19 September 2022

To:
Malaysia Securities Commission
Submitted by email to: cpresponse@seccom.com.my

ASIFMA Response to SC Consultation on "Proposed Regulatory Framework on Technology Risk Management"

Dear Sir/Madam,

ASIFMA[1] and its members welcome the opportunity to respond to the Malaysia Securities Commission (SC) public consultation paper No. 1/2022 on a Proposed Regulatory Framework on Technology Risk Management (TRM) (Consultation Paper).

On behalf of our members, we share with you below our general comments on the consultation paper which include the need for the framework to be principles-and risk based throughout, clarity around the legal application, the need to recognise global financial institutions' group level technology risk management frameworks, risk-based approach towards testing with Third Party Providers, and the adoption of the Financial Sector Profile. This is followed by detailed comments on some of the paragraphs in the draft framework.

We are grateful for the opportunity to share our feedback on the Consultation Paper. We hope our suggestions will be reflected in the final TRM framework and are more than willing to discuss our response in more detail during a meeting. We remain at your disposal for any questions you might have in relation to the below response.

Best regards

Laurence Van der Loo

Executive Director Technology and Operations

ASIFMA

[1] ASIFMA is an independent, regional trade association with over 165 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.

ASIFMA Headquarters
Unit 3603, Tower 2, Lippo Centre
89 Queensway
Admiralty, Hong Kong
Tel: +852 2531 6500

ASIFMA Singapore Office
One Raffles Quay, North Tower
Level 49, Unit 51B
Singapore, 048583
Tel: +65 6622 5970

General comments:

- **Principles- and risk-based approach**

We note and welcome SC's commitment to take on a principle-based approach. A principle-based and risk-based approach is prudent as it allows Capital Market Entities (CMEs) to demonstrate security capabilities and outcomes in proportion to their size, complexity, and risk appetite. In the spirit of this risk-based approach for TRM we submit that there should also be distinction between critical service providers and other service providers for the provisions around as due diligence, disaster recovery, and other areas found in this draft framework, which stand out as being prescriptive. Given that each firm has a unique operating model and risk appetite, we encourage SC to focus only on high-level, outcome-focused requirements within this framework and remove any prescriptive provisions such articles 4.16(c) On 5.12(j), 6.14, and 7.11.

- **Legal application**

We would like to clarify with SC if compliance with this framework is mandatory for CMEs. If it is indeed mandatory, we reiterate the importance of keeping the document at a high-level and remove prescriptive requirements. Instead, guidance on how to implement the framework could be shared by SC through a separate guidelines document that would be non-binding. This would help remove any confusion around implementation. Alternatively, SC can use symbols within this framework to denote parts which are mandatory and those that are recommendations. This approach is consistent with the approach in Bank Negara Malaysia (BNM)'s Risk Management in technology (RMiT) where BNM uses "S" and "G" to denote a requirement and a recommendation respectively.

- **Recognition of financial institutions' group level technology risk management frameworks**

Malaysia is home to many international firms which have firmwide technology risk management frameworks. We encourage SC to include a provision that recognizes international firms' firmwide technology risk management frameworks and allows CMEs to leverage their group-wide established TRM frameworks without the need to build and entirely new framework for their operations in Malaysia. Further detail is provided in the section below in response to parts 2.4 - 2.5, 3.1 - 3.5, 4.34(a) and others.

- **Risk-based approach towards testing with third-party providers**

We note recommendations in the TRM framework for joint BCP or IT Disaster Recovery exercises with third-party providers or for a CME to perform an adversarial attack simulation exercise on the infrastructure hosted with third-party service providers. We recommend that SC allow CMEs to take a risk-based approach and focus on critical third-party providers when considering joint BCP or IT Disaster Recovery exercises. This a prudent approach as conducting joint exercises require a tremendous amount of resources and covering all third-party providers is not practical. In addition, we would like to recommend SC to remove the requirement to perform an adversarial attack simulation exercise on the infrastructure hosted with third-party service providers as this could be perceived as malicious cyberattack by the third-party and could create significant disruptions to third-party service providers, even to CMEs themselves.

In addition, we suggest that CMEs should be allowed to establish their own testing framework and requirements for intra-group providers on a risk-based approach and that the joint testing requirements be limited to true third-party providers.

- **Adoption of International Framework – Financial Sector Profile**

Finally, in order to boost sector's overall resilience, it is important that SC focus on encouraging firms to make use of a risk-and principles-based cybersecurity framework that could be appropriately applied to all

financial market participants regardless of size. The global financial industry created the Financial Sector Profile[2] (or Cyber Risk Institute Profile or FSP), a cyber risk management assessment tool that the industry created which allows an organisation to diagnose cyber risk and apply relevant standards and best practices to appropriately manage that risk. The FSP adopts a tiering mechanism that serves as a scaling device to customise the Profile based on an individual institution's risk and activities. Four categories of impact are most reflective of the institution's impact: National, Subnational, Sectoral, or Localised. As an example, tier 1 institutions with national impacts are expected to assess against 277 diagnostic statements while tier 4 institutions with localised impact need only to answer to 137 diagnostic statements. FSP synthesizes the best cyber practices from industry, as well as regulators in different jurisdictions. We believe adoption of the FSP by FIs and recognition of the FSP by SC would increase global regulatory harmonisation and elevate the sector's cyber posture as well as make communication between firms and competent authorities in Malaysia more effective. SC could benefit from the standardised risk assessment tool to better discern the sector's systemic risk with more time for jurisdictional specialisation.

