Suruhanjaya Sekuriti
Securities Commission
Malaysia

PUBLIC CONSULTATION PAPER

No. 1/2022

PROPOSED REGULATORY FRAMEWORK ON TECHNOLOGY RISK MANAGEMENT

The Securities Commission Malaysia (SC) invites your written comments to this consultation paper. Comments are due by **19 September 2022** and should be sent to:

Email: cpresponse@seccom.com.my

Additional copies of this document may be made without seeking permission from the SC or downloaded from its website at www.sc.com.my.

Confidentiality: Your responses may be made public by the SC. If you do not wish for all or any part of your response or your name to be made public, please state this clearly in the response. Any confidentiality disclaimer that may be generated by your organisation's IT system or included as a general statement in your fax cover sheet will be taken to apply only if you request that the information remain confidential.

The SC agrees to keep your personal data confidential and in full compliance with the applicable principles as laid under the *Personal Data Protection Act 2010*.

CONTENTS

PART A: GENERAL

1. INTRODUCTION

1.1 This consultation paper (CP) is intended to generate discussions and seek feedback from interested parties in relation to the SC's proposed regulatory framework for capital market entities' management of technology risks.

1.2 Digital revolution has led to a constantly changing business environment which offers increasing opportunities for capital market entities to grow and enhance its services. Consequently, the SC notes that in recent years there are more capital market entities leveraging technologies to carry out their activities. While the SC is supportive of this, the SC recognises that opportunities arising from these technological advancements also come with risks.

1.3 Acknowledging the needs for the capital market to be cyber resilient, the SC published a consultation paper in 2016 for the proposed regulatory framework on cyber security resilience. Thereafter, the SC issued *Guidelines on the Management of Cyber Risk* (Cyber Risk Guidelines) in 2016 to guide capital market entities in achieving cyber resilience which commensurate with their respective cyber security risk exposure and impact.

1.4 Since then, the adoption of technology in the capital market has expanded to include new technologies such as artificial intelligence (AI), machine learning (ML) and distributed ledger technology (DLT). To further strengthen the capital market's ability to detect and mitigate risks that come with these new technologies, the SC is proposing to introduce a comprehensive regulatory framework comprising the management of technology risks, data management and principles relating to the adoption of AI and ML (Framework).

1.5 This Framework is expected to subsume the current requirements in Cyber Risk Guidelines, consolidate other requirements relating to technology risks

management in the various guidelines issued by the SC and introduce new requirements.

2. WHAT ARE TECHNOLOGY RISKS

2.1 Technology risks refer to risks emanating from the use of information technology (IT), IT systems and the internet, and includes cyber risks. These risks arise from failures or breaches of IT systems, and platforms or infrastructure which can result in financial loss, disruptions in services or operations, or reputational harm to a capital market entity. Ultimately it may also affect the integrity of the capital market.

3. THE SC'S APPROACH FOR TECHNOLOGY RISK MANAGEMENT

3.1 The Framework will apply on a wide range of capital market entities. Similar to the Cyber Risk Guidelines, the SC is proposing for the Framework to cover the following capital market entities:

(a) Bursa Malaysia Bhd and its subsidiaries;
(b) Federation of Investment Managers Malaysia;
(c) Private Pension Administrator Malaysia;
(d) Capital Markets Services License holders;
(e) Recognized market operators;
(f) Registered persons in Part 2 of Schedule 4 *Capital Markets and Services Act 2007* (CMSA); and
(g) Capital market service providers registered under section 76A of the CMSA.

3.2 Considering the above, the SC strives towards a more principle-based Framework and capital market entities are expected to assess the application of the Framework which commensurate with their respective business operations as well as technology risk exposures. The outcome desired by the

SC for the Framework is two-pronged, i.e. for all capital market entities to have a robust and sound technology risk management framework that promotes strong oversight of technology risks in the capital market entity, and ultimately for the capital market to be cyber resilient.

3.3 Nevertheless, in ensuring that the Framework is comprehensive and is able to provide sufficient mitigation measures to the capital market against technology risks, there are areas in which prescriptive requirements are imposed. Thus, capital market entities will see that the proposed Framework provide a mixture of principle-based and prescriptive requirements.

PART B: PROPOSED REGULATORY FRAMEWORK

1. THE FRAMEWORK

1.1 Essentially, the Framework comprises governance requirements, and requirements on technology risks management, technology operations, technology outsourcing, cyber security and data management. It also comprises principles relating to the adoption of AI and ML.

1.2 The SC expects a capital market entity to establish and implement robust and effective technology risk management framework, technology operations management, technology service provider management, cyber security framework, data management policies and procedures and principles relating to the adoption of AI and ML, wherever applicable (collectively 'TRM Framework') to manage its technology risks and data risks effectively. For this purpose, a capital market entity should review and update its TRM Framework periodically, and in any event, at least once in every three (3) years. The TRM Framework should also be supported with comprehensive and effective policies and procedures that are reviewed and updated at least annually.

1.3 To ensure compliance with the TRM Framework and policies and procedures, a capital market entity should establish an internal compliance process. The internal compliance process should also include an appropriate approval process where senior management's approval should be obtained prior to any deviation from the TRM Framework and policies and procedures. Approval for departure should only be given if the departure is supported with–

(a) an appropriate justification; and

(b) alternative solution or a reasonable timeframe to comply with the TRM Framework and policies and procedures.

