RESPONSE TO CONSULTATION PAPER

Consultation topic:	Technology Risk Management Guidelines
Organisation:	Asia Securities Industry & Financial Markets Association (ASIFMA)
Contact number for any clarifications:	Laurence Van Der Loo, Director (852) 2531-6511 Clement Kwan, Analyst (852) 2531-6519
Email address for any clarifications:	lvanderloo@asifma.org ckwan@asifma.org
Confidentiality	
I wish to keep the following confidential:	

Section 1: General Comments

- *ASIFMA welcome the opportunity to respond to the draft Guidelines on Technology Risk Management (TRM) and we are pleased to set out our comments in what follows.*

- *To encourage the adoption of certain emerging technologies, a less-prescriptive approach will allow financial institutions (FIs) flexibility to determine and design appropriate technologies, guidelines, controls and frequency that best meet business needs and better align with the supervisory objectives at the discretion of the FIs.*

- *Issuing specific local requirements pose challenges to FIs that operate in multiple jurisdiction and markets. Implementing different standards will also create technical challenges and economic impact for FIs to establish controls. To achieve effectiveness, multinational FIs create consistent frameworks and standards that span across different jurisdictions. This drives effective reduction in risk to FIs in accordance with global nature of the threat landscape, while still meeting regulatory requirements. We suggest that MAS cooperate with comparable foreign regulators to agree common standards for the regulation of technology risk so that FIs that operate across borders have the benefit of a seamless or at least aligned regulatory structures or that it is possible to rely on substantively equivalent foreign regulatory regimes (e.g. of home jurisdiction regulators).*

- *We suggest that MAS consider allowing FIs to substitute and leverage existing industry standard technology risk management frameworks to meet the MAS's supervisory requirements. Allowing FIs to demonstrate compliance with the use of existing industry framework increases efficiency by enabling FIs to focus on control improvement rather than competing framework implementation.*

- *To ensure MAS's supervisory requirements are met in a considered and globally-harmonized manner, we recommend that MAS allow a two-year phase-in period so FIs of different sizes have sufficient time to comprehensively identify material gaps, and establish and implement additional controls where required.*

- *Given the considerable number of footnotes in the consultation paper, we suggest at glossary for definition of terms to be utilised instead.*

- *The definition of information assets has been updated with the inclusion of End User Application (EUA) and data. The applicability of all Technology Risk Management (TRM) guidelines across this broad definition requires further clarification.*

- *There are some potential challenges in implementation for smaller local entities that are part of a significantly larger and complex global entity.*

Section 2: Application of the MAS Technology Risk Management Guidelines

Section 3: Technology Risk Governance and Oversight

- ***3.1.2 Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats.***

  While the organization should have members with the knowledge to understand and manage technology risks, the Board should have access to the knowledge and expertise needed to manage this risk. It is not clear from clause 3.1.2 if the requirement is for the Board to change the composition of its members to include someone with this specific skill set. We recommend that the focus should be on access to the right knowledge and expertise, instead of requiring changes to the composition of the Board.

  Indeed, depending on the size and type of the local business, it may be disproportionate to have a tech expert on the Board and it may be more appropriate for the Board to delegate to the relevant Senior Management including for example regional management for Tech.

- ***3.1.5 The Board of directors or a committee delegated by it, is responsible for:***
  (c) appointing a Chief Information Officer, Chief Technology Officer, or Head of Information Technology with the requisite expertise and experience, to be responsible for Information technology and computer systems that support enterprise goals;
  (d) appointing a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme

  - *We would like to bring to the MAS attention that generally, the board of directors does not appoint these roles. Instead, this is usually the responsibility of the senior management of an organization. Also, individuals that are accountable for information security and information technology can have many titles. Thus, instead of listing a number of titles, we suggest MAS consider outlining the role attributes (e.g., expertise, experience, accountable, empowered) rather than the titles.*

  - *It should be up to FI's board of directors to designate/delegate relevant committees where necessary, instead of just one committee. Suggest rephrasing section 3.1.5. to "The board of directors or a relevant committee delegated by it, is responsible for…"*

  - *There is overlap with the MAS proposal for Individual Accountability and Conduct (IAC). In the draft IAC Framework, it is clearly indicated that these senior persons can be located outside Singapore and can dual/triple hat these roles and we request clarification on this matter.*

- *With respect to section 3.1.5(d), we would like to seek clarification on the required competence level, and if there are any expectations on the level of experience and industry certifications required within the technology and cyber security risk domains.*

- ***3.1.5 The Board of directors or a committee delegated by it, is responsible for: (h) undertaking regular reviews of the technology risk management strategy for continued relevance***

  In line with our suggestion for clause 3.1.2, we suggest it should be clarified that the focus is for the board to have access to necessary knowledge and expertise, instead of changing the board's composition.

- ***3.2.1 The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards to manage technology risks and safeguard information assets in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape***

  We would like to seek clarification from the MAS on what would be the recommended industry standards. For example, some of the industry standards that could be mentioned in the guidance are NIST Cybersecurity Framework for Cybersecurity framework or ISO 27017/18, SOC1/2/3 for Cloud. The recommended industry standards would be especially useful for emerging technologies such as API.

- ***3.2.3 Compliance processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner***

  The required 'monitoring and review' processes could be carried out by any independent team with the relevant subject matter expertise and not necessarily the Compliance team. We recommend that the MAS accordingly changes this requirement such as – "Monitoring and Review processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner. These monitoring and review processes could be carried out by any independent team with relevant subject matter expertise such as an internal control unit or compliance."

- ***3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes.***

  We recommend that the requirement of registration by an FI of all information assets, establishment of its ownership and the roles and responsibilities of the staff managing the information assets should be limited to the information assets which are categorised as 'material' based on its security classification or business impact criticality. Otherwise, we are concerned that documentation and risk management requirements may lead to *disproportionately high operational and compliance burdens for FIs. This is particularly so for global FIs.*

Our understanding is that this requirement also applies to any shared information assets that may be critical for the delivery of services. This should be clarified.

MAS should clarify if this requirement also applies to any shared information assets not limited to those within the FI's environment (e.g. on cloud infrastructure).