Comments on specific articles in Part B: Proposed Regulatory Framework:

Clause 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.

Feedback/Comments:

- We would like to confirm that the list of frameworks listed in clause 1.2 refers to CMEs' existing frameworks. We therefore submit that CMEs should not be required establish an entirely new, duplicative framework as part of this proposed TRM framework, as that would drain resources and introduce duplication without adding much value or any additional security.

Clause 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.**

Feedback/Comments:

- We encourage a flexible and principles-based approach to for CMEs to manage technology risk in proportion to their size, complexity, and risk appetite. However, clause 1.3 (b) prescribes CMEs to studiously meet TRM requirements and leaves CMEs with limited ability to accept risk based on its

[2] CRI: https://cyberriskinstitute.org/the-profile/

size, complexity and risk appetite. To achieve the outcome of the TRM framework, it's critical that SC to adopt a risk-based approach and allow CMEs the ability to define or apply an appropriate framework based on its size, complexity and risk appetite.

Consultation Q1: 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).

Feedback/Comments:

- We would like to suggest that "SC allow capital market entities to decide its review frequency, commensurate with the size of business, and the criticality of the cybersecurity risk exposure in the local market entities, but not exceeding 3 years". For a CME leveraging a mature global framework, there is minimal value or benefit to reviewing policies and procedures annually.

Consultation Q2: 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?

Feedback/Comments:

- Local CMEs are leveraging existing group technology risk management frameworks and policies. The threshold/risk appetite has been defined across all entities including Malaysian entities.
- We would like to clarify if Q2 in the consultation paper refers to the "Board" because provision 1.3 in the consultation paper refers to the "senior management", which seems to be a contradiction.
- Regardless, SC should allow CMEs to take a risk-based approach in determining the reporting escalation process within the firm and to report only those material departures from the TRM frameworks, policies and procedures to the Board for board-level awareness/decision. The Board should be able to delegate senior management to review and approve the majority of changes in exercising day-to-day oversight for departures that are not considered material. For example, there is minimal value and benefits for reporting of all departures from the TRM Framework, policies, and procedures to Board. This approach may inundate the Board and divert their focus from more important matters. Typically, firms tend to take a risk-based approach and report material departures to the Board so that they can make a Board-level decision. Moreover, materiality thresholds vary from organisation to organisation based on its setup, nature of business, business exposure and others. The TRM framework should not prescribe the materiality threshold and the frequency of reporting. SC should provide flexibility for the respective CME to determine the threshold for reporting.

Clause 2.3: In this regard, the SC is proposing that the Board's roles and responsibilities include – (i) ensuring that the Board keeps itself up-to-update of new or emerging trends of cyber threats and understand the potential impact of such threats to the entity.

Feedback/Comments:

- Yes. The Board is kept apprised of key cybersecurity issues through meetings and they are the appropriate committee to discharge the oversight functions in relation to technology risk management. The Board should be able to delegate to senior management.
- We suggest that the local CMEs should be able to leverage their global framework, in which the group level Board of Directors has the capability and competencies to discharge the oversight function. Depending on the size, scale, nature and complexity of operations, local senior management and CISO, or delegate, could provide regular updates on general Technology Risk Management and cybersecurity matters to enable the local Board of Directors to discharge their oversight functions.

Consultation Q4: 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?

Feedback/Comments:

- We recommend that SC not mandate separate people to carry out separate activities like article 2.3(g)(i). The framework should be outcome-based and only describe high-level technology risk managements, and not require specific implementation approaches. SC should leave the implementation and management of the resources to respective CMEs so that they can determine the best way to allocate resources, taking into consideration their business size, scale and operating model. In firms with international/global presence, the functions may be separate at a global level with local oversight being provided by the local business team. The Senior Manager for Technology would be expected to cover both aspects, as long as the people doing the actual work have the required segregation and the business is also involved in managing these risks. Mandating the required resources will impact the operation overhead and the headcount is subjective because it is based on the CMEs setup and size. We would like to confirm that SC recognises that some local offices or subsidiary firms in Malaysia TRM leverage headcounts and resources from global/regional teams or intra-group affiliates.
- If the SC would nevertheless keep this requirement, we submit that there should not be a requirement for these individuals to be located in Malaysia.

Clause 2.5: (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.