Consultation Questions		
Question 1	:	Do you agree for the TRM Framework to be reviewed and updated at least once in every three (3) years while the policies and procedures be reviewed annually? Please provide your reason(s).
Question 2	:	Do you agree that all departures from the TRM Frameworks and policies and procedures are reported to the board, or should there be any materiality threshold to the departures to be reported to the board? If your answer is the latter, what would be your materiality threshold for the purposes of escalation of the departures?

2. GOVERNANCE

Board of Directors

2.1 In an evolving technology risk landscape, it is pertinent that the board of directors (Board) continuously oversee and assess the risk management practices of a capital market entity.

2.2 The Board is critical in setting direction at the strategic level, giving adequate priority in board agenda and allocating sufficient resources for effective management of technology risks.

2.3 In this regard, the SC is proposing that the Board's roles and responsibilities include—

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

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

(c) ensuring that the TRM Framework, policies and procedures are robust, sound and suitable in assisting the capital market entity achieve security, reliability and resilience of its IT operating environment;

(d) in discharging its obligation in paragraph (c) above, the Board should–

(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 Board's approval at least once in every three (3) years;

(iii) ensure that the policies and procedures are regularly reviewed and updated by the senior management for Board's approval at least annually; and

(iv) ensure that the strategies formulated by the TRM Framework are adequately designed to address the technology risks of the capital market entity;

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

(f) ensuring the impact of technology risks 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 arrangement;

(g) ensuring adequate resources are allocated for technology risks management and data management, including identifying at least one responsible person from among the senior management:

(i) who would be responsible for overseeing the day-to-day management of the technology risks and data management; and

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

(h) ensuring clearly segregated line of responsibilities and accountability across all levels and functions in the capital market entity to manage technology risks; and

(i) ensuring that the Board keeps itself up-to-date of new or emerging trends of cyber threats and understand the potential impact of such threats to the entity.

Consultation Questions		
Question 3	:	Does your Board have the capability and competencies to discharge the above oversight functions? If no, please identify the specific function that your Board would have challenges to discharge and provide your reason(s).

Question 4	:	In relation to the requirement under subparagraph 2.3(g)(i) above, do you foresee any issues and challenges if the SC mandates it to be carried out by two (2) different responsible persons? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

Senior Management

2.4 Senior management's support is important in developing and implementing policies and procedures to mitigate technology risks. In this regard, the SC places accountability on the senior management to develop robust and sound TRM Framework and policies and procedures, which commensurate with the risks exposure of the capital market entity.

2.5 Additionally, the SC is proposing that the senior management's roles and responsibilities include—

(a) formulating for Board's approval 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;

(b) 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;

(c) recommending to the Board appropriate strategies and measures to manage technology risks, including making necessary changes to existing policies and procedures, as appropriate;

(d) reporting to the Board on a regular basis matters related to key technology risks, cyber breaches, business impact analysis (BIA) and critical technology operations;

(e) providing the Board with regular updates on cyber security issues, cyber security risks and compliance with cyber security framework;

(f) reviewing, tracking and reporting deviations from the TRM Framework and policies and procedures to the Board;

(g) keeping the Board informed of new and potentially emerging technology risks that may be critical to the entity risk appetite;

(h) establishing a mechanism to monitor and identify any weakness in data management and internal control of the capital market entity which would jeopardise the capital market entity's compliance with SC's policy document;

(i) advising the Board on the appropriate remedial actions to address the identified weakness in data management and internal control; and

(j) implementing the remedial actions as approved by the Board in an effective and timely manner.

Consultation Question		
Question 5	:	Would your current senior management have the capability and competencies to discharge the above functions? If no, please identify the specific function that your senior management would have challenges to discharge, and please provide your reason(s).

Cybersecurity Awareness and Training

2.6 For a capital market entity to manage and mitigate its technology risks, the Board, senior management, employees and agents should be prepared to manage a wide range of technology risks, cyber incidents and scenarios. Thus, a capital market entity should conduct cybersecurity awareness training programme at least annually for its Board, senior management, employees and agents.

Consultation Question	
Question 6	: Do you agree that it is sufficient for cyber security awareness and programme for your Board, senior management, employees and agents to be conducted at least annually? Please provide reasons for your views.

Technology Audit

2.7 Through regular technology audit, a capital market entity may detect risks and implement the proper controls needed to eliminate or mitigate risks associated with the adoption of technology. This would in turn ensure the systems used are not vulnerable to, amongst others, any irregular activities and data are well protected.

2.8 In this regard, a capital market entity should carry out regular technology audit which is able to determine whether the capital market entity's—

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

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

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

2.9 The technology audit should at the minimum comprise independent and objective opinion on the effectiveness of the capital market entity's TRM Framework, governance, and internal controls in mitigating its technology risks.

2.10 A capital market entity should ensure that the auditors performing its audit possess the necessary competency, knowledge and experience to carry out its technology audit work. This includes the ability to challenge the capital market entity's IT processes for improvement.

