out their activities in recent years.

1.03 To further strengthen the ability of capital market entities to detect and mitigate risks that come with greater technology adoption, these Guidelines introduce a comprehensive regulatory framework for the management of technology risk in capital market entities.

1.04 These Guidelines set out the following requirements:

(a) Roles and responsibilities of the board of directors and senior management in the oversight and management of technology risk;

(b) Frameworks, policies and procedures that should be developed and implemented by capital market entities;

(c) Requirements for managing technology risk; and

(d) Reporting and notification requirements to the SC.

Chapter 2

APPLICABILITY

2.01 These Guidelines apply to the capital market entities as defined in paragraph 4.01 below.

2.02 Capital market entities are expected to assess the application of these Guidelines and ensure the extent and degree of implementation commensurate with their respective business operations as well as the level of technology risk exposures.

2.03 The outcome desired by the SC for the Guidelines is two-pronged, that is for all capital market entities to have a robust and sound technology risk management framework which promotes strong oversight of technology risk in the capital market entity, and ultimately for the capital market to be cyber resilient.

2.04 Where relevant, capital market entities should adopt the Guiding Principles Relating to the Adoption of Artificial Intelligence (AI) and Machine Learning (ML) as specified in **Appendix 3**. The guiding principles shall be read together with these Guidelines, relevant laws and regulations, and guidelines issued by the SC or any other relevant regulator.

2.05 Where appropriate, guidance is provided in these Guidelines. Any departure from the guidance will be taken into consideration in the SC's assessment on whether a breach of these Guidelines had occurred.

2.06 The SC may, upon application, grant an exemption from or a variation to the requirements of these Guidelines if the SC is satisfied that—

(a) such variation is not contrary to the intended purpose of the relevant requirements in these Guidelines; or

(b) there are mitigating factors which justify the said exemption or variation.

Chapter 3

RELATED PROVISIONS

3.01 These Guidelines shall supersede and replace the *Guidelines on the Management of Cyber Risk* (GMCR) on the date on which these Guidelines come into effect. Any reference to the GMCR in any other guidelines or handbooks issued by the SC shall be substituted with these Guidelines instead.

3.02 Subject to paragraph 3.01, these Guidelines are in addition to and not in derogation of any requirements as provided for under securities laws or any other guidelines issued by the SC.

3.03 Capital market entities that are jointly regulated by other regulators are required to comply with all relevant guidelines and requirements. Where there are differing requirements, the more stringent requirements shall apply.

3.04 For avoidance of doubt, compliance with these Guidelines does not relieve a capital market entity from other obligations which may be imposed on the capital market entity under any other written law or by any other relevant regulator.

Chapter 4

DEFINITIONS

4.01 Unless otherwise defined, all words used in these Guidelines shall have the same meaning as defined in the CMSA. In these Guidelines, unless the context otherwise requires:

board	means the board of directors of a capital market entity including a board committee;
business impact analysis or BIA	means the process of assessing the impact of operational disruptions on a critical business function of a capital market entity, and identifying the critical business functions or operations and resources that are necessary to be prioritised in the recovery strategies of a capital market entity;
capital market entity	means—

(a) an exchange holding company, stock exchange, derivatives exchange, clearing house and trade repository approved under the CMSA, and a central depository approved under the *Securities Industry (Central Depositories) Act 1991*;

(b) a self-regulatory organization recognized under the CMSA;

(c) a private retirement scheme administrator approved under the CMSA;

(d) a Capital Markets Services License holder;

(e) a recognized market operator registered under the CMSA;

(f) a registered person provided in Part 2 of Schedule 4 of the CMSA; and

(g) a person providing capital market services registered under section 76A of the CMSA;

critical	means a core component, failure or absence of which would have significant impact to the capital market entity's business operations, clients, reputation or compliance with applicable laws and regulatory requirements;
cyber incident	means an observable occurrence indicating an actual breach in the information assets, IT systems, network and operating environment of a capital market entity;
cyber resilience	means the ability to anticipate, absorb, adapt to, rapidly respond to, and recover from disruption caused by a cyber attack;
cyber risk	means the risk of cyber threats occurring within the realm of the information assets, IT systems, network and operating environment of a capital market entity;
cyber threat	means a circumstance or incident with the potential to exploit one or more vulnerabilities intentionally or unintentionally in the information assets, IT systems, network and operating environment of a capital market entity;
data sanitisation	means the process by which data is irreversibly removed from the device or is permanently destroyed;
detection	means the development and implementation of the appropriate activities to identify the occurrence or potential occurrence of a cyber incident or technology incident;
EOL (end of life)	means the end of the lifecycle of a product which prevents users from getting updates, and indicates that the product has reached its useful lifespan;
EOS (end of support)	means the end of the provision of support for a product by a provider except for limited technology support and parts availability which would still be provided until it depletes;

information assets	means information or data that is of value to the capital market entity, including such information as company records, intellectual property, client information, networks, hardware, software, device, or other component of the environment that supports information-related activities and are not limited to those that are owned by the capital market entity;
IT	means information technology;
IT systems	means the set of hardware, software and facilities that integrate the information assets of a capital market entity, specifically the equipment (including servers, routers, switches and cabling), software, services and products used in storing, processing, transmitting and displaying all forms of information for the usage of the capital market entity;
malware	means malicious software used to disrupt the normal operation of an IT system in a manner that adversely impacts its confidentiality, integrity or availability;
near miss event	means an event that has a high potential to become— (a) a technology incident that may potentially affect its business operations or clients; or (b) a cyber incident, but was detected and mitigated before any substantial impact occurred;
production environment	means the live environment where software, hardware, data, processes, and programs are made available to users, as opposed to any testing, training, and other non-production, non-live environments;
recovery	means restoration of any capabilities or services that have been impaired due to a technology incident or cyber incident;

recovery time objective	means the targeted duration of time for which an information system and network must be recovered after a cyber incident or technology incident;
risk appetite	means the amount of different types of risk a capital market entity is willing to accept to achieve its objectives;
risk tolerance	means the level of risk a capital market entity is willing to take on in terms of individual risk;
system	means any application, incorporating both hardware and software in various configurations, that supports the business, operations and provision of services of a capital market entity;
technology incident	means an unexpected event or issue that disrupts the normal functioning of a technology system, application, or service. Technology incidents may be caused by a variety of factors, including hardware or software failures, human errors, natural disasters, and other external events;
third-party service provider	means an internal group affiliate or an external entity to which the capital market entity has outsourced any of its technology-related functions or services, and include any subsequent service provider(s) to whom the initial service provider has further contracted the outsourced functions; and
TRM Framework	means the framework which include technology risk management, technology operations management, technology service provider management, cyber security management and principles relating to the adoption of AI and ML, wherever applicable.