Feedback/Comments:

- 2.5 (a) It should not be required for the Board to approve all aspects of the organisational chart. This level of detail should be done by senior management.
- (c) Implies the Board is required to approve strategies and measures. This should be dependent on the materiality of the decision.
- (d) Given the context, we seek clarification on the definition of the BIA and would like to understand the reason for BIA to be reported to the Board. Instead of the BIA, we submit that the Board should be made aware of business processes that are critical to the on-going survival of the entity.

Consultation Q5: 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).

Feedback/Comments:

- We recognize that this draft framework takes into account the operations of local CMEs. But given the diverse presence of international firms in Malaysia, we encourage SC to include provisions on how the TRM framework can be applied for firms with international/global presence and support and suggest that the local CMEs should be able to leverage their global framework. The local CME should be allowed to leverage and benefit from the global framework, and the senior management at group level could discharge oversight functions, as long as key matters impacting the entity are addressed by the local entity's senior managers, and Board.
- We propose the insertion of this text: "International banking groups operating in Malaysia (whether in the form of a local subsidiary or a branch) may rely on group operational risk management framework/policies with adaptions as appropriate, provided that the operational risks inherent in the local operations are sufficiently addressed having regard to the size, nature and complexity of the operations."

Clause 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.

Feedback/Comments:

- 2.6. The terms cybersecurity and technology are being referred to either interchangeably or inconsistently throughout the TRM. These terms should be used consistently so it is clear when an element refers to cyber, tech or both, supported by clear definitions.

- We suggest to include a definition of “agent” in this context, clarifying that it relates to organisations or people who are contractually representatives of the entity and can commit the entity to a course of action.

Consultation Q6: 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.

Feedback/Comments:

- CMEs typically conduct these trainings once a year or even more frequently than that (e.g quarterly for 15 minutes). SC should allow individual organisations to determine training frequency, priorities and content based on its own risk posture.
- As pointed out in Article 2, the Board has oversight roles and senior management are in charge of day-to-day operations. When it comes to cyber incident response and recovery and technology risk management, CMEs should rely on subject matter experts within the firm in line with TRM framework.

Clause 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.

Feedback/Comments:

- In defining what is "regular", we suggest that the frequency of IT audits be commensurate with the criticality of and risk posed by the IT information asset, function or process.
- We suggest that the SC clarifies that all the stated auditable areas/ activities do not have to be covered in a single audit/ review. Firms’ internal uudit teams generally adopt a risk-based approach and each of the auditable areas/ activities may have a different audit cycle, depending on the firms’ risk assessments.

Clause 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.
Clause 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 the challenge the capital market entity’s IT processes for improvement.

Feedback/Comments:

- We encourage SC to add in clause 2.8 that the CME should determine the scope of the technology audit using a risk-based approach. We would like to confirm that the "technology audit" (as mentioned in 2.7) can be conducted by the CME’s internal or external auditors, or personnel from a unit/department (i.e. RMG Operations, Risk, etc.)

Consultation Q7: 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?

Feedback/Comments:

- Audits are generally planned and scheduled throughout the year and it is typically not practical to have audit teams perform a complete review in the same period or in a year.
- SC can add a text to confirm that CMEs should determine the frequency of the IT audit and it should be commensurate with the criticality and risk posed by the IT asset/function or process. Technology auditors would possibly include internal audit resources, external auditors and control assurance work performed by teams in first line and second line, independent of the control operators.

Clause 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.

Feedback/Comments:

- Following our earlier comments in relation to legal application, in Section 3.4, the word 'guideline' has been used. Please confirm that the outcome is that these are requirements (must be met) or guidelines (should be met, but are not a requirement)?

Consultation Q8: Do you foresee any implementation issues and challenges with regards to the technology risk management framework, specifically on emerging technology that your organization 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?

Feedback/Comments:

- We recognize that this draft framework takes into account the operations of local CMEs. But given the diverse presence of international firms in Malaysia, we encourage SC to include provisions on how the TRM framework can be applied for firms with international/global presence and support. We propose the insertion of this text: "International banking groups operating in Malaysia (whether in the form of a local subsidiary or a branch) may rely on group operational risk management framework/policies with adaptions as appropriate, provided that the operational risks inherent in the local operations are sufficiently addressed having regard to the size, nature and complexity of the operations."
- By including AI and ML in the TRM, this implies that AI, ML and data governance are technology risks or issues rather than business issues. We suggest these requirements should be separated from the TRM final requirements.

Clause 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.

Feedback/Comments:

- 4.4 indicates that a project steering committee should be formed and is comprised of at least one senior representative from each business function. We submit that a representative from each business function should not be required but that instead, only the relevant/impacted business functions should be represented and the entity should determine the appropriate representatives based on the business outcome of the project the appropriate representatives. The project steering committee should oversee the project scope, resources and budget – they should not recommend changes to project team members 4.4 (b).