Consultation Question	
Question 7 :	Do you foresee any implementation issues and challenges with regards to the proposed technology audit above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

3. TECHNOLOGY RISK MANAGEMENT FRAMEWORK

3.1 Technology risk management framework is an essential part of a capital market entity's enterprise risk management. It would allow the capital market entity to make informed decisions on managing technology risks throughout its organisation. The technology risk management framework shall preserve the confidentiality, integrity, and availability of information by applying a risk management process and give confidence to the key stakeholders that risks are adequately managed.

3.2 The technology risk management framework established and implemented by a capital market entity should comprise risk identification, risk assessment, risk mitigation, and risk monitoring, and review and reporting on the existing and any emerging technology adopted by the capital market entity.

3.3 Risks should be assigned to the appropriate risk owner who would be accountable for ensuring the proper risk treatment plan are implemented and enforced for a specific technology risk. The role of the risk owner should be clearly defined and might be assumed by a function or team within the organisation, with the authority to manage the technology risks. The risk owner is to establish appropriate, effective, and efficient technical and organisational measures in all steps of the process.

3.4 Where relevant, a capital market entity should adopt the principles relating to the adoption of AI and ML as specified in Appendix A. The principles relating to the adoption of AI and ML should be read together with these Guidelines, relevant laws and regulations, and guidelines issued by the SC.

3.5 Due to fast evolving nature of emerging technology and the increasing levels of adoption of new technology in the market, a capital market entity should regularly review its risk exposures and associated controls to confirm that it remains in line with the capital market entity risk appetite.

Consultation Question	
Question 8 :	Do you foresee any implementation issues and challenges with regards to the technology risk management framework, specifically on emerging technology that your organisation may adopt as mentioned in paragraph 3.2? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

4. TECHNOLOGY OPERATIONS MANAGEMENT

Technology Project Management

4.1 Technology project management is the process of managing technology and technology-related projects. A capital market entity should establish and implement clear and comprehensive internal guidelines on technology project management so that any technology and technology-related project could be completed with clarity, alignment, traceability, and effective resource utilisation.

4.2 A capital market entity should 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.

4.3 A capital market entity should conduct risk assessments to identify, manage and monitor risks arising from the implementation of the technology projects and throughout the project life cycle as project risks can adversely impact the project delivery timeline, budget, and quality of the project deliverables.

4.4 Where appropriate, a project steering committee comprising at least one senior representative from each business function should be formed. This steering committee should–

(a) serve as technology and technology-related project coordinator and advisor, providing overall direction on project management and making user-related decisions about system and programme design; and

(b) be responsible for all deliverables, project costs and schedules including regularly reviewing and evaluating progress of the project, making recommendations regarding changes of the project team members, managing budgets or schedules, changing project objectives, deciding on the need for redesign, and taking corrective action where required.

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

4.5 A capital market entity should also establish and implement internal processes encompassing:

(a) System acquisition and development;
(b) System testing and acceptance; and
(c) Access control management.

System Acquisition and Development

4.6 A capital market entity should establish and implement clear–requirements and processes to manage the capital market entity's system development life cycle (SDLC) encompassing planning, requirement analysis, design, implementation, testing, and acceptance.

4.7 It should include, among others, requirements and processes for—

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

(b) assessment of the vendor's software development, to ensure that the capital market entity's security is not compromised and its quality assurance is met;

(c) the capital market entity to ensure that source codes for critical systems acquired are accessible by the capital market entity during the contract period and after termination of the contract with its vendor; and

(d) the capital market entity to enter into a source code escrow agreement or if an escrow agreement cannot be implemented, for the identification of an appropriate alternative.

4.8 A capital market entity should incorporate security requirements into the system design which would enable it to carry out constant security evaluation and comply with security practices throughout the SDLC in order to minimise system vulnerabilities and reduce risk exposure.

4.9 At the minimum, the security requirements should 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

4.10 A capital market entity should 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 should cover the system's

business logic, function, controls and performance under various load and stress conditions.

4.11 Where feasible, the capital market entity is recommended to use automated testing methodology to ensure comprehensiveness of the testing scopes, as part of the testing strategy.

Access Control Management

4.12 To minimise risk of unauthorised access to information assets, a capital market entity should—

(a) establish user access management policies and procedures which provide, modify and revoke access rights to information assets. Access rights and privileges should be granted in accordance to 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 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.

4.13 A capital market entity should use stronger fraud deterrents for sensitive system functions to safeguard the systems and data from unauthorised access on a best effort basis. For example, using multi-factor authentication (MFA), or two factor authentication (2FA) and privilege access management to secure employee and customer authentication process.

Consultation Questions		
Question 9	:	Do you foresee any implementation issues and challenges in performing risk assessment from the implementation of technology projects and throughout the project life cycle regardless of the project size? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 10	:	Do you have a project management steering committee to manage technology projects regardless of the project size? If no, please state who manages the technology projects in your organisation.
Question 11	:	Do you foresee any implementation issues and challenges with regards to the need to have a source code escrow agreement? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 12	:	Do foresee any implementation issues and challenges on the proposed requirements with regards to- (a) access control management; (b) logging facility; and (c) fraud deterrents mechanism. If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

Change Management

4.14 For this section, a change can be described as any addition, removal, or modification to the systems that could have a direct or indirect effect on the capital market entity's IT system.

4.15 A capital market entity should establish a change management process to oversee any changes made to the IT system covering among others, impact assessment, approval, scheduling, implementation and communication of the IT system.