We understand that MAS has expanded the definition of information assets as compared to 2013. It will be helpful to provide clarity on inventorying data as information assets. Would this include both hard copy and soft copy formats? (foot note for 3.2.1 , Information assets include data, hardware and software)

- ***3.4 Management of Third Party Services***

  It would be helpful if MAS can provide examples of the type of certification and accreditation which are recognised by MAS. For industry recognised certification and accreditation, these would include ISO 27001, SOC1, SOC2, NIST.

- ***3.4.2 Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognised by the industry, before entering into a contractual agreement or partnership with the service provider.***

  We encourage MAS to allow FIs to adopt separate but comparable due diligence processes applicable to FinTech firms given that the FinTech industry landscape is rapidly evolving. Traditional third party due diligence considerations such as track record may not fully apply to FinTech firms. For example, the due diligence performed for FI's partnership with Fintech start-up firms to develop a Proof-of-Concept innovation solution (without customer information) will differ from the FI's engagement of a third-party service provider for outsourcing arrangement.

- ***3.5.2 Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who has access to the FI's data and systems, should be performed to minimise this risk.***

  The requirement of a background check on personnel, who has access to an FI's data and systems could represent a significant task; especially for FIs who have a large global footprint or where the technology processes or systems are sub-outsourced. We would therefore recommend for the background check requirement to be limited to all personnel who has access to critical data or information assets in the production and data recovery environment. This combined with a strong Operational Infrastructure Security framework (section 11) should minimise the risk of theft of confidential, sabotage of systems or fraud by staff, contractors or service providers.

  We, therefore, recommend that para 3.5.2 be changed to – "Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and *services providers, is considered one of the key risks to an organisation. A background check on personnel, who need access to the FI's sensitive and confidential data or information assets in the production and data recovery environment, should be performed where permitted by law to minimise this risk."*

- ***3.6 Security Awareness and Training***

  - *It may be unreasonable to require "all service providers" to have their staff participate in the FI's training program due to the fact that service providers generally have many customers. Part of the due diligence process for new vendors should involve determining that they have a suitable security awareness program for their staff.*

  - *Generally, a service provider has clients from the same industry – which would face the same set of risks. Hence it would alternatively be reasonable for the MAS to expect that the vendor staff should be trained on suitable security awareness program. Additionally, para 3.5.1 requires that service providers have the requisite level of competence and skills to manage technology risks. So, training would be useful to make sure they are aware of the technology risks.*

  - *Further clarification is needed on whether this can be global training programme with a Singapore supplement*

Section 4: Technology Risk Management Framework

Member feedback

- ***4.1.1 The FI should establish a risk management framework to manage technology risks in a consistent and systematic manner. As part of the framework, effective risk management practices and internal controls should be instituted to achieve data confidentiality (including footnote 5) and integrity, system security and reliability, as well as resilience in its IT operating environment.***

  - *Suggest that this paragraph include proportionality and we ask the MAS to consider this drafting language: "The FI should establish a risk management framework consistent with the level of risk and complexity inherent to its business to manage technology risks…"*
  - *The technology risks terminology varies across chapters. For example - In section 7.1, there is reference to "stability of the production IT environment" but it is not referred to under chapter 4 (para 4.1.1). Service availability represents a key tech risk and we believe that both Information security and system availability should be specifically referenced in the context of technology risk management. We acknowledge that this could potentially be inferred from "Data confidentiality and integrity, system security and reliability, as well as resilience in its IT operating environment." However, we believe that for the sake of consistency and clarity, stability of the production IT environment should also be captured in chapter 4.*

- ***4.1.3 (d) - Risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, systems, environmental or operating conditions; and report key risks to the board of directors and senior management***

  We suggest to add a qualifier where risk that customers exposed within the "scope of service provided" by FIs.

- ***4.2.1 The FI should identify the threats and vulnerabilities, as well as the risks posed to its IT environment, including information assets that are maintained or supported by third party service providers.***

  The risks posed to information assets that are maintained or supported by third party service providers should be assessed in an appropriate way.

- ***4.4.1 For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of the information assets and the level of risk tolerance.***

  We suggest that paragraph 4.4.1 be amended to include the criticality of service as follows:

  a. For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of information assets, level of risk tolerance and the criticality of service.

- ***4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, the FI should give priority to threats and vulnerabilities with a higher risk rating, such that those which could cause significant harm or impact to the FI's information assets and operations***

  Suggestion to reword for clearer understanding: "The FI should identify the threats and vulnerabilities, as well as the risks posed to its IT environment".

- ***4.4.5 The FI should refrain from implementing a system or acquiring an IT service where threats to the safety and soundness of the FI cannot be adequately controlled and the risks out-weigh the benefits.***

  The decision to refrain from implementing or acquiring a system is not only limited to threats to the safety and soundness of an FI. This should be a conscious decision derived through a risk assessment to determine if residual risks can be effectively mitigated to an acceptable level. Suggested edits below.

  "The FI should refrain from implementing a system or acquiring an IT service outside the FI's risk appetite or tolerance limit".

- ***4.4.6 To mitigate risks, the FI could consider taking insurance cover for various insurable technology risks, including recovery and restitution costs.***

  As insurance cover does not mitigate the risk, but only transfers the financial impact of the risk event to the insurers, we suggest para 4.4.6 be mentioned as a risk transference approach and not as a risk mitigation.

Section 5: IT Project Management and Security-by-Design

Member feedback

- ***5.1.2 Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.***

  - *We suggest that MAS refrains from prescribing how FI's should run IT projects based on the prescriptive nature of 5.1.2 and 5.2.1. We suggest that this should be left to FI's to determine who is required for such projects within their organisation.*

  - *FIs may define and use Agile framework that applies to both Project Lifecycle and Software Development Lifecycle (while ensuring that secure coding, source code review and application security standards are applied during Agile Software Development). By requiring the use of Waterfall project management and System Development Lifecycle (SDLC) framework for agile projects, this would negate the commercial gains FI seek with Agile, such as reduction of risk, increase quality and faster solution delivery time.*

- ***5.1.4 As project risks, such as an ill-defined project scope and poor cost management, can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle. For large and complex projects that impact the business, the FI should report significant project risks to its board of directors and senior management.***

  - *For IT project management, we would assume it is applicable to those IT projects that will follow the SDLC methodology. Project management should not mandate Agile Development to adhere to the SDLC way.*

  - *We would like to seek clarification on what is meant by "large and complex projects".*

  - *Suggestion to use terminology which provide guidance for project-centric and product-centric delivery alike.*

- ***5.3.4 A source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI.***

The feasibility of having a company providing its intellectual property to its customers is questionable.