Clause 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

Feedback/Comments:

- We propose this text change: A capital market entity should incorporate security requirements into the system design which would enable it to carry out ~~constant~~ security evaluation, **according to a frequency determined by CMEs**, and comply with security practices throughout the SDLC in order to minimise system vulnerabilities and reduce risk exposure.

Clause 4.10: System Testing and Acceptance -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.

Feedback/Comments:

- Further clarification is needed to confirm that the rigorous system testing should be determined by CMEs and the definition of the testing.

Clause 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.

Feedback/Comments:

- Currently firms adopt automated testing as part of an overall testing strategy and the scope is as required by individual business units.

Consultation Q9: 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?

- We suggest that SC include the consideration of risk-based approach instead of all projects i.e. a risk assessment for high risk projects. A firm's SDLC framework will provide required controls for general project development activities based on the project's risk profile.

Consultation Q10: 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 organization

Feedback/Comments:

- It will be impractical to mandate a project steering committee regardless of the project size. We suggest this should be left to the discretion of each market entity. We would recommend consideration of a risk-based approach, instead of all projects, so that the project management steering committee provides oversight on programs with a higher criticality, cross departmental projects, etc.
- As an example, how will this requirement apply to agile delivery? For example, the Monetary Authority of Singapore (MAS) Technology Risk Management guidelines[3] have considered the implications of their guidelines for agile methodologies, DevSecOps and user developed changes.

Clause 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.

Feedback/Comments:

- We suggest a risk-based approach requiring change management processes to oversee material changes to the IT system (instead of any change).

Clause 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.

Feedback/Comments:

- We suggest a risk-based approach, scoping out minor changes. The current definition (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) is very broad.

Consultation Q11: 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?

Feedback/Comments:

- The TRM Framework should focus on the protection and continuation of business. In this instance, it should not make source code escrow as an explicit requirement as it is not practical. For instance, in article 4.7(c), if a firm terminates a contract, then it will no longer use the system. Hence, there is no need for the source code.

[3] MAS, 2021: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

- If the SC would nevertheless choose to keep this requirement, CMEs should be given the flexibility to decide on the appropriate approach based on risk and on the accessibility of the source codes for critical systems. It should not be a mandatory requirement and be required to enter into source code escrow agreements as this would increase the cost of transaction.
- We ask escrow agreements are not required for intra- software.

Consultation Q12: 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?

Feedback/Comments:

- Implementing a logging facility can be difficult when regulator applications are involved which are required to be hosted at a firm's premise. The applications and databases are built from a standard framework. Customization of such applications per individual firm logging technology solution would be a challenge as it will likely deviate from the standard framework and applications provided to firms cannot always be altered.
- Moreover, on logging facility, we encourage SC to add a text that articulates that CMEs should determine their log retention strategies and archival requirements based on their operations
- For article 4.13, we would like to clarify that multifactor authentication is a security control and not a deterrent measure. Moreover, two factor authentication is a subset of multifactor authentication. The examples in 4.13 should be removed for accuracy and also to keep the document timeless as approaches may evolve in the future.

Clause 4.19: Patch Management and Technology Obsolescence: 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.

Feedback/Comments:

- 'A proper patch management process would also ensure that a capital market entity's IT systems are not obsolete.' We want to highlight that the action of patching does not mean that a system is not 'obsolete'.

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

Feedback/Comments:

- The word 'those' needs to be clarified. We suggest to rephrase to "Security vulnerabilities that are published after a hardware or software's end of support date should be assessed and monitored as to the potential risk of them being exploited."

Consultation Q13: 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?

Feedback/Comments:

- For article 4.16(c), we would like to flag that firms take a risk-based approach and would only flag high risk analysis results to the senior management. There is little value in sharing all analysis results and having them approved by the senior management. We propose that SC remove this prescriptive requirement.

Consultation Q15: 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?

Feedback/Comments:

- For article 5.8(g), we seek clarification on the definition of detrimental risk.

Clause 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.

Feedback/Comments:

- We would like to confirm that independent third-party report such as SOC2 and ISO27001 could be leveraged by CMEs when assessing third-party service provider.

Clause 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.

Feedback/Comments:

- 4.38 Paragraph should be moved to a 'logging and monitoring' requirement or clarified as to how this applies to data centre management.

Clause 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.

Feedback/Comments:

- '4.41 A capital market entity's DRP should consist of...'
- Can the SC clarify the impact of the word 'should' on the application of this requirement? (i.e. is this a recommendation or a must requirement?)

Consultation Q16: 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?

Feedback/Comments:

- For articles 4.34(a) and 4.35, many firms leverage data center risk assessment (DCRA) conducted by internal global or international teams that are independent from the operations team, and others may rely on external assessors. These two approaches provide the same level of objectivity for the DCRA. As mentioned in response to Q4 and Q5, we encourage SC to recognize arrangements within global firms.

Consultation Q17: 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?