4.16 A capital market entity should ensure, prior to deploying any changes to its IT system in the production environment—

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

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

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

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

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

4.17 In addition to the above, a capital market entity should also establish and implement clear process and procedures to handle any emergency change to the production environment.

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

Patch Management and Technology Obsolescence

4.19 Patch management is the process of distributing and applying updates to software. These patches are necessary to correct errors and fix vulnerabilities in the software that are susceptible to cyber-attacks, hence reducing security risk. A proper patch management process would also ensure that a capital market entity's IT systems are not obsolete.

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

4.21 Any hardware's or software's end-of-support (EOS)[1] dates should be closely monitored including those relating to security vulnerabilities that surface after the EOS date.

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

[1] EOS means the provider will no longer provide support for a product such as repairs, limited tech support and parts availability are still be provided until depleted.

4.23 A capital market entity should also ensure that its critical IT systems are not running on obsolescence systems or end-of-life (EOL)[2] information assets. If there is a need for a capital market entity to continue using IT systems which are running on obsolescence systems, it should—

1. ensure that approval is obtained from senior management and a validity period is assigned to the continued use of such IT systems that commensurate to the identified risks and capital market entity's risk mitigation process; and

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

Cryptography

4.24 Cryptography is used to protect sensitive data and information from unauthorised or unintentional disclosure while the data is in transit (either electronically or physically) and in storage. In this regard, cryptography is an important tool for safeguarding the confidentiality, authenticity and integrity of its sensitive data including business information and client data.

4.25 A capital market entity should implement suitable cryptographic controls to secure the confidentiality of sensitive data and information encompassing data-in-motion, data-in-use and data-at-rest.

4.26 Cryptographic controls may include—

(a) data encryption;

(b) digital signature or message authentication codes; or

(c) cryptographic techniques,

which may be used to obtain evidence of the occurrence or non-occurrence

[2] EOL means a product that is at the end of the product lifecycle which prevents users from getting updates, which indicates the product has reached its useful lifespan. Most EOL products are not supported by the manufacturer.

of an event or action (non-repudiation) and to verify users with the right access (authentication).

4.27 A capital market entity should establish robust and sound policies and procedures to manage the use of cryptography including cryptographic key management, and controls for its critical business application and transfer and storage of confidential data and information. A capital market entity should also ensure that its policies and procedures are being effectively implemented.

Consultation Questions	
Question 13:	Do you foresee any implementation issues and challenges with regards to the proposed requirements on Change Management above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 14:	Do you foresee any implementation issues and challenges with regards to the proposed requirements on Patch Management and Technology Obsolescence above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 15:	Do you currently use cryptography as a tool to secure the confidentiality of your data-in-motion, data-in-use and data-at-rest? Do you foresee any implementation issues and challenges with regards to the use of cryptography in your organisation? If yes to the latter question, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

Network Resilience

4.28 A capital market entity should design a sound network architecture to support its business activities and future growth. The network architecture should enable the capital market entity to achieve high network availability, redundancy, accessibility and resiliency.

4.29 A capital market entity should also continuously assess its network architecture design to identify any flaws to sustain an acceptable level of availability to support its business activities.

4.30 A capital market entity should ensure its network infrastructure with systems that demand high availability and reliability to have no single point of failure. This may be done by implementing redundancy, fault tolerance, congestion control and diversity in network routing.

4.31 The change management process discussed in paragraph 4.17 is also applicable to any changes made to the network infrastructure.

Operational Resilience

4.32 A capital market entity's data centre operation including the use of cloud services should be supported by a sound IT infrastructure which considers its IT operational resiliency and availability target as well as being aligned to its business needs.

4.33 The availability target set by the capital market entity should result in reducing the impact of any failure or disruption to the capital market entity's data centre operations.

4.34 Among others, a capital market entity should—

(a) conduct a data centre risk assessment to ensure data centre's resiliency which considers the capital market entity's business model and risk appetite. The assessment should be aligned with 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 capital market entity's business needs;

(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.

4.35 Where a third-party service provider manages the data centre, the capital market entity should ensure that the third-party service provider furnishes the

Data Centre Risk Assessment report upon request by the capital market entity or the SC. The report should cover the review of the data centres system, suitability of its design of controls and effectiveness of the controls. The capital market entity should perform its own risk assessment of such report to ensure it is consistent with its risk appetite and tolerance.

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

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

4.38 A capital market entity should establish a monitoring and reporting mechanism of its network, application and system to flag abnormal behaviour and aid in analysis. It should undertake a follow-up action in accordance with the procedures set out by the capital market entity upon the detection of any abnormal behaviour. It should retain adequate network, application and system device logs for investigation and troubleshooting for an appropriate period as it determines.

IT Disaster Recovery Plan

4.39 A capital market entity should establish and test its IT Disaster Recovery Plan (DRP) on a regular basis to manage availability and restore IT system within the recovery objectives being set in the event of disruption.

4.40 To ensure the implementation effectiveness of the DRP, all relevant key stakeholders from business and IT functions of the capital market entity should participate in the DRP.

4.41 A capital market entity's DRP should consist of—

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

(b) criteria for plan activation (circumstances the disaster is declared, when the plan is put into action, type of scenarios the disaster is declared);

(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 develop long-term risk mitigations.