Applicability of escrow agreement guidelines across all critical software vendors requires further clarification as vendors like SAP, Oracle may not agree with such an agreement.

The stability of the vendor, as well as the criticality of the software should also be considered in the decisions to require a software escrow agreement. For example, many FIs rely on critical software from Microsoft, however it will not be a good use of time and resources to require software escrow agreement in this case.

Smaller scale IT service providers tend not to have escrow agreements due to cost and intellectual property considerations. MAS may like to consider providing more flexibility in choosing alternative mitigating measures in the absence of an escrow arrangement from such service providers (e.g. adequate contractual clauses with third party contracts).

In addition, we suggest MAS clarifies the scope of the agreement as some of the front end digital technologies require open source code, hence implementing escrow would not be relevant.

We also want to seek clarification required for type source code escrow agreement, especially for propriety software from vendor verses software that an FI purchases for use in-house.

- ***5.4.2 The security-by-design principle requires the design and implementation of security in every phase of the SDLC in order to develop an IT system that is reliable and resilient to attacks. This includes incorporation of security specifications in the system design, continuous security evaluation and adherence to security practices throughout the SDLC. The principle should be adhered to such that security requirements are clearly specified in the early phase of system development. The security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.***

    - *Security requirements may vary depending on the threat and risk to information assets and we suggest that MAS does not mandate these minimum-security requirements in all development projects.*

    - *Suggestion to reword that "The security requirements are commensurate with project scope and complexity…."*

- ***5.4.3 The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.***

The wording "involve IT security function in each phase of the life cycle" seems too prescriptive. We suggest MAS to consider using "where relevant, the IT security function should be involved as part of the SDLC framework".

- ***5.5.1 Functional requirements, key requirements such as system performance, resiliency and security controls, should also be established and documented.***

  We respectfully propose amending paragraph 5.5.1: "Functional requirements, key requirements such as system performance, resiliency and security controls, should also be taken into account"

- ***5.7.4 The FI should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing system to validate that the system continues to function properly after the changes have been implemented.***

We request more clarity on the scope of change that requires regression testing, and if it is the intention it will apply to all functional changes. Generally, executing regression test is a standard approach for major functional changes and is non-standard for small enhancements (e.g. minor bug fixes which would be also considered as change) and we recommend this is reflected in 5.7.4.

- ***5.8.2 Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI's policies, procedures and standards, and achieve the project objectives.***

  - *It would be helpful if MAS can provide clarification on the independent quality assurance function. Would this include members within the Quality Assurance function of the project phase?*

  - *Suggestion to use terminology which provide guidance for project-centric and product-centric delivery alike. Suggested edit as follows:*

    "Quality assurance should be performed by an independent quality assurance function to ensure ***technology delivery*** *activities and deliverables comply with the FI's policies, procedures and standards, and achieve* ***the delivery*** *objectives."*

  - *Can MAS please clarify the scope (i.e. all system build-outs or only critical / major systems?*

Section 6: Software Application Development and Management

Member feedback

- ***6.1.1 Software bugs or vulnerabilities are typically targeted and exploited by hackers to compromise an IT system, and they often occur because of poor software development practices. To minimise the bugs and vulnerabilities in its software, the FI should establish standards on secure coding, source code review and application security testing, and ensure the standards are applied and adopted throughout the SDLC.***

  We propose that the standard should be risk based.

- ***6.1.6 The FI should ensure issues and software defects discovered from the source code review and application security testing, which affect the confidentiality,***

integrity and availability of information and the IT system, are tracked and remediated before production deployment.

We would recommend for the remediation requirement to be based on materiality as some software defects may not affect the confidentiality, integrity and availability of information and the IT system.

For issues and software defects discovered from the source code review which affect the confidentiality, integrity and availability of information: We recommend that remediation is performed on ***a risk based approach*** *rather than expecting all software defects to be remediated before production, given that certain software defects come with mitigation controls which manage risks to an acceptable level.*

- ***6.3.2 The FI should enforce segregation of duties for the development, testing and operations functions in its DevOps processes, and ensure the respective DevOps activities are logged and reviewed in a timely manner.***

  MAS should consider allowing alternative controls that mitigate risks when segregation of duties control is not in place within DevOps teams as that may undermine the value the methodology brings. An example of this would be automating releases and aspects of testing. Strict segregation of duties between development, testing and operations would stop the efficient flow of information across the lifecycle of service that DevOps is meant to deliver.

- ***6.4 Application Programming Interface Development***

  This section applies to direct application-to-application interfaces using request-reply internet-based standards. Clarification is required if the browser-applications (e.g. the use of HTML/JavaScript to request information and perform actions) and other styles of API (e.g. messaging (MQ,EMS), web streaming, file transfer) are included in the scope of this section.

- ***6.4.1 Application programming interfaces (APIs) (including foot note 12) enable various software applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIs that provide developers with programmatic access to a proprietary software application or web service. FIs collaborate with FinTech companies and develop open APIs, which are used by third parties to implement products and services for customers and the marketplace. Hence, it is important for the FI to establish adequate safeguards to manage the development and provision of APIs for secure delivery of such services.***

  Paragraph 6.4.1 seems to suggest that FIs always collaborate with FinTech firms to develop open APIs. This is not always the case, as many FI's have in-house technology development centres working on developing APIs. Para 6.4.1 should be accordingly amended and adequate safeguards should be established to manage the development and provision of APIs, irrespective of whether the APIs are built by FI independently or in partnership with a FinTech firm.

- ***6.4.3 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party***

API access. The vetting criteria should take into account the third party's nature of business, security policy, industry reputation and track record amongst others.