Feedback/Comments:

- For article 4.42, we seek confirmation that SC allows firms to take a risk-based approach. There are contractual agreements for critical third-party service providers to ensure availability and business recovery objectives for information assets.

Clause 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.

Feedback/Comments:

- Due to complexities in confidentiality and/or co-ordination, participation in or joint ITDR testing with the technology service provider may be challenging. We suggest SC to remove the requirement of 5.3. and allow CMEs to decide whether to "participate in the technology service provider's BCP and IT disaster recovery exercise or conduct joint testing with the CME" on a risk-based approach.
- We also suggest to focus instead on reviewing technology service provider ITDR test results to ensure that ITDR is adequately implemented.

Clause 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 and 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.

Feedback/Comments:

- We would like to confirm that independent third-party report such as SOC2 or ISO 27001 could be leveraged by CMEs when assessing third-party service provider.

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

Feedback/Comments:

- 'As per the above comment the 'service level agreement' referred to here appears to be used to refer to the 'services agreement' generally.
- See comments in respect of Q18 re the need to specify the scope of the service providers in question and apply a materiality test.
- Re (f), many technology service providers are unwilling to share the results of their BCP tests.
- Re (h) very few technology service providers will agree to an "immediate notification" obligation in relation to a technology and cyber incident as they need time to investigate and validate the incident and work out which customers are impacted. Most will only agree to notify "without delay" or "as soon as reasonably possible and in any event within [24 / 48 / 72] hours of becoming aware of the incident.

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

Feedback/Comments:

- Can the SC please clarify as to whether the intent is to cover general 'availability' of data held by service providers (which would be governed by for example the relevant service level in the agreement) or if it means access to critical data in a disaster or insolvency event (which is a BCP / DR issue).

Consultation Q18: 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?

Feedback/Comments:

- We encourage SC to allow CMEs to take a risk-based approach for articles 5.2 and 5.3. CMEs have provisions in their contracts to require critical suppliers to maintain robust internal exercises that covers BCP and IT disaster recovery. In terms of joint testing with technology service providers, CMEs also take a risk-based approach for this given the resources needed for such testing and we urge SC to tweak article 5.3 to "The capital market entity should develop their risk-based framework on when to require **critical third party service providers** to participate in ~~the technology service provider's BCP and IT disaster recovery exercise or conduct~~ joint testing with **the CME**." Technology service providers which are not providing or supporting critical systems should be excluded from this requirement since there is limited risk and impact.
- We would ask that this requirement be defined for true third-party service providers, not intra-group arrangements, and allow the CMEs to establish its own requirement on a risk-based approach. In addition, we suggest SC to remove the requirement of 5.3. and allow CME to decide to "participate in the technology service provider's BCP and IT disaster recovery exercise or conduct joint testing with the CME" on a risk-based approach.
- For article 5.8, CMEs would like to confirm that the factors listed are recommendations and CMEs can take a risk-based approach and determine their due diligence framework during onboarding or during the length of service provision. We propose the following tweak to the article: "A capital market entity should conduct adequate due diligence **of their** ~~prior to selecting a~~ technology service provider and ~~conduct periodic assessment on the technology service providers'~~ **their** capabilities during the contract period.
- For article 5.12, we note that the framework requires firms to conduct a comprehensive risk assessment prior to cloud adoption. We would like to confirm that in the instances of PaaS adoption, the assessment is expected to be performed at the platform level only, and not for each and every application hosted on that platform.
- We note 5.12(g) raises risks of "vendor lock-in and portability or interoperability solutions" in cloud risk assessment. We support greater efforts towards increased and improved interoperability and portability. But currently, the concepts of interoperability and portability has significant technical limitations. Challenges around portability include: a) technical complexity introduced into cloud environments; b) variation based on cloud service type (SaaS, PaaS, IaaS); c) loss of differentiated service benefits; and d) lack of comparable services to achieve portability. Hence, given that portability/interoperability are still new concepts, we encourage SC to remove the terms

"portability" and "interoperability". Currently, there are discussions at the Basel Committee on portability issues and we encourage SC to closely follow the consensus reached to avoid policy fragmentation. If the concern is vendor lock-in, this issue can be mitigated through contractual agreements with the service provider.

- On 5.12(j), the text "timely measures" is vague and introduces uncertainty. Moreover, given the evolving cybersecurity best practice and standards, we propose removing the prescriptive text. We recommend this amendment: "~~Constant~~ ability to meet regulatory requirements ~~and timely measures of security standards~~ on cloud computing"
- For 5.16(h), we recommend SC to change it to "a clearly defined arrangement that a technology service provider should notify CMEs as soon as possible when the technology service provider determines that it has experienced a technology and cyber incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours". Reporting of incident of non-material impact would lead to reporting fatigue and doesn't necessarily enhance cyber resilience. For example, the Office of the Comptroller of the Currency, Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation's Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers issued in 2021 requires a bank service provider to notify each affected banking organization customer **as soon as possible** when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

Consultation Q19: 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.