4.42 Where information assets are managed by third-party service providers, the capital market entity should regularly assess the third-party service provider's capability in ensuring its availability and to co-ordinate the DRP with involvement from the third-party service provider for these information assets to meet the business recovery objectives.

Consultation Questions	
Question 16:	Do you foresee any implementation issues and challenges with regards to the proposed requirements on Network Resilience and Operational Resilience above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 17:	Do you foresee any implementation issues and challenges with regards to the proposed requirements on IT Disaster Recovery Plan above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

5. TECHNOLOGY SERVICE PROVIDER MANAGEMENT

5.1 A capital market entity should be able to demonstrate that it implements and upholds robust and sound risk management in relation to its outsourced arrangements including any sub-arrangements.

Business Continuity and IT Disaster Recovery Plan

5.2 The capital market entity should ensure that the technology service provider regularly test its BCP to validate the feasibility of the RTO, recovery point objective and resumption of its operating capacities. In this regard, the capital market entity should proactively seek assurance on the state of BCP preparedness of the technology service provider.

5.3 The capital market entity should also participate in the technology service provider's BCP and IT disaster recovery exercise or conduct joint testing with the respective technology service provider.

5.4 The capital market entity should ensure that the technology service provider notify the capital market entity of any test finding that may affect its performance, may result in substantial changes in the technology service provider's BCP and any adverse development that could substantially impact the service provided to the capital market entity.

5.5 The capital market entity should ensure that the technology service provider notify the capital market entity promptly any substantial changes in its BCP.

Due Diligence, Contract Management and Performance Monitoring

5.6 The Board should perform its oversight role over the IT outsourcing arrangements and is accountable for ensuring the effectiveness of the capital market entity's outsourcing policies and processes.

5.7 Apart from the technology itself, a capital market entity should ensure that all technology service providers it engages are reliable so as to minimise any risks related to the technology it expects to adopt from the technology service provider. Therefore, it is pertinent for a capital market entity to conduct due diligence on the technology service provider, establish proper policies and procedures governing contract management with all technology service providers, and monitor their performance on an ongoing basis.

5.8 A capital market entity should conduct adequate due diligence prior to selecting a technology service provider and conduct periodic assessment on the technology service providers' capabilities during the contract period. The scope of the due diligence should include the technology service provider's financial stability, reputation, managerial skills, technical competency, operational capability and capacity to undertake the provision of the outsourced task effectively at all times. Other factors to be considered in assessing the technology service provider's capabilities in managing the risk are, among others:

(a) Data loss;
(b) Technology risk;
(c) Reputational;
(d) Exit risk;
(e) Concentration risk;
(f) Operational risk including resiliency to operational and system disruption, disaster preparedness plan and business continuity plan;
(g) Detrimental risk;
(h) Data security of the 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
(i) Resiliency to cyber risk.

5.9 A capital market entity should ensure that the technology service provider selected practice cyber hygiene and remain cognisant in protecting its data's confidentiality, its system's integrity and resilience.

Cloud Services

5.10 A capital market entity should ensure the level of governance and controls implemented over cloud service provider including cloud strategy and cloud operational management commensurate with the risks posed by 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.

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

5.12 A capital market entity should, 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 cloud infrastructure;
(c) Multi-tenancy or data commingling;
(d) Identity and access management (IAM) controls, data protection and cryptographic key management;
(e) Expansion of the capital market entity's cyber security operations 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.

5.13 A capital market entity should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the cloud service provider during the contractual period of the cloud services agreement.

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

Contract Management

5.15 A capital market entity should establish a service level agreement when engaging technology service providers.

5.16 The service level agreement entered by a capital market entity with its technology service provider should 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 its clients' data during and after the end of the contract period;

(c) access rights, and information or documents of the technology service provider related to the outsourced activity required for the relevant regulatory bodies and the capital market entity for the purpose of performing review or audit on the relevant systems;

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

(e) business continuity plan of the outsourced task (i.e. in the event of system failure/disruption);

(f) regular business continuity plan testing of the technology service provider, and the result of such testing is provided to the capital market entity;

(g) system development and maintenance arrangements with the technology service provider including requirements for such technology service provider to comply with the capital market entity's data and information security policy;

(h) a clearly defined arrangement for immediate notification by technology service providers to the capital market entity and other relevant regulatory bodies in the event of a technology and cyber incident; and

(i) clearly defined cyber security responsibilities of all parties.

5.17 A capital market entity should ensure data residing in technology service providers are recoverable in a timely manner.

5.18 A capital market entity should regularly review the technology service providers performance and the service level agreement to ensure it remains relevant and effective.

5.19 A capital market entity should ensure its technology service providers comply with all the relevant regulatory requirements.

Consultation Questions	
Question 18:	Do you foresee any implementation issues and challenges with regards to the proposed requirements on technology service provider management above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 19:	Do you review your technology service provider's performance and the service level agreement on a regular basis? If yes, how often is the review conducted.

6. CYBER SECURITY FRAMEWORK

Cyber Security Framework

6.1 A capital market entity should develop a cyber security framework that articulates the governance and implementation of adequate cyber security controls which commensurate with the risk and business profile of the capital market entity.