PART B: TECHNOLOGY RISK MANAGEMENT FRAMEWORK

Chapter 5

GOVERNANCE

Board of Directors

5.01 The board must provide oversight and accord sufficient priority and resources to manage technology risk, as part of the overall risk management framework of a capital market entity.

5.02 In discharging its oversight functions, the board must—

(a) approve the TRM Framework of a capital market entity and its policies;

(b) approve the risk appetite and risk tolerance statement which provides clarity as to the nature and degree of technology risk within the risk acceptance of the capital market entity;

(c) ensure that the TRM Framework and policies are robust and sound, and commensurate with the risk exposure of the capital market entity so that it may assist the capital market entity in achieving security, reliability and resilience of its IT operating environment;

(d) in discharging its obligation in paragraph (c) above, the board must—

(i) oversee the effective implementation of the TRM Framework and policies and procedures. This may include setting performance metrics or indicators as appropriate;

(ii) ensure that the TRM Framework is regularly reviewed and updated by the senior management for the approval of the board at least once in every three years;

(iii) ensure that the policies are regularly reviewed and updated by the senior management for the approval of the board at least annually; and

(e) ensure that the strategies formulated within the TRM Framework are adequately designed to address the technology risk that the capital market entity may be exposed to;

(f) ensure appropriate internal controls are in place for the effective implementation of the TRM Framework;

(g) ensure the impact of technology risk is adequately assessed prior to the capital market entity undertaking new activities, which may include any proposed investments, merger and acquisition, adoption of new technology and outsourcing arrangements;

(h) ensure adequate resources are allocated for technology risk management, including identifying at least one responsible person from among the senior management:

(i) who would be responsible for the day-to-day oversight and management of technology risk; and

(ii) who would be responsible for the implementation of the technology and cyber security strategy as determined by the board;

(i) ensure clear segregated line of responsibilities and accountability across all levels and functions in the capital market entity to manage technology risk; and

(j) ensure that the board keeps itself up to date with new or emerging trends of technology risk including cyber threats and understand the potential impact of such threats to the capital market entity.

5.03 The board must perform its oversight role over the IT outsourcing arrangements and is accountable for ensuring the effectiveness of the outsourcing policies and procedures of the capital market entity.

Senior Management

5.04 The senior management is responsible for–

(a) developing and implementing the TRM Framework and policies which are robust and sound, and commensurate with the level of risk exposure of the capital market entity so that it may assist the capital market entity in achieving security, reliability and resilience of its IT operating environment;

(b) approving and implementing technology risk management procedures which are robust and sound, and commensurate with the risk exposure of the capital market entity so that it may assist the capital market entity in achieving security, reliability and resilience of its IT operating environment;

(c) ensuring that technology risk management procedures are regularly reviewed and updated for its approval at least annually;

(d) formulating, for the approval of the board, segregated line of responsibilities and accountability across all levels and functions in the capital market entity and implementing the same as approved by the board;

(e) ensuring that employees, agents and third-party service providers are aware and understand the TRM Framework and policies and procedures, the possible impact of various cyber threats and their respective roles in managing such threats;

(f) recommending to the board appropriate strategies and measures to manage technology risk, including making necessary changes to existing policies and procedures, as appropriate;

(g) reporting to the board on a regular basis on matters relating to key technology risk, cyber breaches, business impact analysis (BIA) and critical technology operations;

(h) providing the board with regular updates on cyber security issues, cyber security risk and compliance with cyber security framework;

(i) reviewing, tracking and reporting material deviations from the TRM Framework, and policies and procedures to the board;

(j) keeping the board informed of new and potentially emerging technology risk that may be critical to the capital market entity risk appetite; and

(k) implementing the remedial actions approved by the board in an effective and timely manner.

Cybersecurity Awareness and Training

5.05 A capital market entity must ensure that its board, senior management, employees and agents, if any, attend cybersecurity awareness training programme at least annually to enhance their awareness and preparedness to deal with a wide range of cyber risk and to carry out their respective roles effectively.

Technology Audit

5.06 A capital market entity must—

(a) establish a technology audit plan that provides appropriate coverage of critical technology; and

(b) carry out its technology audit regularly. The frequency of the technology audit should commensurate with the business model, risk appetite and level of technology dependency of the capital market entity.

5.07 At the minimum, the technology audit carried out by a capital market entity must determine whether its—

(a) information systems are in compliance with applicable laws, regulatory requirements and industry guidelines;

(b) data and information have appropriate level of confidentiality, integrity and availability; and

(c) IT service operations are being managed efficiently, and its effectiveness targets are being met.

5.08 A capital market entity must ensure that the auditors performing its audit possess the necessary competency, knowledge and experience to carry out the technology audit.

5.09 A capital market entity must—

(a) ensure that the technology audit report comprises, at a minimum, independent and objective opinion on the effectiveness of risk management, governance and internal controls of the capital market entity relative to its existing and emerging technology risk; and

(b) report the outcome of its technology audit to the board.

5.10 Where necessary, the SC may appoint any independent party to perform a review on the capital market entity's compliance with these Guidelines including a technology audit and any costs of carrying out such review shall be borne by the capital market entity.

Chapter 6

TECHNOLOGY RISK MANAGEMENT

6.01 A capital market entity must establish and implement robust and effective TRM Framework to manage its technology risk effectively. The TRM Framework must be reviewed and updated periodically, and in any event, at least once in every three years by the capital market entity.

6.02 A capital market entity must establish and implement comprehensive and effective policies and procedures to support the TRM Framework. The policies and procedures must be reviewed and updated at least annually by the capital market entity.

6.03 A capital market entity must establish an internal compliance process to ensure compliance with its TRM Framework, policies and procedures. The internal compliance process must include an appropriate approval process where—

(a) the approval of senior management must be obtained prior to any deviation from its TRM Framework, policies and procedures of the capital market entity; and

(b) the approval for deviation must only be given by the senior management if the deviation is supported by—

(i) an appropriate justification; and

(ii) alternative solution or a reasonable timeframe to comply with its TRM Framework, policies and procedures.

