RESPONSE TO FEEDBACK RECEIVED

Proposed Revisions to Technology Risk Management Guidelines

Monetary Authority of Singapore

Contents

1 Preface

1.1 On 7 March 2019, MAS issued a Consultation Paper on the proposed revisions to the MAS Technology Risk Management Guidelines (TRMG). The TRMG has been enhanced to include new guidance on effective cyber surveillance, secure software development, adversarial attack simulation exercise,[1] and management of cyber risks posed by the emerging technologies such as Internet of Things. Financial institutions (FIs) are expected to have in place effective technology risk management practices and controls to protect their IT infrastructure. The consultation period closed on 8 April 2019.

1.2 MAS thanks all respondents for their feedback and comments. MAS' responses to the feedback and comments are set out in the subsequent paragraphs. Unless specifically requested for confidentiality, the respondents' identities and their submissions are provided in Annex A and Annex B respectively. The annexes may be accessed at this link.

2 General Comments

Applicability of the TRMG

2.1 Respondents sought to confirm the type of FIs to which the TRMG will be applicable. A respondent asked whether the TRMG will be applicable to the following categories of FIs:

(a) Overseas branches and subsidiaries of FIs that provide financial and non-financial services; and

(b) Singapore based subsidiaries of FIs that provide non-financial services.

MAS' Response

2.2 The TRMG is applicable to all FIs as defined in Section 27A(6) of the Monetary Authority of Singapore Act. The TRMG will not apply to overseas subsidiaries and branches of the FI.

2.3 If the FI's overseas subsidiaries or branches are providing IT services that are used by the Singapore operations, the FI should ensure the technology risk management practices are aligned with the TRMG as part of its outsourcing management.

[1] Adversarial attack simulation exercise tests the FI's capability to prevent, detect and respond to threats by simulating perpetrators' tactics, techniques and procedures to target the people, processes and technology underpinning the FI's business functions or services.

Applicability of TRMG to Third Parties

2.4 Respondents sought clarification on the applicability of the TRMG to third parties, including intragroup or outsourced service providers, where the responsibilities for technology, including cyber security, policies, processes and systems are established and owned by third parties, and are not within the control of the FIs.

MAS' response

2.5 The TRMG is applicable to intragroup and outsourced service providers. For other third party arrangements, which FIs do not have control of the technology policies, processes and systems, FIs should assess the exposure to technology risks from the use of these third party services and put in place appropriate measures to address the identified risks.

Group Policies and Procedures

2.6 A respondent sought clarification on whether they could adopt their Group's IT practices, policies and procedures to meet the expectations in the TRMG.

MAS' response

2.7 FIs may adopt their Group's IT practices, policies and procedures as long as the expectations in the TRMG are met.

Risk-based Approach

2.8 Respondents commented that the nature, size and complexity, as well as the cyber security maturity, of FIs vary. Hence, the applicability of the TRMG on FIs may differ. They recommended that MAS calibrate the TRMG for different types of FIs.

2.9 Some respondents suggested that a distinction be made between what are expected and good practices. One respondent requested MAS to establish a roadmap to help FIs achieve the expectations in the TRMG.

MAS' Response

2.10 As stated in Chapter 2 of the TRMG on "Application of Technology Risk Management Guidelines", the TRMG comprises a set of key technology and cyber risk management principles and best practices which FIs should adopt based on the nature, size and complexity of their business.

2.11 Depending on its risk exposure and tolerance, the FI should draw up its own roadmap to implement IT practices that meet the expectations in the TRMG.

Harmonisation of the TRMG with Other Technology Risk Management Guidance

2.12 Respondents proposed that MAS should consider harmonising the TRMG with the cyber security guidance established by industry associations and international organisations, such as the Financial Services Sector Coordinating Council or National Institute of Standards and Technology. A consistent set of standards will facilitate FIs in complying with the MAS' and other regulators' technology risk management guidelines.

2.13 Respondents also suggested MAS to allow the industry to develop IT standards before setting them as best practices in the TRMG.

MAS' Response

2.14 In drafting the revised TRMG, MAS had referred to the technology risk management and cyber security guidelines published by international standards setting organisations, financial regulators and industry associations.

2.15 The intent of the TRMG is to establish principles and best practices on technology risk management for the Singapore financial industry.

Adherence to the TRMG

2.16 A respondent suggested that as a good practice, MAS should consider instituting a regime to ensure FIs' adherence to the TRMG.

MAS' Response

2.17 While MAS closely supervises FIs' adherence to the TRMG, FIs are expected to ensure adequate oversight and governance of their IT controls and processes to maintain the availability, integrity and confidentiality of their data and systems.

Differences between the Notice on Cyber Hygiene and the TRMG

2.18 Some respondents sought clarification on the differences between the Notice on Cyber Hygiene and the TRMG.

MAS' Response

2.19 The Notice on Cyber Hygiene requires relevant entities to implement a set of essential cyber security requirements to protect and secure their systems from cyber attacks. The Notice imposes legally binding requirements.