6.2 The cyber security framework should be translated into relevant policies and procedures to address interoperability, usability, and privacy of the entity business information and client data within its custody, and safeguarding its confidentiality, integrity and availability. Roles and responsibilities should be defined to ensure accountability for cyber security activities throughout the organisation.

6.3 A capital market entity should implement cyber risk management strategies and measures in a structured and methodical manner, as part of its wider risk management programme.

6.4 A capital market entity should consider the following methodology in implementing effective cyber security strategies and measures to help the entity understands, manages, structures, minimises cyber security risks and potential compromise of its cyber security defence:

(a) Identify

A capital market entity should fully understand its business environment to ensure it can successfully manage rising cyber security threats, vulnerabilities and risks at various levels surrounding its data, systems, and assets.

(b) Protect and Prevent

A capital market entity should develop and implement the appropriate strategy against cyber threats identified to ensure continuous delivery

of its services. These control measures should minimise or contain the impact of a cyber security incident.

(c) Detect

A capital market entity should develop and implement the appropriate strategy to identify the occurrence of a cyber security event. Timely detection is crucial as it allows the proper response to be commenced.

(d) Respond

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

(e) 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 capital market entity's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.

Cyber Security Measures and Monitoring

6.5 A capital market entity should establish, implement and regularly review the security hardening standards on its operating systems, databases, application systems, network and security devices. The security hardening standards checklist should be updated regularly. A capital market entity should conduct continuous review and update of rules and configurations for operating systems, databases, application systems, network and security devices.

6.6 A capital market entity should establish a monitoring and detection process to support continuous surveillance of any cyber event. The monitoring and detection process should include among others clearly defined escalation and

decision-making processes to ensure any adverse effect of a cyber incident is properly managed.

6.7 A capital market entity should proactively monitor any cyber event, detect any anomalous activity and conduct analysis on any detected event.

6.8 A capital market entity should establish 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 on a best effort basis. This is because the SOC and MSS will enable the capital market entity to have greater speed in recognising attacks and resolving them before it cause more damages thus improved the security visibility of its cybersecurity posture.

6.9 The SOC implemented should be secured with proper access controls, skilled resources, and accommodated with disaster recovery capabilities and dashboard to oversee the overall capital market entity's network perimeter.

6.10 A capital market entity should establish a process to collect, review and retain system logs to facilitate the capital market entity's cyber events monitoring operations to protect the system logs against unauthorised access.

6.11 A capital market entity should establish a baseline indicator for each of the IT systems being monitored. Any anomalies or suspicious user behaviour detected against the baseline indicator should be analysed and escalated timely in accordance with the capital market entity's escalation and decision-making processes.

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

6.13 If reasonably practicable, a capital market entity should 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.

6.14 A capital market entity should regularly review its cyber threat analysis report. The cyber threat analysis report should be communicated to the senior management. At minimum, the report should encompass the cyber threat trends and statistics, incidents grouping by type of attack, target and source of IP addresses.

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

Consultation Question	
Question 20:	Do you foresee any implementation issues and challenges with regards to the proposed requirements above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

Cyber Security Incident Response and Recovery

6.16 A capital market entity should establish a cyber incident response capability to manage and minimise damage from cyber incidents, to recover and learn from such incidents. A capital market entity should also establish a clearly defined escalation and decision-making processes to ensure that any adverse effect of a cyber incident is properly managed and initiate recovery action quickly.

6.17 The cyber incident response capability should encompass the following phases:

(a) Preparation

A capital market entity should 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 should also clearly define the roles and responsibilities of the team.

(b) Detection and Analysis

A capital market entity should 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 should 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 should 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 should be produced from the post incident review and presented to all relevant stakeholders.

For the purposes stated in paragraph 6.17(c), a capital market entity should identify the critical systems and services within its operating

environment that should be recovered on a priority basis in order to provide certain minimum level of services during the downtime.

6.18 A capital market entity should determine how much time it will require to return to its full service and operations.

6.19 A capital market entity should 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

6.20 A capital market entity should 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 should among others outline the relevant control measures to mitigate any vulnerabilities and cyber threats in its operating environment.

6.21 A capital market entity should 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.

6.22 If reasonably practicable, a capital market entity should undertake regular compromise assessment (CA) on its critical systems to prevent and detect any potential compromise of its security posture.

6.23 A capital market entity should also conduct regular penetration testing exercise at least annually to mimic an experienced hacker attacking the capital marker entity's production environment, with the aim to obtain in-depth evaluation of its cyber defences. The scope of penetration testing should

include internal and external network infrastructure as well as critical systems such as web, mobile and external facing applications. When the capital market entity's critical system undergoes major changes or updates, penetration testing exercise should also be carried out.

6.24 A capital market entity should ensure the penetration testing exercise process is documented and performed by experiences and qualified professionals who are aware of the risk of undertaking such exercise and can limit the damage resulting from a successful break-in to a production environment. The capital market entity's senior management approval should be obtained before finalisation of the test scope.

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

(a) Severity level and classification of identified vulnerabilities;

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

(c) Risk assessment and mitigation plans to manage exceptions (for vulnerabilities which the capital market entity's unable to remediate timely) with approval from senior management.