- *If the third party is a start-up, it is unlikely that FI can vet its industry reputation or track record. Suggested edit below. Suggest rephrasing to "A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third-party API access. FI should vet and assess third party's suitability based on applicable criteria under 'Section 3.4 Management of Third Party Services'.*

- *Vetting criteria may be dynamic depending on the nature of API connectivity. We suggest revising such that the FI defines the vetting process based on the nature of the API functionality and its data security.*

- *We request clarification on whether approved API access is only required for third party governance or more on general terms.*

- ***6.4.7 A robust security screening and testing of the API should be performed between the FI and third party before it goes into production. The FI should have the ability to log the access sessions by the third party, such as the identity of the third party making the API connections, and the data being accessed.***

  Further clarification is required whether this refers to the 'penetration testing' of external facing APIs, or to end-to-end testing of the APIs and back-end supporting applications. Where there are multiple third-parties (e.g. end clients) it is not feasible to test each third-party individually.

- ***6.4.8 Real-time monitoring and alerting capabilities should be instituted to provide visibility of the usage and performance of APIs and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.***

  We request further clarification on the requirement to perform real-time monitoring of APIs. E.g. What kind of suspicious activities need to be monitored? Is this required only for critical APIs or based on the classification of data that the API handles?

- ***6.5.1 The prevalence of common business application tools and software on the Internet has enabled end user computing, where business users develop or use simple application to automate their operations, such as perform data analysis and generate reports. Any application developed or acquired by end users should be approved by the relevant business and IT management, and managed as part of the FI's information assets.***

  We request further clarification on what is the scope of impact and definition of application developed or acquired by end user that requires approval from business and IT management. We propose this be risk based for all end user management guidelines in this section.

Section 7: IT Service Management

Member feedback

- ***7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g., fixes for security vulnerabilities and software bugs are implemented within a timeframe that is commensurate with the criticality of the patches to the FI's systems.***

- *Prioritization of patch deployment should take into consideration if FI's systems are mission-critical and accessible from Internet hence more susceptible to exploitation. Suggest section is rephrased as following.*
  Suggest rephrasing to "7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with patch criticality and in accordance to security classification and asset placement of the FI's systems."

- ***7.4.2 All patches should be tested before they are applied to the information assets in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system.***

  The definition of 'Information asset' is too wide under Page 11 as it covers customer-owned and third-party systems of which an FI does not have access to their production environment.
  Suggest section is amended to: "All patches should be tested before they are applied to the FI's systems in the production environment."

- ***7.5.4 A change advisory board, comprising of relevant key stakeholders including business and IT management should be formed to approve and prioritise the changes after considering the stability and security implications of the changes to the production environment.***

- *Not all IT changes will have business impacts and business does not necessarily have the knowledge to assess every IT change. Generally, businesses are engaged as needed.*

- *What is the expectation of business involvement in the change advisory board? Would this be for the purpose of providing approval and sign off? Or would the change advisory board serve as an avenue to promote awareness, and solicit feedback from the business?*

- ***7.5.7 Audit and security logs contain useful information which facilitates investigations and trouble-shooting. As such, the FI should ensure the logging facility is enabled to record activities that are performed during the change process.***

  Suggested to add "where feasible" at the end of para 7.5.7 when incorporating the control as there maybe parts of the change process that could not be logged.

Section 8: IT Resilience

- ***8.1.2 A holistic review of the FI's system and network architectures should be performed to identify any potential single point of failure, and implement appropriate measures to address and mitigate the risk of disruption.***

  Suggestion for MAS to provide guidance on the meaning of "a holistic review".

- ***8.1.3 It is particularly important for an FI which operates systems that support real-time transactions to proactively measure and monitor the utilisation of its system and network resources against a set of pre-defined thresholds 15. Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs, or to identify anomalous system or network behaviour for prompt investigation.***

  The 2013 TRM Guidelines included capacity management under ITSM framework. 2019 TRM does not include capacity management. Is this an intentional omission? Is capacity management intended to be covered by 8.1.3 under IT Resilience?

- ***8.2.1 The FI should perform a business impact analysis to determine its business resumption and system recovery priorities in events where an IT incident leads to large scale service disruption. The FI's systems' recovery time objectives (RTO) and recovery point objectives (RPO), should be defined according to its business needs.***

  We request for the MAS to provide clarity whether this clause should be read on top of the MAS Business Continuity Management (BCM) Guidelines. We suggest that alignment to new requirement from MAS BCM consultation paper should be included or referenced for clarity.

- ***8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management, and avoid taking untested recovery measures which are likely to carry higher operational risks.***

  - *We suggest there is no need to mention the option of taking untested recovery measures and suggest rephrasing to "8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management."*
  - *Could MAS clarify what it means by "untested recovery measures"*

- ***8.3.2 A disaster recovery test plan should include the test objectives and scope, test scenarios, test scripts with details of the activities to be performed during and after testing, test scripts with details of the activities to be performed during and after testing, system recovery procedures, and the criteria for measuring the success of the test.***

  With reference to "criteria for measuring the success of the test", there is currently no industry-wide methodology to measure the success of an RPO. Therefore, we would recommend that further guidance be issued on this in consultation with FIs.

- ***8.3.3 The testing of disaster recovery plans should comprise:***

  a. Various plausible disruption scenarios, including full and partial shutdown or incapacitation of the primary site and major system failures; and

  b. Recovery dependencies between information assets, including those managed by third parties.

  Further clarification is requested for "partial shutdown or incapacitation" and if the definition is consistent among all FI's. For example, partial shutdown could include high availability cluster fail testing within the same data center or partial loss of a data center requiring failover to another data center.

- ***8.3.4 If the system and network architectures support load balancing and high availability, the FI should operate from its recovery site for an extended period as part of disaster recovery testing to gain the assurance and confidence that its recovery site is able to support business needs.***

  Further clarification is requested on the "extended period". Does this mean a few hours or one day?

- ***8.4.3 The FI should periodically restore its system and data backups to validate the effectiveness of its backup restoration procedures...***

  We recommend that this requirement reads: "periodically test the ability to restore its system and data backups to validate the effectiveness of its backup restoration procedures." The test is up to the FI and should not particularly require the live production environment.