6.04 A capital market entity must establish and implement its technology risk management framework comprising risk identification, risk assessment, risk mitigation, and risk monitoring, review and reporting on any existing and emerging technology adopted by the capital market entity. A capital market entity may refer to **Appendix 1** for guidance with regards to these components of the technology risk management framework.

6.05 A capital market entity must ensure that—

(a) all risks are assigned to the appropriate risk owners who shall be accountable for ensuring that proper risk treatment plans are implemented and enforced for a specific technology risk;

(b) the risk owners establish appropriate, effective and efficient technical and organisational measures in all steps of the process; and

(c) any residual risk arising from threats and vulnerabilities after risk treatment, shall be documented and managed by risk owners according to the defined risk acceptance criteria that commensurate with the capital market entity's risk tolerance level.

6.06 A capital market entity must maintain a board-approved key technology risk register to facilitate the monitoring and reporting of technology risk.

6.07 A capital market entity must continuously review its risk exposures and associated controls to ensure that they remain in line with the risk appetite of the capital market entity.

Chapter 7

TECHNOLOGY OPERATIONS MANAGEMENT

Technology Project Management

7.01 A capital market entity must establish and implement clear and comprehensive internal guidelines on technology project management so that any technology and technology-related project can be completed with clarity, alignment, traceability, and effective resource utilisation.

7.02 A capital market entity must conduct a post implementation review (PIR) on all critical technology and technology-related projects, and the findings of the PIR should be taken into account to improve project management.

7.03 A capital market entity must conduct risk assessment to identify, manage and monitor risks arising from the implementation of critical technology-related projects and throughout the project life cycle as project risk may adversely impact the project delivery timeline, budget, and quality of the project deliverables.

7.04 Where a capital market entity carries out a technology-related project, the capital market entity must ensure there are adequate personnel, including key stakeholders to oversee and manage such projects, including serving as project coordinator and advisor and being responsible for all deliverables, project costs and schedules.

System Acquisition and Development, System Testing and Acceptance and Access Control Management

7.05 A capital market entity must establish and implement internal processes encompassing—

(a) system acquisition and development;

(b) system testing and acceptance; and

(c) access control management.

<u>System Acquisition and Development</u>

7.06 A capital market entity must establish and implement clear requirements and processes to manage its system development life cycle (SDLC) encompassing planning, requirement analysis, design, implementation, testing and acceptance. It must include, among others, requirements and processes for—

(a) vendor selection and evaluation of the systems to be procured from all vendors or solution providers; and

(b) assessment of software development by vendors and in-house developer, to ensure that security of the capital market entity is not compromised, and its quality assurance is met.

7.07 Where feasible, a capital market entity should enter into a source code escrow agreement to ensure the source codes for critical systems are accessible. If an escrow agreement cannot be implemented, a capital market entity must identify an appropriate alternative.

7.08 A capital market entity must—

(a) incorporate security requirements into the system design which would enable it to carry out constant security evaluation; and

(b) comply with security practices throughout the SDLC in order to minimise system vulnerabilities and reduce risk exposure.

7.09 At the minimum, the security requirements must cover main control areas including access control, authorisation, data integrity and confidentiality, logging system activity, tracking security event and exception handling.

System Testing and Acceptance

7.10 A capital market entity must establish a methodology for rigorous system testing and ensure that adequate testing is performed prior to deployment of a system so that the system meets its user requirements and performs as intended. At the minimum, the testing conducted must cover the business logic, function, controls and performance of the system under various load and stress conditions.

7.11 Where feasible, a capital market entity should use automated testing methodology to ensure comprehensiveness of the testing scopes, as part of the testing strategy.

7.12 A capital market entity must properly document, track and address the issues identified during testing, including vulnerabilities, deficiencies, system defects or software bugs.

7.13 A capital market entity must ensure that all issues which could have an adverse impact on the operations of the capital market entity or delivery of its services to its clients are reported to the senior management and rectified prior to deployment of the system to the production environment of the capital market entity.

7.13A Prior to deployment of a system, a capital market entity must carry out a cyber security assessment that commensurate with the risk exposure of the capital market entity.

7.14 To ensure that the system is production ready and satisfies all documented requirements, a capital market entity must perform—

(a) final acceptance testing including quality assurance testing focusing on technical aspect of the system; and

(b) user acceptance testing focusing on functional aspect of the system.

7.15 The results of the final acceptance testing and user acceptance testing must be reported to senior management.

7.16 In the case of an acquired system, after attending to the changes during testing by a vendor, a capital market entity must ensure that the final approved version of the acquired system is used for implementation.

Access Control Management

7.17 To minimise risk of unauthorised access to information assets, a capital market entity must—

(a) establish user access management policies and procedures for providing, modifying and revoking access rights to IT systems. Access rights and privileges shall be granted in accordance with the roles and responsibilities of the users, and the access matrix should be periodically reviewed;

(b) enforce and review its password controls periodically to enhance the resilience of its system against any attack; and

(c) ensure that the logging facility is enabled to capture system user login, system activities, privilege accounts and service accounts for the purpose of audit and investigation. A capital market entity is also expected to review logs on a regular basis for any irregularity.

7.18 A capital market entity must use strong fraud deterrents for sensitive system functions to safeguard the systems and data from unauthorised access on a best effort basis. For example, the use of multi-factor authentication (MFA) and privilege access management to secure employee and customer authentication process.

Cryptography

7.19 A capital market entity must implement suitable and effective cryptographic controls to safeguard the confidentiality, authenticity and integrity of its sensitive data from unauthorised access and unintentional disclosure.

7.20 A capital market entity must establish robust and sound policies and procedures to manage the use of cryptography including:

(a) cryptographic key life cycle management from generation to disposal;

(b) measures to protect the cryptographic key from use by unauthorised parties;

(c) measures to protect the cryptographic key from being modified, compromised or destroyed during its lifetime; and

(d) procedures to ensure the cryptographic key is available to authorised parties only when needed with appropriate authentication and control mechanisms.

Data Security and Privacy

7.21 As part of its technology risk management, a capital market entity must implement effective measures to prevent losses arising from data breach or other acts of internal or external threats, negligence and cyber attack.