Cyber Simulation Exercise

6.26 A capital market entity should establish a comprehensive business continuity plan and regularly test the effectiveness of its cyber incident response and recovery plan based on current and emerging cyber threat scenarios.

6.27 A capital market entity should ensure the simulation exercise is conducted with involvement from key stakeholders comprising senior management,

business unit leaders, corporate public relations and communication, crisis management team, third-party service providers and technical employee who perform detection, investigation, containment and recovery process.

6.28 To ensure the capital market entity is prepared to respond to cyber incidents, the capital market entity should—

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

(b) consider incidents in the capital market and where applicable, 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.

6.29 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. Typically, there will be three types of team involved:

(a) The Red Team

This group acts like the cyber attacker utilising the same techniques and procedures (TTPs) used and tries to break through the defence perimeter of the entity in a controlled environment with no disruption to production systems.

(b) The Blue Team

This group acts like the IT security employee of the entity and attempts to thwart of the cyberattacks that have been launched by the Red Team.

(c) The Purple Team

This is a combination of both the Red and Blue Teams and works with both sides in order to yield the maximum results for the entities.

6.30 The objectives, scope and conditions of engagement for the cyber simulation exercise should be determined before the initiation of the exercise.

Consultation Question	
Question 21:	Do you foresee any implementation issues and challenges with regards to the proposed requirements above? If yes, please describe your specific issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

7. MANAGEMENT OF DATA

Governance

7.1 A capital market entity should establish and implement robust and sound data management policies that define its approach to data and information management.

7.2 A capital market entity should ensure that its data management include—

(a) policies and procedures that encompass the full life cycle of data, from acquisition to use to disposal;

(b) adequate controls to effectively monitor among others, data quality, data security and privacy, data storage and data disposal; and

(c) a proper governance arrangement that clearly outlines the ownership, usage and sharing of data within the capital market entity to ensure confidentiality, integrity and availability of the data.

7.3 A capital market entity should perform regular assessment of its data management policies and procedures to ensure its continuous effectiveness. This includes conducting periodic risk assessment and reporting to the senior management and the Board and recommending enhancements or corrective measures to address any gap in the data management policies and procedures.

7.4 A capital market entity should also ensure its data management policies and procedures is at all times consistent with all relevant legislation, regulations and guidelines, including the Personal Data Protection Act 2010.

7.5 The responsible person as appointed by the Board pursuant to paragraph 2.3 (g) should ensure that the requirements under this data management policies and procedures are carried out by the capital market entity.

7.6 A capital market entity should provide continuous development and technical support, including training to its Board and employees, and update its user guidelines and manuals to users to ensure smooth business operations.

Data Quality

7.7 Data quality is a measure of the overall condition and utility of a dataset(s) including its ability to be easily processed and analysed for the full lifecycle of data processing.

7.8 A capital market entity should maintain good data quality at all times based on the following main criteria:

(a) Accuracy

Data accuracy refers to error-free data that aligns with its representation to be utilised as a reliable source of data.

(b) Completeness

Data completeness refers to the comprehensiveness or wholeness of the data for the intended purpose. A capital market entity should store data at granular level or the lowest level possible. A capital market entity should determine whether a data asset contains unacceptable gaps, as this would affect data quality.

(c) Timeliness

Data timeliness refers to the time expectation on the readiness of the data when it is needed.

(d) Consistency

Data consistency refers to the reliability and trustworthiness of data throughout its lifecycle. It also refers to consistent view of the data, including visible changes made by the user's own transactions and transactions of other users.

(e) Currency

Data currency refers to the degree to which how current or up-to-date the data is at the time of release

7.9 A capital market entity should ensure that there is no duplication or overlaps recorded in the data set on a best effort basis.

Data Security and Privacy

7.10 A capital market entity should ensure that its data management policies and procedures are robust and sound to prevent losses arising from data breach or other acts of internal or external threats, negligence and cyber attack.

7.11 To ensure that all data are adequately safeguarded, a capital market entity's data management policies and procedures should cover the process of identification, handling, transmission, movement, destruction and availability of data based on the following measures:

(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 information assets 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 information asset. Access to data and information assets 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 and mandate third-party governance standards to ensure data and information assets 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 which should include the process for preparation, identification, containment, eradication, recovery and lesson learned from data breaches.

7.12 A capital market entity should 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.

7.13 A capital market entity should establish and implement data loss prevention (DLP) mechanism to cover:

(a) Data in-use – data being processed by IT resources.
(b) Data in-motion – data being transmitted on the network.
(c) Data at-rest – data stored in mediums such as servers, backup media and databases.

Data Storage

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

7.15 If upon conducting an assessment, the results of the assessment warrants for a migration, a capital market entity should develop and execute a plan to migrate its data and IT systems into a new environment which commensurate

with the capital market entity's data management policies and procedures, taking into consideration the results of the risk assessment.

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

7.17 A capital market entity should ensure data is protected by an adequate backup schedule and perform regularly testing according to the needs of the capital market entity, to ensure data can be restored from backups.

Data Disposal

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

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

7.20 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 should ensure the data will be deleted from those devices after the data is no longer in use. Data disposal involves putting the information 'beyond use' by the user of the device. Data held in a recycling 'bin' on the device or data which can be easily recovered by the user is not regarded as being 'beyond use' and may still be subject to discovery and disclosure.