- ***8.5.1 The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. In addition, the TVRA should consider the political and economic climate of the country in which DCs is located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.***

  Clarification on whether TVRA should be done by an independent entity or can it be done in-house.

- ***8.5.6 The DC should have adequate physical access controls including:***

  (a) access granted to staff should be on a need-to-have basis, and revoked immediately if access is no longer required.

  Propose to replace the word "immediately" with "promptly"

  (d) access to equipment racks should be recorded, monitored and supervised at all times;

- *Can MAS clarify what kind and to which extent the monitoring of access to equipment racks is expected?*
- *Suggestion to reword the "recorded, monitored, and supervised" as it is redundant, to "Access to equipment racks should be adequately controlled and have adequate surveillance in place."*

Section 9: Access Control

Member feedback

- ***9.1.2 The FI should establish a user access management process to provision and revoke access rights to information assets. Access rights should be authorised and approved by the information asset owner.***

  Organizations Line manager is accountable to ensure that staff is granted with user access relevant to his/her role and responsibilities. Suggesting edits below.
  "Access rights should be authorized and approved by information asset owner or user's line manager or delegate."

- ***9.1.4 The FI should establish a password policy and a process to enforce strong password controls (including footnote 18) for users' access to IT systems.***

  This requirement and footnote risk quickly becoming outdated given that some organisations don't use passwords for authentication. MAS should consider amending requirement to ""The FI should establish a standard for authentication that mitigates brute force attacks to IT systems".

- ***9.1.5 Multi-factor authentication[19] should be implemented for users with access to critical system functions[20] to safeguard the systems and information from unauthorised access***

  In addition to implement multi-factor authentication on specific users, we encourage MAS to consider allowing FIs to alternatively implement multi-factor authentication based on factors such as user's purpose of use, system criticality and user's login location.

- ***9.1.6 The FI should ensure information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as incorrectly provisioned access rights. Exceptions noted from the user access review should be resolved as soon as practicable.***

  Information asset owners are not in a position to determine appropriateness of user access e.g. internal transfer, redeployment by line manager to perform different functions, etc. Suggested edits below.
  "The FI should ensure line managers perform periodic user access review to verify the appropriateness of privileges that are granted to their staff and contractors users"

- ***9.2.1 Users granted with privilege system access have the ability to inflict severe damage on the stability and security of the FIs IT environment. Access to privileged accounts should only be granted on a need-to-know basis; activities of these accounts should be logged and reviewed as part of the FIs ongoing monitoring.***

  Organizations have implemented multiple controls from onboarding background checks, strong access and authentication controls, to the logging of user activities. These layered controls are in place to limit the organizations' exposure to employees and contractors conducting activities which requires privileged access.
  While it is agreed that accounts should be granted on a need-to-use basis, the additional activity of monitoring activities then conducted by the use of these accounts may not provide the additional security benefits when compared to the cost of implementation. The activity of reviewing log entries and tying these activities back to a change description may, in many cases, be inconclusive as log entries to application activities may not provide sufficient information to determine all activities conducted by a user.

- ***9.3.1 Remote access allows users to connect to the FIS's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connection should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.***

  Clarification on whether BYOD email such as Blackberry be classified as remote access assets since they do not have access to internal networks

  9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards.

- *Virtual Devices (e.g., VDI) that are accessed through secure channels including from BYOD should be allowed.*

- *FI cannot harden employee-owned personal mobile devices used for remote access, hence BYOD security policy applies. As such, we propose to draw reference to the Annex B in the draft consultation paper. Suggested edits below.*

- *"The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. For personal-owned mobile devices, please refer to Annex B: BYOD Security."*

- *This control is impractical as FIs cannot enforce its security expectations on the non FI-owned equipment personnel may use to access the FI's information assets. This completely defeats the purpose and benefits of a BYOD strategy. Instead, FIs should be allowed to rely on its own security measures regarding how those assets are accessed, if the device may not have the strongest security measures in place. Given the extensive guidance provided in the revised TRM (e.g. multi-factor authentication, data leakage controls, disallow mobile applications on jail-broken devices, etc.) we believe adequate measures are already in place to mitigate this risk.*

Section 10: Cryptography

Member feedback

- ***10.1.1 The FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.***

  Cryptographic algorithms (e.g. 3DES, AES, etc.) are selected based on industry best practices or advisory papers issued by authoritative sources (e.g. NIST); instead of rigorous testing to be performed by FI of cryptographic algorithms, it would be more pragmatic to use industry recognized strong encryption standard (implied in 10.1.1) and keep abreast of encryption vulnerabilities (10.1.3)

- ***10.2.1 A cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established.***

  FIs are unlikely to need a policy for cryptography, just a technical standard. Suggest rephrasing section to "a cryptographic key management policy or technical standard and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established.

- ***10.2.4 The FI should ensure the systems that store the cryptographic keys and authenticate customer passwords are hardened and tamper resistant, e.g. hardware security module.***

  Outside the payment card applications, password authentication is not an activity typically performed by HSMs. To reduce ambiguity, separate treatment should be given to password authentication versus payment card applications.

Section 11: Operational Infrastructure Security

Member feedback

- ***Section 11 in general***
  Any device connected to an FI's network must adhere to acceptable Network Security Standards. IoT brings into scope a large variety and number of devices and FI's should be aware of that. The MAS should consider removing this section, as it is essentially covered throughout the other sections of this document.

  Would an employee's own personal device that connects to corporate Wifi be considered an IoT device and subject to monitoring?

- ***11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:***

(a) data in motion - data that traverses a network or that is transported between sites; and
(b) data at rest - data in computing endpoints such as notebooks, personal computers, portable storage devices and mobile devices, as well as files stored on servers, databases, backup media and storage platforms (e.g. cloud).

Clarity on the scope of "Endpoints" for "Data at Rest" required as these guidelines should be limited to devices owned and/or managed by FI as FI cannot manage personal devices used by FI resources from an endpoint perspective (11.1.1)

Alternatively, consider including "FI to encrypt when confidential data resides within the end point devices owned by personnel"

- ***11.1.2 The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI's service providers.***

Suggest adding ", where feasible" at end of paragraph 11.1.2 as there could be systemic and procedural restrictions on implementing firm tools in the endpoints or appliances provided/managed by service providers.