7.22 The measures must cover the process of identification, handling, transmission, movement, destruction and availability of data based on the following—

(a) maintain a comprehensive and updated inventory of all information assets including data classification and risk across the capital market entity;

(b) deploy adequate security measures to safeguard IT systems residing in the production environment, non-production environment and all other media;

(c) implement appropriate controls to ensure no unauthorised person is able to access data and IT systems. Access to data and IT systems should be on a need-to-have basis;

(d) implement clear desk policy to ensure information assets are not left unprotected which could potentially lead to security breaches;

(e) review audit logs or trails particularly on access to critical data to identify anomalies or abnormal activities;

(f) enhance monitoring and assurance activity over third parties to ensure data and information assets of the capital market entity are adequately protected;

(g) conduct a periodic gap analysis at least once a year on data and information assets processes and controls to improve data security;

(h) establish a remediation plan to prioritise rectification according to the capital market entity's risk assessment; and

(i) develop, operate, manage and test the data breach management processes which should include the process for preparation, identification, containment, eradication, recovery and lesson learned from data breaches.

7.23 A capital market entity must establish appropriate data security measures to protect the confidentiality, integrity and availability of its critical data and this should include data stored in cloud or where blockchain-based application is used.

7.24 A capital market entity must establish and implement data loss prevention (DLP) policy and procedures to safeguard:

(a) Data in-use – data being accessed and processed by a system.

(b) Data in-motion – data being transferred over the network.

(c) Data at-rest – data stored in mediums such as servers, backup media, storage platform and databases.

Data Storage

7.25 A capital market entity must ensure its data and IT systems are stored or hosted in an environment that is secure, robust and resilient. It must also observe a similar approach for cloud storage.

7.26 A capital market entity must undertake a storage capacity assessment periodically to determine its current and future storage capacity and utilisation. If the results of the assessment warrants for a migration, a capital market entity must develop and execute a plan to migrate its data and IT systems into a new environment.

7.27 A capital market entity must determine the appropriate retention period to archive its data based on the usage requirement or its criticality for its data.

7.28 A capital market entity must ensure data is protected by an adequate backup schedule and perform regular testing according to the needs of the capital market entity and ensure data can be restored from backups.

Data Disposal

7.29 A capital market entity must establish and implement appropriate policies for the disposal of data on its IT systems, mobile devices and storage media to safeguard the data from unauthorised disclosure.

7.30 A capital market entity must dispose the data kept in its IT systems when it is no longer required for business usage, legal or contractual purposes for which it was originally created or held.

7.31 Where a capital market entity has decided that data kept in its IT devices, such as Bring-Your-Own-Device (BYOD) or corporate mobile devices, is to be disposed, the capital market entity must ensure its data will be deleted from those devices after such data is no longer in use.

7.32 A capital market entity must implement a clear data sanitisation procedure to ensure data is irretrievably destroyed from its IT systems and IT devices. The data sanitisation procedure of a capital market entity must include—

(a) record data sanitisation activities performed such as location of the IT systems and IT devices, sanitisation date and name of responsible individual(s); and

(b) clear identification of data accessible by a third party and access controls to address the risk of third-party having access to data that is not appropriately disposed.

7.33 A capital market entity must require all third parties who have the data of the capital market entity in its custody to perform data sanitisation appropriately and securely to avoid the risk that the data that is no longer in use to be accessible by a third party. A capital market entity should include such requirements in any contract entered into with a third-party service provider.

Change Management

7.34 A capital market entity must establish a change management process to oversee any changes made to its IT systems covering among others, impact assessment, approval, scheduling, implementation and communication to key stakeholders.

7.35 A capital market entity must ensure, prior to deploying any changes to its IT systems in the production environment—

(a) a risk and impact analysis is conducted on all proposed changes to the IT systems. This risk and impact analysis should be included in the test plans of the capital market entity;

(b) the analysis takes into account security factor and implication of the change in relation to the capital market entity's other IT systems;

(c) the results of the analysis are accepted and approved by senior management;

(d) all key stakeholders (comprising the relevant business groups in the capital market entity that will be affected by the proposed change) are informed and provided with recommendations on the proposed change; and

(e) the IT systems configuration is backed up and a fall-back plan is prepared in case a problem arises during or after the implementation of a change.

7.36 A capital market entity must establish and implement clear process and procedures to handle any emergency change to the production environment.

7.37 A capital market entity must record activities performed during the change process in an activity log to facilitate investigation and troubleshooting.

Patch and Technology Obsolescence

7.38 A capital market entity must establish a patch management process to administer the remediation effort, risk assessment, monitoring and implementation of security patch that is applicable to its IT systems. A capital market entity must perform patch management diligently and continuously monitor and implement the latest patch releases in a timely manner.

7.39 A capital market entity must closely monitor the EOS dates of its hardware and software including those relating to security vulnerabilities that surface after the EOS date.

7.40 A capital market entity must develop a technology refresh plan for the replacement of its hardware and software before they reach EOS. A capital market entity must assess the impact and include risk mitigation process should the EOS system be utilised within a certain period.

7.41 A capital market entity must ensure that its critical IT systems are not running on obsolescence systems or EOL systems. If there is a need for a capital market entity to continue using critical technology which are running on obsolescence systems, it must—

(a) ensure that approval is obtained from senior management and a validity period is assigned to the continued use of such critical IT systems that commensurate with the identified risks and risk mitigation process of the capital market entity; and

(b) closely monitor, assess the impact and establish a risk mitigation process that corresponds to its risk acceptance level for such critical IT systems.

7.42 The capital market entity must ensure that the latest inventory list of all IT systems is mapped to its criticality and is available for patch administration for the purpose of determining its patches severity and for further remedial action.

7.43 A capital market entity must conduct patch compatibility testing on its IT systems that use standardised configurations before deploying to its IT systems in production environment to ensure it does not introduce any adverse effect. The patch deployment must be carried out within a specified timeframe depending on the severity level of the patch.

7.44 The capital market entity must ensure the remediation action is approved, monitored and tracked according to the change management process.

Network Resilience

7.45 A capital market entity must design a sound network architecture to support its business activities and future growth and to enable it to achieve high network availability, redundancy, accessibility and resiliency.

7.46 A capital market entity must continuously assess its network architecture design to identify any flaws and to sustain an acceptable level of availability which may support the business activities of the capital market entity.

7.47 A capital market entity must ensure its network infrastructure with systems that demand high availability and reliability to have no single point of failure by implementing redundancy, fault tolerance, congestion control and diversity in network routing, where applicable.

7.48 A capital market entity must ensure that the change management process provided in paragraph 7.34 is applicable to any changes made to the network infrastructure.

Operational Resilience

7.49 A capital market entity must ensure that its data centre operation, including the use of cloud services, is supported by a sound IT infrastructure taking into consideration IT operational resiliency and availability target that is aligned to the business needs of the capital market entity. The availability target set by the capital market entity should result in reducing the impact of any failure or disruption to the data centre operations of the capital market entity.