7.21 A capital market entity should implement a clear data sanitisation procedure to ensure data is irretrievably destroyed from its IT equipment and IT devices. The capital market entity's sanitisation procedure should include—

(a) record data sanitisation activities performed such as location of the device, 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.

7.22 A capital market entity should require all third parties who have the capital market entity's data in its custody to perform data sanitisation appropriately and securely.

7.23 A capital market entity should ensure third-party service provider performs disposal of the capital market entity's data within its custody appropriately and securely to avoid the risk that the data that is no longer required is accessible to a third-party. Such requirements should also be included in any contract entered into with a third-party service provider.

Submissions of Data to the SC

7.24 For the purposes of submission of data to the SC pursuant to SC's requirements[3], it is pertinent that a capital market entity ensures all submitted data adhere to the level of data quality as expected by the SC. In line with this, the SC views it important for a capital market entity to:

(a) ensure that all data submitted to the SC adhere to all the criteria in paragraph 7.8 above;

(b) appoint a head of reporting from among the senior management who will be responsible for:

(i) overseeing management of data and implementing appropriate

[3] For example, data that are submitted to the SC via common reporting platform.

internal controls to ensure the capital market entity's compliance with the reporting requirements of the SC;

(ii) all data submissions to SC; and

(iii) ensure sufficient resources are allocated for the data management reporting.

7.25 Further to the requirements in paragraph 7.24, a capital market entity should ensure all submissions of data to the SC are made in a timely manner.

Consultation Questions	
Question 22:	Do you foresee any issues and challenges with regards to implementing the data management policies and procedures in your organisation? If yes, please describe your issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?
Question 23:	Do you foresee any issues and challenges with regards to requirements for submission of data to the SC? If yes, please describe your issues and challenges. What would be the appropriate steps that would suit your current entity towards meeting similar objective?

8. COMPLIANCE PROCESS

Notification for Technology-Related Application

8.1 Prior to implementing any major technology-related services or major enhancement on its critical systems that may potentially affect its business operations or clients, a capital market entity should ensure a readiness assessment is conducted by an independent party and endorsed by the senior management. At the minimum, the readiness assessment should include the following:

(a) Acceptance testing report and resolution of issues identified;

(b) Risk management according to the risk identified and its strategies to manage such risks. This includes responsibilities, policies, procedures and controls to address the risks;

(c) Supporting system, system security including internal controls;

(d) Organisational structure;

(e) Operational manuals;

(f) Information technology policies and procedures;

(g) Business continuity plan; and

(h) Description of the enhancements to the existing technologies with risk assessment of the proposed enhancements.

Consultation Question		
Question 24	:	Do you think the minimum requirements listed in paragraph 8.1 are sufficient to assess readiness? Please provide specific reasons for your views.

APPENDIX A: PRINCIPLES RELATING TO THE ADOPTION OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

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

(a) Accountability;
(b) Transparency and Explainability;
(c) Fairness and Non-Discrimination; and
(d) Practical Accuracy and Reliability.

A. Accountability

1. Accountability aims to reduce harm to investors and strengthen market integrity by making a capital market entity's senior leadership, i.e. its Board and senior management accountable for the actions and outcomes of its AI and ML.

2. Therefore, 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 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 applicants whenever required.

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

B. Transparency and Explainability

1. Transparency, explainability, and traceability are key requirements for trustworthy AI and ML. Transparent AI and ML is understandable, explainable and interpretable. It allows users to see whether the models have been thoroughly tested and make sense, and that they can understand why particular decisions are made.

2. Explainability promotes understanding AI and ML's logic and reasoning. It is more than just double-checking the outcome of AI and ML. In this regard, 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, it be able to provide explanation on—

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

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

3. Traceability is related to the need of a capital market entity to maintain a complete account of data, processes and decision-making during the AI and ML system lifecycle and documented in a way that can be easily understood and analysed. In this regard, a capital market entity should keep appropriate records with the intention to ensure traceability and auditability.

C. Fairness and Non-Discrimination

1. 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.

2. 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.

D. Practical Accuracy and Reliability

1. Accuracy in AI and ML refers to the accuracy of input data and outputs generated, both in terms of accuracy of decisions or predictions. A reliable AI and ML system is one that works properly as designed and intended and resilient against cyber-attacks and vulnerabilities. Accuracy and reliability reinforce a trustworthy AI and ML.

2. To achieve 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.

Consultation Question	
Question 25 :	Do you agree with the recommended principles for the use of AI and ML? Do you think there are any additional principles that should be included? Please provide reasons for your views.

PART C: GLOSSARY OF TERMS

Cyber Incident	means an observable occurrence indicating a possible breach in the systems, network and operating environment;
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 a capital market entity's Information Assets, IT Systems and operating environment;
Cyber Threat	means a circumstance or incident with the potential to exploit one or more vulnerabilities intentionally or unintentionally in an entity's information assets, systems and operating environment;
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;
Information Assets	means information or data that is of value to the capital market entities, 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;
IT	means information technology;
IT System	means the set of hardware, software and facilities that integrates an entity's information assets. 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 entity's usage;
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;
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 or cyber incident; and
Recovery Time Objective (RTO)	means targeted duration of time which an information system and network must be recovered after a cyber breach.