- ***11.1.3 Databases, systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in databases, systems and endpoint devices should be encrypted and protected by strong access controls.***

- *It is not always technically feasible to encrypt confidential information stored in databases due to the constraints on performance and search functions which such encryption cause. Encryption protects against the physical theft of information; however, most attacks on database contents are made by compromising user accounts of persons who have access to unencrypted database information. Physical theft concerns can be mitigated by encrypting the underlying media on which databases are stored.*

- *We suggest the MAS also clarifies if backup media and storage platforms (for instance cloud databases) would fall within the scope of 11.1.3.*

- *Confidential data stored in-Company managed infrastructure will be governed by authorized user access and hence encryption of such data should not be mandated. Requiring encryption of data should focus on non-Company managed infrastructure.*

- *Suggestion to use the term 'safeguarded' instead of encryption. Please see suggested minor edits as: "11.1.3 As such, confidential data stored in databases, systems and endpoint devices, should be safeguarded and protected by strong access controls."*

- ***11.1.4 The FI should ensure only authorised mediums are used to communicate, transfer, or store confidential data. Strong access controls should be implemented to protect the information from unauthorised disclosure.***

It is unclear what ‘medium’ is. Suggested edits below:

“The FI should ensure only authorized delivery channels and storage devices are used to communicate, transfer or store confidential data”

- ***11.1.7 The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of...***

  Confidential data should be purged not only prior to asset destruction but also prior to asset transfer/re-assignment. As such, we propose the following suggested edits to provide a more comprehensive approach in handling confidential data. Suggested edits below:
  “The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of or redeployed for other use.”

- ***11.2.2 To minimise the impact of the security exposure originating from third party or overseas systems, as well as from internal trusted network, the FI should deploy firewalls, or other similar measures, within internal networks to segregate information assets within the FI’s internal networks. Information assets could be grouped into network segments based on the criticality of the business that they support, their functional role (e.g. database and applications) of the sensitivity of the information.***

  Suggestion to replace “segregate information assets” with “protect information assets”

- ***11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet.***

  Clarification is needed on the expectation – only systems handling critical business and system functions or containing sensitive data should have Internet surfing separation implemented, or should it be implemented on all end-user computers and devices?

  The requirement to implement internet surfing separation is too prescriptive and should be left to the FI to assess and determine the most appropriate and holistic approach / solution (e.g. browser and email isolation, content threat removal, micro-VMs, AI/ML, etc) to safeguard online services from cyber threats. Suggested amendments below.
  “the FI should perform a risk assessment to ensure such systems are adequately ringfenced and segregated to mitigate likelihood of exploitation from Internet. “

  Suggested amendments reasons:
  Guidelines should be less-prescriptive, instead of recommending to isolate system and data from internet

*"[…] the FI should perform a risk assessment and implement Internet surfing separation by isolating system***s** *or have strong controls in place that effectively reduce the risk of cyber threats from the internet."*

- ***11.3.2 The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.***

  Deviation from standard does not necessarily constitute a risk. It is a non-conformity. Suggested edits below.
  "The FI should establish a process to verify that standards are applied. Non-conformities arising from deviations should be addressed in a timely manner."

- ***11.3.5 To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform real-time scanning of indicators of compromise (IOCs), and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.***

  We suggest that para 11.3.5 be reworded: "To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities." As the Guidelines should be less-prescriptive.

  Real time scanning may cause performance issues and we would like to suggest that an FI can adjust the scanning frequency based on the risk assessment (11.3.5)

- ***11.3.6 Security measures, such as application white-listing, should be implemented to ensure only authorised software is allowed to be installed on the FI's systems.***

  We suggest in para 11.3.6 the words ", such as application white-listing" should be deleted because application white-listing may not be a viable approach for all FIs due to the large and complex environment.

  Additionally, the decision to implement additional security measure (or not) should be derived from assessment.
  Suggested edits below.
  "The FI should consider additional security measures, to ensure only authorized software is allowed to be installed on the FI's systems."

- ***11.5.1 Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which are connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, the networks which they are connected to and their physical locations.***

  References to specific computing techniques such as hypervisor / virtualisation / IoT / BYOD can never be comprehensive. We respectfully propose MAS remove Section 11.5 *as IoT is a technological trend. IoT can be treated similarly as untrusted devices, e.g. customer-owned devices, kiosks and BYOD, and there should be no need to prescribe additional controls against IoT devices.*

Alternatively, we suggest "maintain an inventory of all its IoT devices" be replaced with "maintain an inventory of FI owned IoT devices" for the Guidelines to provide clarity on the scope of IoT.

Can the MAS also clarify whether or not BYOD devices considered IOT and are the FI's required to maintain an inventory of all BYOD's that end users may use? Access control can be accomplished by various methods.

We propose that multifunction printers may not be IOT if they are only connected to the internal networks; however, they should have adequate security, patching, and updates.

Some IoT related devices are not part of an FI's network but connected to the Internet (For instance, CCTV cameras owned by the building management, Mobile devices used for building management, WiFi routers provided by the building management for guests). We would seek clarification with regards to whether such IoT devices listed above which are not connected to FIs network but on the Internet, are out of scope and therefore not required to maintain an inventory as part of the FIs inventory management framework.

- ***11.5.2 Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with function and criticality of the data that, collected, stored and processed by the IoT devices.***

We respectfully propose amending paragraph 11.5.2:

"Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with **the business process***/function and criticality of the data that is* **transmitted***, collected, stored and processed by the IoT devices."*

- ***11.5.3 The network that hosts IoT devices should be secured using strong authentication and network access controls to limit the cyber attack surface. For instance, restrict the inbound and outbound network traffic to and from IoT device. The FI may consider hosting IoT devices in a separate network segment from the network that hosts the FI's systems and confidential data.***

We suggest to make the paragraph less prescriptive and take into account that some devices can be less or more secure than others.