7.50 Where applicable, to reduce the impact of any failure or disruption to the data centre operations, a capital market entity must—

(a) conduct a data centre risk assessment to ensure the resiliency of the data centre, taking into consideration the business model and risk appetite of the capital market entity, and industry best practices;

(b) ensure no single point of failure (SPOF) to its critical IT infrastructure including power equipment, network connectivity, cooling equipment, electrical utility and diversification of data communication and network paths attending the IT system;

(c) maintain a secondary data centre for recovery purposes based on the business needs of the capital market entity;

(d) undertake a data storage capacity assessment to determine its current and future storage capacity and utilisation;

(e) ensure adequate maintenance of the data centres;

(f) continuously monitor the data centre resources according to internal thresholds determined by the capital market entity to ensure the performance of the data centre resources are not disrupted;

(g) implement an escalation process and response plan to analyse and remediate any potential or actual threats related to the data centres; and

(h) implement adequate physical access controls for its data centres including process on authorised employees, visitor access and access to selected areas.

7.51 Where a third-party service provider manages the data centre, the capital market entity must ensure that the third-party service provider furnishes a data centre risk assessment report upon request by the capital market entity or the SC. The report must cover the review of the system of the data centre, suitability of its design of controls and effectiveness of the controls. The capital market entity must perform its own risk assessment of such report to ensure it is consistent with the risk appetite and risk tolerance of the capital market entity.

7.52 A capital market entity must ensure that its IT system has adequate storage, central processing unit power, memory and network bandwidth to support its business operations and future growth.

7.53 A capital market entity must monitor its technology operation status including its network performance, application and system utilisation to ensure its IT resources meet its current needs and future growth, and for capacity management planning.

7.54 A capital market entity must establish a monitoring and reporting mechanism of its network, application and system to flag abnormal behaviour and aid in analysis. Upon

the detection of any abnormal behaviour, the capital market entity must undertake a follow-up action in accordance with its internal procedures.

7.55 A capital market entity must retain adequate network, application and system device logs for investigation and diagnosis for an appropriate period as it determines.

IT Disaster Recovery Plan (IT DRP)

7.56 A capital market entity must establish and test its IT DRP on a regular basis to manage availability and restore IT system within the recovery time objectives being set in the event of disruption according to its defined BIA.

7.57 A capital market entity must ensure that all relevant key stakeholders from business and IT functions participate in the IT DRP to ensure the IT DRP is implemented effectively.

7.58 A capital market entity must ensure that the IT DRP consists of–

(a) procedures for declaring a disaster with escalation procedures;

(b) criteria for plan activation (including circumstances in which a disaster is declared, type of scenarios of disasters and when the recovery plan should be put into action);

(c) its linkage with overarching plans such as emergency response plan or crisis management plan for business continuity plan (BCP) for different lines of business;

(d) the responsible employee for each function in plan execution;

(e) recovery teams and their responsibilities;

(f) emergency contact and notification (recovery teams, recovery manager, stakeholders, important third-party service providers);

(g) a detail procedure of the recovery process (initiation of recovery place, type of recovery to be conducted, the flow of recovery);

(h) identification of the various resources required for recovery and business operation continuation; and

(i) post incident review incorporating lessons learned and developing long-term risk mitigations.

7.59 Where IT systems are managed by a third-party service provider, the capital market entity must ensure that the third-party service provider is capable in ensuring availability and recovery of the IT systems. The capital market entity must coordinate the DRP with involvement from the third-party service provider for such IT systems to meet the business recovery objectives.

Chapter 8

TECHNOLOGY SERVICE PROVIDER MANAGEMENT

8.01 A capital market entity must implement and uphold robust and sound risk management in relation to its outsourced arrangements including any sub-arrangements.

Due Diligence and Performance Monitoring

8.02 A capital market entity must ensure that—

(a) the third-party service providers it engages are reliable by conducting due diligence prior to selecting a third-party service provider; and

(b) it carries out contract management and performance monitoring so as to minimise any risks related to the technology it expects to adopt from the third-party service provider.

8.03 The scope of the due diligence to be conducted by a capital market entity pursuant to paragraph 8.02 above must include the following:

(a) financial stability and reputation of the third-party service provider;

(b) where applicable, the managerial skills, technical competency and operational capability of the third-party service provider; and

(c) the third-party service provider's capacity to undertake the provision of the outsourced task effectively at all times.

8.04 A capital market entity must conduct periodic assessment on the capabilities of the third-party service providers during the contract period, including the third-party service provider's capability in managing risk. In assessing the capabilities of the third-party service provider in managing risk, a capital market entity must also consider the following factors:

(a) Data loss;

(b) Technology risk;

(c) Reputational risk;

(d) Exit risk;

(e) Concentration risk;

(f) Operational risk including resiliency to operational and system disruption, disaster preparedness plan and business continuity plan (BCP);

(g) Data security of the capital market entity and its clients' data integrity including unauthorised access and mishandling of data and information during data-at-rest, data-in-motion and data-in-use; and

(h) Resiliency to cyber risk.

8.05 A capital market entity must ensure that the selected third-party service provider practices cyber hygiene and remains cognisant in protecting its data confidentiality, and the integrity and resilience of its systems.

8.06 Notwithstanding that the operation or maintenance of IT systems are outsourced to a third-party service provider, a capital market entity remains responsible for ensuring compliance with the requirements set out in these Guidelines.

Cloud Services

8.07 A capital market entity must ensure the level of governance and controls implemented over cloud service providers including cloud strategy and cloud operational management commensurate with the risks posed by the cloud services it adopts. The board of the capital market entity should be responsible and accountable for maintaining effective oversight and governance in this regard.

8.08 A capital market entity must be cognisant of and ensure risks associated with the use of cloud services are adequately addressed. It must perform a comprehensive risk assessment when planning for cloud adoption and manage the risks identified appropriately.

8.09 A capital market entity must, prior to cloud adoption, conduct a comprehensive risk assessment which addresses key risks associated with among others, the following:

(a) Cloud risk management strategy, considering different cloud service models tailored to their needs;

(b) Location of the cloud infrastructure;

(c) Multi-tenancy or data commingling;

(d) Identity and access management (IAM) controls, data protection and cryptographic key management;

(e) Expansion of cyber security operations of the capital market entity including the security of public cloud infrastructure;

(f) Cloud resilience risk management such as cloud redundancy or fault tolerant capability, high availability, scalability, multiple geographically separated data centres;

(g) Vendor lock-in and portability or interoperability solutions;

(h) Exposure to cyber-attacks via cloud service providers;

(i) Migration of existing systems to cloud infrastructures; and

(j) Constant ability to meet regulatory requirements and timely measures of security standards on cloud computing.