Feedback/Comments:

- We would ask SC to exclude intra-group entities and allow the CMEs to establish its own requirement on a risk-based approach -dependent on the importance and the criticality – to conduct regular reviews on true third-party service providers.

Consultation Q20: 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?

Feedback/Comments:

- We recommend that SC remove the requirement for firms to have a standalone and separate Cybersecurity Framework because of duplication with the TRM framework. The TRM framework that a CME has, covers the governance and controls of cybersecurity matters. Hence, there is no need for a separate framework. We propose SC to emphasize of having cybersecurity governance and controls specified within the Technology Risk Management framework instead. Firms may refer to industry risk assessment framework such as the Financial Sector Profile (mentioned above) which allows an organisation to diagnose cyber risk and apply relevant standards and best practices to appropriately manage that risk. The FSP adopts a tiering mechanism that serves as a scaling device to customise the Profile based on an individual institution's risk and activities.
- For article 6.7, we recommend to reflect a risk-based approach: "capital market entity should proactively monitor any cyber ~~event~~ **threat**, detect any anomalous activity and conduct analysis on any detected event **that has a material impact**".

- For article 6.14, we recommend for SC to leave it to CMEs to decide what to include in the cyber threat analysis report. The current requirement to include "cyber threat trends and statistics, incidents grouping by type of attack, target and source of IP addresses" is too prescriptive and are not relevant to senior management.
- For article 6.15, we would like to confirm with SC that international firms' global resources and centralized support is taken into consideration when reviewing a CME's expertise. For international firms, it is common to have high quality teams of subject matter experts responsible for cybersecurity threat analysis, cyber defense and others. We recommend removing this text and allowing firms to determine the best structure for strong cyber capability and allow CMEs with a global presence to leverage their global framework given their expertise across the globe.
- Lastly, we suggest SC to allow CMEs to take a risk-based approach to exclude the threat and risk that are not material (e.g. article 6.7).

Clause 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.

Feedback/Comments:

- We hope the SC can clarify a cybersecurity function's responsibility with respect to the interoperability and usability of business information and client data. While these are important characteristics, they are generally the result of business decisions supported by technology.

Clause 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.

Feedback/Comments:

- Cyber event refers to an occurrence that happens or takes place. By using the term here, 'continuous surveillance for cyber events' it would imply that CMEs are continuously looking for a past event. We suggest to replace "of any cyber event" by "for cyber events".
- If the aim is to identify and detect, the term cyber threat should be used.

Clause 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.

Feedback/Comments:

- We request that CMEs are allowed to determine the best approach to reporting the cyber threats and that the content is not prescribed.

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

Feedback/Comments:

- Our view is that a post incident review should be performed based on materiality. Performing a review for every incident does not deliver significant value.

Clause 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.

Feedback/Comments:

- We suggest the SC confirms the definition of a 'Compromise Assessment' and its likely content.

Clause 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.

Feedback/Comments:

- Can the SC confirm that based on separate guidance for a red team under Section 6.29 that the use of the words 'mimic an experienced hacker' that this means that this test is not a threat intelligence led or a red team.
- For 6.23, we encourage that SC take a risk-based approach to penetration testing and allow firms to determine the frequency of penetration testing should be based on factors such as system criticality and the system's exposure to cyber risks, which is also the approach taken by financial regulators such as MAS[4].
- In addition, we encourage SC not to prescribe the requirement for CMEs to conduct penetration testing "When the capital market entity's critical system undergoes major changes or updates."

Clause 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.

[4] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

Feedback/Comments:

- The Management of Data section should be excluded from the TRM Framework, in line with most other technology risk management guidelines in other leading jurisdictions (e.g. APRA[5]). The inclusion of data governance/management as part of a TRM implies that this is a technology issue rather than a business issue.

Consultation Q21: 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 objectives?

Feedback/Comments:

- For article 6.22, it is common practice for CMEs with global presence and support on technology to leverage the compromise assessment exercise performed by the global/regional experienced and qualified professionals/team. Moreover, the compromise assessment is a constant effort and it is not a one off assessment. Similar to our comments earlier, we would like to confirm with SC that such approaches are acceptable.
- For article 6.23, the frequency of penetration testing should be determined based on factors such as system criticality and the system's exposure to cyber risks. For systems that are directly accessible from the Internet, the FI is expected to conduct penetration testing to validate the adequacy of the security controls at least once annually or whenever these systems undergo major changes or updates. We encourage SC to take a risk-based approach similar to MAS's approach that CMEs could decide penetration testing based on factors such as system criticality and system's exposure to cyber risk and attach greater importance to systems that are directly accessible from the Internet[6]. We encourage SC to not prescribe the requirement to conduct penetration testing when the CME's critical system undergoes major changes or updates. We propose the removal of this text: "~~When the capital market entity's critical system undergoes major changes or updates, penetration testing exercise should also be carried out~~."
- For article 6.24, we recommend SC to tweak the text to include the term "internal or external": "A CME should ensure the penetration testing exercise process is documented and performed by experienced and qualified **internal or external** 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." Firms should also be allowed to determine their conditions on what constitutes as "experienced and qualified".
- For article 6.26, we propose the following revision to provide clarity that the CME will determine the frequency of testing based on their operational needs: "A capital market entity should establish a comprehensive business continuity plan and ~~regularly~~ **determine a frequency** to test the effectiveness of its cyber incident response and recovery plan based on current and emerging cyber threat scenarios."
- For article 6.27, we would like to clarify that cyber simulations or cyber drill exercises are conducted based on specific scenarios. The involvement of the stakeholders may vary and is dependent on the scenario planned. We propose the language to be revised to "A capital market entity should ensure