- ***11.5.4 The FI should manage the administrator access to the IoT devices where feasible to minimise the risk of unauthorised access.***

  We respectfully propose amending paragraph 11.5.4:

  *"The FI should manage the administrator access to the IoT devices where feasible to minimise the risk of unauthorised access. **Where access control is not provided by the IoT device, the FI may select an alternative control, such as restricting traffic as outlined in 11.5.3.**"*

  Amendments reasons:
  The guidelines should acknowledge that not all devices may allow for administrator access configuration.

- ***11.5.5 The FI should log and monitor the system activities of IoT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours.***

  There are IOT devices that are purpose-built to be active outside normal working hours e.g. security cameras, and such 'behaviour' should not necessarily be deemed as anomalous. If Section 11.5 still remains - Suggested edits below.
  "The FI should log and monitor the system activities of IOT devices for suspicious or anomalous system activities or user behavioural patterns."

Section 12: Cyber Surveillance and Security Operations

Member feedback

- ***12.1.1 To maintain good cyber situational awareness…. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities...***

  Suggest adding footnote on these terminologies 'situational awareness', cyber alerts' and 'cyber events' for additional clarity. Refer to FSB Cyber Lexicon (http://www.fsb.org/wp-content/uploads/P121118-1.pdf), released on November 2018, for these terminologies. We also added a suggested footnote below.
  12.1.1 To maintain good cyber situational awareness1 …. Cyber-related information would include cyber alerts2, cyber events3, cyber threat intelligence and information on system vulnerabilities.
  Footnote
  1 Situational Awareness is the ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event.
  2 Cyber Alert is notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems.
  3 Cyber Event refers to any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
  Adapted from FSB Cyber Lexicon published on 12 November 2018.

- ***12.1.2 The FI could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties.***

  Could MAS further clarify whether procuring cyber intelligence monitoring services is considered as "outsourcing" or "third party services"

- ***12.1.5 The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation.***

  We respectfully propose amending paragraph 12.1.5:
  "The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services to facilitate evaluation and identification of online misinformation."

  Suggested amendments reasons:
  Guidelines should not suggest mandating the use of specific technology in the regulations, instead focus on the control objectives that need to be achieved.

  Detect and respond to 'Misinformation' is a broad statement; a clearer understanding of the intention and scope of this guideline would be useful (12.1.5).

- *12.2 Cyber Monitoring and Security Operations*

  We suggest that the way anomalous user behaviour is detected shouldn't be tied to a particular methodology.

  Profiling individual users and their behaviour leads to legal/privacy/regulatory concerns. This relate to how the data can be used, how it is shared and protected, and what country specific regulatory requirements will need to be addressed when storing this type of information considering many FIs operate in many different countries.

- ***12.2.2 As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be tell-tale signs of intrusions.***

  Suggested amendments below for clarity:
  As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block call-backs, which can be intrusions indicators of attempted intrusions.

- ***12.2.6 To facilitate identification of anomalies, the FI should establish a baseline profile of each system and user's routine activity. The profiles should be regularly reviewed and updated.***

Establish a baseline profile of each system and user's routine activity; applicability in its current form is too broad and clarity should be provided if this can be limited to critical systems / services (12.2.6).

We also request further clarification if this is intended for external customers.

- ***12.2.7 User behavioural analytics is the use of machine learning algorithms in real time to analyse system logs, establish a baseline of normal user behaviour and identify suspicious or anomalous behaviour. The FI should consider applying user behavioural analytics to enhance the effectiveness of security monitoring.***

Further clarification if this is intended for external customers.

- ***12.3.3 The cyber incident response plan should be reviewed, updated and tested at least annually. Lesson learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.***

The testing of the cyber incident response plan is covered in section 13.3 (Cyber Exercises) and hence can be removed from here. To follow a risk-based approach, we recommend this requirement to be periodic as determined by FI rather than annual and suggest the following amendment:

"12.3.3 The FI's cyber incident response plan should be periodically reviewed and/or updated based on current cyber threat intelligence, information-sharing and lessons learned following a cyber event."

Section 13: Cyber Security Assessment

Member feedback

- ***13.1 Vulnerability Assessment***

The 2013 TRM guidelines included that Vulnerability Assessment (VA) should have a combination of automated tools and manual techniques to perform a comprehensive VA. Is this a mandatory requirement in the latest 2019 guidelines?

- ***13.2.1 The FI should carry out penetration testing (PT) to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services.***

We suggest that PT may not necessarily provide in-depth evaluation of security posture, rather helps in identifying gaps in cybersecurity defences and suggest the following amendment:

"13.2.1 The FI should carry out penetration testing (PT) to identify gaps in cybersecurity defences of its IT environment. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT."

- ***13.2.3 To obtain a more accurate assessment of the robustness of the FIs security measures, penetration testing should be conducted on the production environment.***

Proper safeguards should be implemented when penetration testing is conducted on the production environment.

The guideline may lead to significant risk to an FI and we recommend this to include production-like environment as well. The production-like environment should have similar hardware/software/application configuration as that of Production. As a result, we suggest the edit below:

*"13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production or equivalent production-**like** environment. Proper safeguard should be implemented when PT is conducted on the production environment."*

We suggest to allow a mechanism to defer production penetration testing in favour of interim non-production penetration testing where risks have been identified. Known risks under remediation may result in PT of the underlying production asset posing an undue risk to operational stability leading to potential production impact.

- ***13.5.1 To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on real cyber incidents.***

Suggest adding a footnote for red team using 'Section 4 Definition' on 'Attacker (Sometimes referred to as 'Red Team')' in line with the 'ABS Guidelines for the Financial Industry in Singapore, Red Team: Adversarial Attack Simulation Exercises' which was referenced by MAS under Section 13.4.
Footnote on Red team
1 Attacker (sometimes referred to as Red Team) is an individual or a team who is employed or contracted by an organisation to simulate the attack tactics of a real-world adversary based on intelligence about prevailing and/or probable cyber threats and incidents.
Adapted from ABS Guidelines for the Financial Industry in Singapore, Red Team: Adversarial Attack Simulation Exercises, version 1, November 2018.