8.10 A capital market entity must assess and manage its exposure to technology risk that may affect the confidentiality, integrity and availability of the IT systems and data at the cloud during the contractual period of the cloud services agreement.

8.11 A capital market entity must ensure adequate measures are undertaken by the cloud service provider to safeguard the data of the capital market entity and the data of its clients against unauthorised disclosure and access. For encrypted data, a capital market entity must ensure that appropriate cryptographic key management is established, including assessing the ability of the cloud service provider to restore the services effectively.

Contract Management

8.12 A capital market entity must establish a service level agreement when engaging third-party service providers.

8.13 The service level agreement entered by a capital market entity with its third-party service provider must at a minimum include provisions on—

(a) scope of arrangement, duration of the service and performance metrics;

(b) confidentiality and security requirements of the capital market entity and the data of its clients during and after the end of the contract period;

(c) access rights to information or documents of the third-party service provider related to any outsourced function as may be required by the SC or the capital market entity for the purpose of performing review or audit on the relevant systems;

(d) the right for the SC to appoint an independent party to perform a review or audit of the relevant information or document of the capital market entities

stored with or held by the third-party service provider and the costs for such review or audit shall be borne by the capital market entity;

(e) contingency plans and exit strategies with minimal impact on the continuity of the operations of the capital market entity;

(f) system development and maintenance arrangements with the third-party service provider including requirements for such third-party service provider to comply with the data and information security policies of the capital market entity;

(g) a clearly defined arrangement for immediate notification by the third-party service provider to the capital market entity in the event of a technology incident or cyber incident;

(h) clearly defined cyber security responsibilities of all parties;

(i) modification or termination of the arrangement between the capital market entity and the third-party service provider in the event the SC issues a direction to the entity to that effect under securities laws, these Guidelines or any other relevant guidelines, guidance or practice notes; and

(j) compliance with applicable laws, regulations, guidelines and requirements by the third-party service provider.

8.14 A capital market entity must—

(a) periodically review the performance of its third-party service providers to ensure satisfactory performance is achieved and review the service level agreement it enters into to ensure it remains relevant and effective; and

(b) ensure its third-party service providers comply with all applicable laws, regulations, guidelines and requirements.

8.15 A capital market entity must ensure that all of its data residing with third-party service providers are recoverable in a timely manner.

Chapter 9

CYBER SECURITY MANAGEMENT

Cyber Security Framework

9.01 A capital market entity must—

(a) develop a cyber security framework comprising the governance and implementation of adequate cyber security controls which commensurate with the risk appetite and business profile of the capital market entity; and

(b) ensure that the cyber security framework is supported by policies and procedures to address interoperability, usability, and privacy of the data of the capital market entity and its clients within its custody, and to safeguard the confidentiality, integrity and availability of the data.

9.02 A capital market entity must ensure that roles and responsibilities are defined to ensure accountability for cyber security activities within the capital market entity.

9.03 As part of a wider risk management programme, a capital market entity must implement cyber risk management strategies and measures in a structured and methodical manner which includes identification, protection and prevention, detection, response and recovery measures. The capital market entity may refer to **Appendix 2** for guidance on the methodology in implementing its cyber risk management strategies and measures.

Cyber Security Measures and Monitoring

9.04 A capital market entity must deploy defence-in-depth and preventive cyber security measures which commensurate with its business model, risk appetite and level of technology dependency. A capital market entity must put in place the appropriate measures which may include the following:

(a) Deployment of anti-virus software and malware programme to detect and isolate malicious code;

(b) Layering systems and systems components;

(c) Deployment of firewalls to reduce weak points through which attacker can gain access to an entity's network;

(d) Web and email filtering systems; and

(e) Solution to counter advance persistent threats such as zero day and signatureless-malware.

9.05 A capital market entity must—

(a) establish, implement and continuously review the security hardening standards on its operating systems, databases, applications, network and security devices; and

(b) ensure that the security hardening standards checklist is kept updated.

9.06 A capital market entity must conduct continuous review and update of rules and configurations for its operating systems, databases, applications, network and security devices.

9.07 A capital market entity must establish—

(a) on a best effort basis, a security operation centre (SOC) or engage a managed security services (MSS) provider that has sufficient capabilities for pre-emptive surveillance and monitoring of its cyber events. The SOC implemented must be secured with proper access controls, skilled resources, and accommodated with disaster recovery capabilities and dashboard to oversee the overall network perimeter of the capital market entity;

(b) a process to collect, review and retain system logs to facilitate the cyber events monitoring operations of the capital market entity while ensuring the system log remains protected; and

(c) a baseline indicator for each of the IT systems being monitored. Any anomalies or suspicious user behaviour detected against the baseline indicator must be analysed and escalated in a timely manner in accordance with the escalation and decision-making processes of the capital market entity.

9.08 A capital market entity must establish a monitoring and detection process to support continuous surveillance of any cyber event, which should include, among others, clearly defined escalation and decision-making processes to ensure any adverse effect of a cyber incident is properly managed;

9.09 A capital market entity must proactively monitor any cyber event, detect any anomalous activity and conduct analysis on any detected event that may have material impact on the business or systems of the capital market entity.

9.10 Where feasible, a capital market entity should use its best endeavours to conduct regular monitoring of fake websites to minimise adverse effect on its customers, employees and agents from phishing or other types of social engineering attacks.

9.11 A capital market entity must perform correlation of multiple events registered on system logs to identify anomalous system activity or suspicious user behaviour patterns according to the baseline indicator.

9.12 If reasonably practicable, a capital market entity must apply advanced user behavioural analysis to detect sophisticated cyber events such as signature-less and file-less malware, as well as to identify anomalies at endpoints and network layers.

9.13 A capital market entity must regularly review its cyber threat analysis report that commensurate with its business model, risk appetite and technology dependency. The cyber threat analysis report must be communicated to its senior management. At the minimum, the report must encompass the cyber threat trends and statistics, incidents grouping by type of attack, target and source of IP addresses.

9.14 A capital market entity must equip itself with the knowledge and understanding of the current and evolving cyber threats, new cyber attack techniques, analyse and determine the appropriate countermeasures.