[5] APRA, 2013: https://www.apra.gov.au/sites/default/files/CPG-235-Managing-Data-Risk.pdf
[6] MAS, 2021: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

the simulation exercise is conducted with involvement from key stakeholders such as 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 **where appropriate**." For internal simulation exercises, we propose that SC refine the provision and enable firms to take a risk-based approach and the scope of the adversarial attack simulation exercise should only limited to critical systems/applications so that it is not overly burdensome. Similar to our comment for article 6.24, we recommend SC recognises adversarial attack simulation exercises carried out by either the CMEs' own internal qualified and experienced professional/teams or external vendors.

- For article 6.29, given that due to the nature of red teaming, the Security Operations Center is not aware of a test being conducted. We would therefore like to clarify that CMEs do not conduct red teaming exercises on a third-party's infrastructure as it may be construed as a malicious act. Instead, third-parties conduct their own red teaming exercises. Therefore, we recommend the removal of article 6.29.

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

Feedback/Comments:

- We would welcome more guidance on the requirements around the gap analysis and what will be the scope of the controls for the analysis.

Clause 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.

Feedback/Comments:

- We suggest SC confirm which systems are in-scope of 7.14, so that compliance with the regulatory framework can be determined by the appropriate service owners.

Clause 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.

Feedback/Comments:

- It may not be feasible to force 'empty a recycle bin', particularly for a BYOD device. We hope the SC can clarify the expectation with respect to this statement.

Clause 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.

Feedback/Comments:

- We suggest that this section should also specify a degree of controls commensurate with the sensitivity or the data or similar language - i.e., should apply to critical or sensitive data as determined by the CME, not for example any metadata or incidental data that is not sensitive in any way.

Clause 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.

Feedback/Comments:

- We submit that this section should also specify a degree of materiality – i.e., should apply to critical or sensitive data, not for example any metadata or incidental data that is not sensitive in any way.

Clause 7.24: For the purposes of submission of data to the SC pursuant to SC's requirements3, 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
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.

Feedback/Comments:

- Having one person responsible for all data submissions to the SC is impractical. The person responsible will depend on the submission.

Consultation Q22: 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?

Feedback/Comments:

- For article 7.5, we refer back to our response in Q4 about the appointment required in 2.3(g).
- As pointed out in Article 2, the Board has oversight roles and senior management are in charge of day-to-day operations. For data management, CMEs should rely on subject matter experts. For article 7.6, we would like to seek confirmation that CMEs can take a risk-based approach and

information provided by CMEs to the Board in Board meetings is considered as training. SC should allow individual organisation to determine training frequency, priorities and content based on its own risk posture.

- For article 7.9, the statement “A capital market entity should ensure that there is no duplication or overlaps recorded in the data set on a best effort basis” is too broad. There are situations where data is deliberately downloaded offline for processing (e.g., data analysis) and the offline version is kept to support the data analysis (i.e., duplicated data). Typically, such risk of duplication is addressed by ensuring that firms have clearly defined systems of record which serves as the golden source for any major processing. Given that the concerns for duplicated data are accuracy and consistency issues, and firms are already required to maintain good data quality, including ensuring accurate and consistent data under article 7.8(a) and (d), it appears that article 7.9 is duplicating article 7.8. Hence, we recommend removing article 7.9.
- The overall requirements in article 7.11 are onerous and it would entail a large-scale project plus significant overheads to maintain on an ongoing basis. Other comments for article 7.11 are:
  - 7.11(a) we suggest to remove ambiguous terms like “complete and updated” and simplify the statement to: "Maintain an inventory of all information assets including data classification and risk across the capital market entity".
  - 7.11(d) on implement clear desk policy is prescriptive and we suggest removing it. Regulators typically put in place high-level principles around integrity and confidentiality and allow CMEs to determine their approaches.
  - As the CMEs will determine the definition of critical data, 7.11(e) can be tweaked to "Review audit logs or trails particularly on access to critical data**, as determined by the capital market entity,** to identify anomalies or abnormal activities."
  - 7.11(g) requiring an annual gap analysis on data and information assets processes and controls is prescriptive. CMEs typically take a risk-based approach and controls may differ for different organizations. Hence, we recommend the removal of this article.
  - Similar to Q1, we would recommend SC to allow CMEs to decide their review frequency as needed for 7.11(g), commensurate with the size of business, and the criticality of the cybersecurity risk exposure. For a mature company leveraging a global framework, there is minimal value and benefit to review policies and procedures annually.
  - We propose removing article 7.11(i) as there are industry best practices and standards that cover data management that CMEs leverage.
- For article 7.16, we suggest rephrasing the statement to "A capital market entity should determine the appropriate retention period to archive its data, **including all the log files** based on the usage requirement or its criticality for its data".
- Data management policies and procedures are typically driven based on type of data and data ownership. Related process around the management of data section should be considered separately and not within the Technology Risk Framework. Where data policies are typically closely knitted with the business process, technology typically acts as the custodian of the data. The inclusion of data management inclusion submission of data as part of a TRM implies that this is a technology issue rather than a business issue.