Section 14: Online Financial Services

Please clarify if Section 13 (2013 TRM) - Payment Card Security (Automated Teller Machines, Credit and Debit Cards) is now under Online Financial Services. If yes, which subsection in Section 14 covers this? If it is not under Online Financial Services, then which section should it be under in the revised TRM?

- ***14.1.1 Online financial services refer to banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. In delivering online financial services, the FI should implement security and control measures which commensurate with the risk involved to ensure data confidentiality and integrity, and the security, availability and resilience of the online services.***

Would applications created to enhance client's experience (e.g. Virtual Reality) be included as part of the scope? These are the applications not created for *financial/payment services but its usage is for events whereby clients are required to download the mobile application for a better client experience.*

Are read-only applications included as part of the scope for paragraph 14.1.1?

- ***14.1.5 Distribution of mobile applications or software to customers should only be performed through official mobile application stores or other secure delivery channels.***

  FIs do not distribute mobile banking application to customers but rather customers choose to download FI's mobile banking application from official mobile application stores. Suggested edit below.

  FIs should only make available mobile applications or software to customers through official mobile application stores or other secure delivery channels.

- ***14.1.6 The FI should actively monitor the internet, mobile application stores, social media websites, emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report the phishing attempts to the service providers and law enforcement agencies to facilitate removal of the malicious content. The FI should alert its customers of such campaigns.***

  We suggest that the guideline should be less-prescriptive. Monitoring of SMS and e-mail of customers is not feasible as it takes place outside the FI's infrastructure. It may not be practical to alert customers of every instance of Phish sites identified as there are many discovered each day. We suggest that the paragraph be reworded as follows:

  *"14.1.6 The FI should actively monitor the Internet, mobile application stores and social media websites for phishing campaigns targeting the FI and its customers. **Timely** action should be taken to report the **impactful** phishing **campaigns** to the service providers and law enforcement agencies **as appropriate** to facilitate removal of the malicious content."*

- ***14.1.7 Rooted or jailbroken mobile devices should be blocked from accessing the FI's mobile applications to perform financial transactions as such devices are more susceptible to malware and security vulnerabilities.***

  This point should also be linked to Section 14.4 – Customer Education and Communication. It is important for customers to be aware about the risks of using devices which are more susceptible to malware and security vulnerabilities.

- ***14.2.1 Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on any two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. OTP generator) and who you are (e.g. Biometrics).***

ASIFMA members suggest that a risk based approach be taken vis a vis multi-factor authentication. We suggest that multi-factor authentication should only be required before a high risk function is performed. For non-high risk functions (such as login), multi-factor authentication should be optional. This is in line with the HKMA Supervisory Policy Manual for the Supervision of E-banking item 4.1.2, which states that two-factor authentication is expected for "transactions with higher risk" such as unregistered third-party transfers or large-value transactions.

Further clarification needed for the practice and requirement for OTP. Is classification required for first time login and mask? As of now all banks are showing the masked information on login without 2FA. Please clarify if this be added in the text.

- ***14.2.2 E2E encryption at the application layer should be implemented for the transmission of customer passwords so that they are not exposed at any intermediate nodes between the customer mobile application or browser and the system where passwords are verified.***

  Browser script-based password encryption is an implied requirement novel to Singapore. Where possible, requirements enabling equivalent protection of credentials should be achievable without FIs producing bespoke cryptographic methods, structures and code.

- ***14.2.3 The FI should implement transaction-signing (e.g. digital signatures) for authorising high risk activities to protect the integrity of customer accounts' data and transaction details. High-risk activities include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details, high value funds transfer and revision of funds transfer limits.***

  Suggestion to take account of PayNow which does not require any transaction signing. Also, it is better to clarify whether merchant/bill payment is out of scope.

- ***14.2.6 Where biometric technologies and customer passwords are used for customer authentication, the FI should ensure the biometrics information and authentication credentials are encrypted in storage and during transmission.***
- ***14.2.7 The performance of the biometrics solution, based on false acceptance rate and false rejection rate, should be calibrated to commensurate with the risk associated with the online activity.***

  Clarification is required on both 14.2.6 and 14.2.7 requirements applicability where FIs rely on biometric capabilities on the device used by customer. In such cases, it is proposed that FIs conduct due diligence on the solution offered by device manufacturers to evaluate if the biometric technologies are suitable to be used for customer authentication in online financial services.

  Suggestion that where feasible, FIs work with and share their technical / security standards with device manufacturers to improve the biometrics solution. However, the device manufacturer should remain responsible and accountable to its customers with regard to the performance of the biometrics solution and the security of the biometric information stored in the user's device.

- ***14.2.12 Where alternate controls and processes (e.g. maker-checker function) are implemented for corporate or institutional customers to authorise transactions, the FI should perform a security risk assessment to ascertain these controls or processes commensurate with the risk of the activities that are being carried out.***

  We would like to request for more clarity on this paragraph. Usually, alternate controls are determined after a risk assessment and controls testing. The paragraph indicates that a security risk assessment is required "after the fact". By this paragraph, are we expected to relook at our alternate controls to assess whether the controls are commensurate with the risk of the activities?

- ***14.3.1 The FI should implement real-time fraud monitoring or surveillance systems to identify and block suspicious or fraudulent online transactions***

  We request further clarification from MAS on what is meant with online transactions.

- ***14.4 Customer Education and Communication***

  Suggestion for FI to alert their customers to cyber threats and incidents, and the risks of using rooted or jailbroken mobile devices. The FI should educate their customers, other than professional and institutional customers, of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services.

Section 15: IT Audit

Annex A: Application Security Testing

Annex B: BYOD Security

Annex B.1(b) Mobile device do not cover the full scope of devices that staff use to gain on demand access to enterprise computing resources and data via virtualisation. Non-mobile devices such as personal computers are also used. Recommendation to MAS to consider using the term "devices" instead to reflect the coverage of staffs' devices used in this process.

Annex C: Mobile Application Security

- *"Annex C.1(e) implement a secure in-app keypad security measures to mitigate against malware that captures keystrokes; and "*

This provision is quite prescriptive, suggest rewording to use security measures instead.