Cyber Security Incident Response and Recovery

9.15 A capital market entity must establish a cyber incident response capability to manage and minimise damage from cyber incidents, and to recover and learn from such incidents. The cyber incident response capability must encompass the following phases:

(a) Preparation

A capital market entity must establish an effective governance process, reporting structure and a team to manage cyber incident and response plan in the event of a cyber incident that cause service disruption. A capital market entity must also clearly define the roles and responsibilities of the team.

(b) Detection and Analysis

A capital market entity must establish a detection process to handle detected cyber events, including disaster declaration and classification of the cyber incident based on the attack vectors. Different types of cyber incidents merit different response strategies.

(c) Containment, Eradication and Recovery

A capital market entity must establish a recovery process to mitigate any service disruption due to cyber-attack by prioritising the recovery based on the criticality of the systems and services within a capital market entity operating environment and to restore IT systems to its normal operation.

(d) Post Incident Review

A capital market entity must ensure that the recovery process carried out by the capital market entity event is well documented to support an effective post incident review. A report must be produced from the post incident review and presented to all relevant stakeholders.

9.16 A capital market entity must establish clearly defined communication plan including escalation and decision-making processes to ensure that any adverse effect of a cyber incident is properly managed and recovery action may be initiated quickly.

9.17 For the purposes stated in paragraph 9.15(c), a capital market entity must identify the critical systems and services within its operating environment that shall be recovered on a priority basis in order to provide an acceptable level of services during the downtime.

9.18 A capital market entity must determine the recovery time objective to return to its full service and operations.

9.19 A capital market entity must regularly review and update the cyber incident management plan taking into account the information gathered from reputable cyber threat intelligence and lesson learned from cyber incidents.

Cyber Security Assessment

9.20 A capital market entity must establish a process to conduct regular assessment, and to identify potential vulnerabilities and cyber threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks. The process must, among others, outline the relevant control measures to mitigate any vulnerabilities and cyber threats in its operating environment.

9.21 A capital market entity must ensure its assessment is comprehensive, which comprise among others making an assessment of potential vulnerabilities relating to systems and technologies adopted including any third-party systems utilised by the capital market entity and business processes.

9.22 Where feasible, a capital market entity should regularly undertake a compromise assessment (CA) on its critical systems to prevent and detect any potential compromise of its security posture.

9.23 A capital market entity must conduct regular penetration testing exercise to imitate an experienced hacker attacking the production environment of the capital market entity, with the aim to obtain in-depth evaluation of its cyber defences. The scope and frequency of the exercise must commensurate with the capital market entity's risk exposure and should at a minimum be conducted annually.

9.23A Penetration testing must also be conducted prior to the deployment of any new critical system or any major changes to the critical systems of a capital market entity.

9.24 A capital market entity must ensure the penetration testing exercise process is documented and performed by experienced and qualified professionals who are aware of the risk of undertaking such exercise and are able to limit the damage resulting from a successful break-in to a production environment. A capital market entity must obtain the approval of its senior management before finalisation of the test scope.

9.25 A capital market entity must establish a comprehensive remedial process to track, monitor and resolve vulnerabilities identified from the cyber security assessments. The remedial process must include at a minimum:

(a) severity level and classification of identified vulnerabilities;

(b) turnaround time to remediate vulnerabilities according to its severity level; and

(c) risk assessment and mitigation plans to manage exceptions (i.e. for vulnerabilities which the capital market entity is unable to remediate timely) with approval from senior management.

Cyber Simulation Exercise

9.26 A capital market entity must carry out a cyber simulation exercise which commensurate with the level of risk appetite of the capital market entity and its reliance on technology to test the effectiveness of its cyber incident response and recovery, including its communication plan based on current and emerging cyber threat scenarios. A capital market entity must determine the objectives, scope and conditions of engagement for the cyber simulation exercise before the initiation of the exercise. It must ensure the simulation exercise is conducted with involvement from key stakeholders.

9.27 To ensure the capital market entity is prepared to respond to cyber incidents detected, at a minimum, the capital market entity must—

(a) identify scenarios of cyber risk that it is most likely to be exposed to;

(b) consider incidents in the capital market and the broader financial services industry;

(c) assess the likely impact of these incidents to the capital market entity; and

(d) identify appropriate response plan and communication strategies that should be undertaken.

9.28 Where feasible, a capital market entity should perform an adversarial attack simulation exercise on the infrastructure hosted with third-party service providers to identify potential vulnerabilities of its cyber defence and response plan against rampant cyber threats.

Chapter 10

NOTIFICATION PROCESS

Notification for Technology-Related Implementation

10.01 A capital market entity must notify the SC through the Vault system prior to implementing any major technology-related services or major enhancement on its critical systems, that may potentially affect its business operations or clients. The notification must include the details set out in **Appendix 4**.

10.02 In the event the Vault system is inaccessible, the capital market entity must notify and submit a detailed report to the SC via email at vault@seccom.com.my in accordance with the notification form provided in **Appendix 4**.

Notification of Technology Incident, Cyber Incident and Near Miss Event

10.03 A capital market entity must immediately notify and submit a report to the SC through the Vault system upon detection of any technology incident that affects its business operations or clients, or any cyber incident or near miss event, on the day of the occurrence of the incident. The notification must include the details set out in **Appendix 5**.

10.04 In the event the Vault system is inaccessible, the capital market entity must notify and submit a report to the SC via email at vault@seccom.com.my in accordance with the notification forms provided in **Appendix 5**.

10.05 The capital market entity must ensure that its board is made aware of the technology incidents and cyber incidents.

10.06 Where a capital market entity has submitted a report in compliance with the requirements under paragraphs 10.03 and 10.04, such capital market entity shall be deemed to have complied with the reporting requirements relating to technology incident or cyber incident under other relevant guidelines issued by the SC.

APPENDIX 1

GUIDANCE TO RISK IDENTIFICATION, ASSESSMENT, MITIGATION, MONITORING, REVIEW AND REPORTING

(1) Risk identification

A capital market entity should identify the extent of the potential threat and vulnerabilities to its IT environment by scoping information risk assessments across different business functions, including any of its information assets that are managed by third-party service providers.

(2) Risk assessment

A capital market entity should assess, identify and profile key technology risk and cyber threats across different business functions by determining associated threat events. In doing so, it should—

(a) perform an analysis of the potential consequences that would result if the technology risk identified were to materialise;

(b) assess the likelihood of the occurrence of the risks identified; and

(c) determine the level of risk impact should the information assets have their confidentiality, integrity or availability compromised.