Consultation Q23: 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 objectives?

Feedback/Comments:

- CMEs find that certain sub-sections of section 7 are currently too specific and prescriptive and should be either removed or re-worded as examples or guidance. Additionally, there are new roles being defined and created by the regulations which may be difficult for some companies to implement due to size and organisation structure. As an example, 7.24(b) is asking for a "Head of Reporting" to be appointed and such roles typically does not exist for large-scale organisations. We recommend SC to remove the requirement for firms to appoint a "head of reporting from among the senior management" or tweak the text in 7.24 (b) to "capital market entities will be responsible for…"
- Similar to above, submission of SC related data should be not included as part of the Technology Risk Framework. The inclusion of data management inclusion submission of data as part of a TRM implies that this is a technology issue rather than a business issue.

Clause 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.

Feedback/Comments:

- 8.1 Compliance Process - Notification for Technology-Related Application
- We suggest that the word 'Notification' is not appropriate given that there is no notification requirement. We suggest it be removed.
  We suggest the SC provides more clarity on the definition of 'major' as well as who will be considered as an independent party. Having an independent party perform a readiness assessment in all cases does not appear practical and will typically be performed by the delivery team.

Consultation Q24: Do you think the minimum requirements listed in paragraph 8.1 are sufficient to assess readiness? Please provide specific reasons for your views.

Feedback/Comments:

- For global firms with local offices or subsidiaries in Malaysia, they often rely on readiness assessment performed by an independent team from the global/regional office, taking into account the location specific aspects. While some firms engage an external independent party to perform readiness assessment on technology related service/enhancement on its critical systems, it may not always be feasible for other firms due to additional overhead costs and the risk of exposure for

the security and confidentiality. Hence, we recommend SC allowing firms to determine the approach that is best fit for them.

- We recommend SC to allow CMEs to define its own framework given the robustness of the Technology Risk Management framework in areas around risk governance, SDLC, project management and change management etc. Our members do not see value of an independent assessment given the robustness of our internal controls.

Consultation Q25: 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.

Feedback/Comments:

- We recommend that the AI guidelines be put down in a separate document and not as part of the TRM framework, in line with the practice in most other jurisdictions.
- We also recommend SC to narrow down the scope of AI and ML more specifically to client or market impacting AI/ML (e.g. client credit checks), while excluding when it is used for enhancing internal operational efficiency.

Section	Citation/ Text from the Document	Feedback
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.	The Board should be able to delegate the accountability of the action and outcomes of AI and ML to the Senior Management.
B. Transparency and Explainability	1. Transparency, explainability, and traceability are key requirements for trustworthy AI and ML.	We propose that SC break this down into two parts in line with the approach in other jurisdictions: • Transparency and Explainability (the need to be able to understand and explain the outcome to be transparent) • Traceability and Auditability
	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—	We propose that point 2a be included under "Accountability" so that Explainability can be focused on the outcomes of AI. Point (a) seems to be more suitable under Accountability as it relates to Accountability section point 2.

	(a) the process, i.e. governance of AI; and (b) the outcome of the AI application i.e., reasoning of the algorithmic decision.	
C. Fairness and Non-Discrimination	Fairness and Non-Discrimination	We propose to simplify he principle by just calling it Fairness
PART C: GLOSSARY OF TERMS		Propose that the document include the definitions of some key terms, leveraging existing internationally-recognised definitions as to avoid fragmentation: • AI • ML • AI and ML systems • AI applicants • AI-assisted decision • AI and ML-driven decisions (how is this different to the above)

We would welcome the opportunity for further engagement and remain at your disposal for any further questions you might have. Do not hesitate to reach out to us at lvanderloo@asifma.org or phone: +65 6622 5972.

Sincerely,

Laurence Van der Loo
Executive Director, Technology & Operations
Asia Securities Industry & Financial Markets Association