(3) Risk mitigation

A capital market entity should—

(a) develop appropriate risk treatment by taking into account the risk assessment result based on the criticality of its information assets and the level of risk tolerance;

(b) implement appropriate control measures and carry out regular review and update by taking into account the rapid change of threat landscape and variations in the capital market entity's risk profile.

(4) Risk monitoring, review and reporting

A capital market entity should—

(a) establish a process for assessing and monitoring the effectiveness of process design, its IT controls implementation and outcomes against identified technology risk. This include incorporating the monitoring results and review of

identified technology risk into the performance management, key performance indicator of the capital market entity, and reporting it to the senior management at a frequency based on the level of risks identified.

(b) regularly monitor controls implemented for its IT systems and its environment of operation for changes, signs of attack and other vector that may affect controls and reassess control effectiveness.

APPENDIX 2

GUIDANCE TO METHODOLOGY IN THE IMPLEMENTATION OF CYBER RISK MANAGEMENT STRATEGIES AND MEASURES (Paragraph 9.03)

(1) Identification

In identifying cybersecurity threats, a capital market entity should fully understand its business environment to ensure it can successfully manage arising cyber security threats, vulnerabilities and risks at various levels surroundings its data, systems, and assets.

(2) Protection and Prevention

A capital market entity should develop and implement the appropriate strategy against cyber threats identified to ensure continuous delivery of its services and to minimise or contain the impact of a cyber security incident.

(3) Detection

A capital market entity should develop and implement the appropriate strategy to identify the occurrence of a cyber security event in a timely manner.

(4) Response

A capital market entity should develop and implement appropriate response strategy in case of any detected cyber security event.

(5) Recover

A capital market entity should develop and implement the appropriate strategy to recover from a cyber breach, and to reinstate any capabilities, capacities or services that were impaired due to a cyber security event within the defined recovery time objective of the capital market entity. A capital market entity should prioritise important services or have some level of minimum services available for a temporary period of time.

APPENDIX 3

GUIDING PRINCIPLES RELATING TO THE ADOPTION OF ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

(a) A capital market entity that is adopting artificial intelligence (AI) and machine learning (ML)[1] should be guided by the following principles:

(i) Accountability;

(ii) Transparency and Explainability;

(iii) Fairness and Non-Discrimination; and

(iv) Practical Accuracy and Reliability.

(b) A capital market entity is expected to exercise its judgement in considering and adopting the guiding principles, taking into consideration the circumstances of the capital market entity including its size, scale and complexity.

1. Accountability

(a) A capital market entity should establish and implement a robust and sound governance framework and process to oversee the development and use of its AI and ML, which should include—

(i) clear goals and objectives for the AI and ML system;

(ii) well-defined roles, responsibilities, and lines of authority, within the capital market entity or by third-party service provider; and

(iii) risk-management processes, that includes the management and oversight of third-party service providers and contingency plan that can promptly suspend AI applications whenever required.

(b) A capital market entity should also have a workforce capable of managing AI and ML systems and a broad set of stakeholders.

(c) A capital market entity should ensure that the workforce uses AI and ML systems in a way that respects the rule of law, ethics, code of conduct, human rights, democratic values and diversity, and should include appropriate policies and procedures to ensure the same.

[1] Examples of adoption of AI and ML include for the purpose of supporting advisory services, risk management, client identification and monitoring, selection of trading algorithms and portfolio management of a capital market entity.

2. Transparency and Explainability

(a) A capital market entity should be able to explain what went into making a specific decision by the AI and ML. In adopting AI-assisted decision, the capital market entity should be able to provide an explanation on—

(i) the process (i.e. governance of AI); and

(ii) the outcome of the AI application (i.e. reasoning of the algorithmic decision).

(b) A capital market entity should keep appropriate records with the intention to ensure traceability and auditability.

3. Fairness and Non-Discrimination

(a) A capital market entity should design its AI and ML systems in a way that respects the rule of law, human rights, democratic values and diversity, and should include appropriate safeguards to ensure that users or groups of users are not systematically disadvantaged or discriminated.

(b) A capital market entity should ensure that data and models used for AI and ML-driven decisions are regularly reviewed and validated to guard against the use of biased data or algorithms.

4. Practical Accuracy and Reliability

A capital market entity should—

(a) rigorously conduct validation and testing on its AI and ML systems;

(b) ensure privacy, data protection and security in AI systems by employing data governance and management, throughout the data lifecycle; and

(c) ensure robust security and resilience of its AI systems through, among others, the implementation of appropriate controls and security measures.

APPENDIX 4

NOTIFICATION FOR TECHNOLOGY-RELATED IMPLEMENTATION

Notification Form

1. Contact information	
Contact details of the responsible person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Alternate contact person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Entity details	
o Entity name	
o Entity address	
o Type of entity (for example, financial institutions, participating organisation, exchange)	
o Contact no.	
o Email address	
2. Technology notification details	
o Type of notification	☐New ☐Enhancement ☐ Other: _____
o Notification titled	
o Description	
o Planned date and time	
o Relevant document or attachment (if any)	

APPENDIX 5

NOTIFICATION OF TECHNOLOGY INCIDENT, CYBER INCIDENT AND NEAR MISS EVENT

**Please fill in the fields wherever relevant for technology incident or cyber incidents, fields not labelled must be filled in.*
***(T) – Technology incident, (C) – Cyber incident*

1. Contact information	
Contact details of the responsible person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Alternate contact person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Entity details	
o Entity name	
o Entity address	
o Type of entity (for example, financial institutions, participating organisation, exchange)	
o Contact no.	
o Email address	
2. Incident/near miss event details	
o Type of incident/event	☐ Technology ☐ Cyber ☐ Near Miss Event
o Date and time of the incident/event	
o Date and time when the incident/event was first observed	
o Details of incident/event - Description/Incident summary - Duration of downtime	

3. Impact to systems, assets or information	
o Affected hardware	
o Affected software	
o Affected operating system	
o Impact to stakeholders	
o Potential number of affected customers/clients (T)	
o Actual number of affected customers/clients (T)	
o Number of enquiries by customers/ clients and by which channel (T)	
o Geographical location and IP address of attacker (C)	
4. Resolution of incident	
o What are the actions taken / initial resolution to minimise and mitigate risks from the incident? o What is the current status or resolution of this incident? ☐ Resolved ☐ Unresolved	