2.20 On the other hand, the TRMG sets out technology risk management principles and best practices which FIs could adopt based on the nature, size and complexity of their business. Contravening guidelines is not a criminal offence and does not attract civil penalties, but specified institutions or persons should observe the spirit of the guidelines.

Differences between the terms "should", "could" and "could consider" in the TRMG

2.21 Respondents sought clarification on differences between the terms "should", "could" and "could consider" in the TRMG.

MAS' Response

2.22 The terms "should", "could" and "could consider" are used according to their ordinary meaning.

Glossary of Terms

2.23 Some respondents requested MAS to define some of the technical and non-technical terms that are used in the TRMG.

MAS' Response

2.24 To harmonise the understanding of common technology terms, the Financial Stability Board had published the Cyber Lexicon[2] on 12 Nov 2018, and MAS has aligned the use of cyber terms in accordance with the definitions in the Cyber Lexicon.

2.25 MAS will not be providing a glossary of terms for the TRMG. FIs may refer to the Cyber Lexicon and glossaries published by international standard setting organisations.

2.26 The ordinary meaning for non-technology terms applies.

Frequency of Review

2.27 Respondents sought clarification on the expected frequency of review, particularly for paragraphs in the TRMG where "periodic review" or "regularly reviewed" were stated.

MAS' Response

2.28 FIs are expected to determine the frequency of review based on the criticality of the control, process, procedure, system or service, and their evaluation of the technology and cyber risks.

2.29 Minimally, FIs should conduct a review whenever there is a significant change in the operating environment or threat landscape.

[2] https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Effective Date of the TRMG

2.30 Respondents requested MAS to grant FIs sufficient time to implement the revised expectations in the TRMG. Some of the respondents requested MAS to consider making the TRMG effective after a period of 18 to 24 months after its issuance, as there could be challenges in meeting the requirements, in particular for small FIs, which might need to engage external parties to help to study the existing IT infrastructure and implement the necessary controls.

MAS' Response

2.31 The TRMG will be effective from the date of issuance.

2.32 The TRMG is a set of technology risk management principles and best practices which FIs could adopt based on the nature, size and complexity of their business. Many of the expectations in the TRMG are from the guidelines published in 2013.

2.33 FIs should conduct an assessment to identify gaps against the TRMG that are relevant to their operations. FIs may adopt a risk-based approach in determining the implementation timeframe to address any gaps between the TRMG and their current practices.

3 Technology Risk Governance and Oversight

Board of Directors' and Senior Management's Oversight of Technology Risks (Section 3.1)

3.1 Respondents sought clarification on the extent of knowledge and skills that the board of directors and senior management of the FI is expected to have or acquire in order to effectively exercise oversight of the FI's technology risks.

3.2 A respondent suggested creating a function that is appointed by the FI's board of directors to oversee the technology risk management framework and strategy.

3.3 The respondent also sought clarification on MAS' expectations on the measures that the board of directors or its designated committee should use to assess the management's competency in managing technology risks.

MAS' Response

3.4 MAS expects the FI's board of directors and senior management to comprise members who are able to competently exercise their oversight of the FI's technology strategy, operations and risks.

3.5 FIs should engage individuals, who have relevant experience in IT, including technology operations, risk management or audit, to be part of its board of directors and senior management.

3.6 A technology risk management function should be put in place to oversee the technology risk management framework and strategy, as well as to provide an independent view of the FI's technology risks.

3.7 As the nature, size and complexity of FIs vary, MAS will not be able to prescribe the specific measures that the board of directors or its designated committee should use to appraise its management performance in technology risk management. Key performance indicators for senior management may include factors that measure the effectiveness of the framework and strategy that are put in place to protect the availability, integrity and confidentiality of data and systems.

Composition of Board of Directors and Senior Management (Section 3.1)

3.8 Respondents enquired whether it is mandatory to have a Chief Information Security Officer (CISO) or Head of Information Security; and whether the responsibilities of the CISO or Head of Information Security could be assumed by the Chief Information Officer (CIO). They also sought clarification on the reporting structure of the CISO.

3.9 There are respondents who commented that the board of directors could be guided by senior management who has knowledge of or specialises in technology risk management.

3.10 Some respondents also highlighted that the board of directors and senior management may not reside in Singapore, particularly for FIs that have an international presence. They enquired whether the expectations under "Role of the board of directors and Senior Management" in Chapter 3 of the TRMG could be met under this circumstance.

3.11 A respondent sought clarification on the composition of the committee that could be appointed by the board of directors to oversee technology risks.

MAS' Response

3.12 The TRMG provides general guidance and is not intended to prescribe a particular governance structure for FIs. Broad guidance is provided on the expected key responsibilities of senior managers (e.g., the Head of Information Technology or CIO, Head of Information Security or CISO) that have oversight and management of technology risks, including cyber risks.

3.13 The FI's board of directors is expected to provide oversight over technology risks. MAS is of the view that the board of directors will benefit by having members who are knowledgeable and experienced in managing technology risks.

3.14 For the FI whose board of directors is not based in Singapore, the roles and responsibilities in Chapter 3 of the TRMG can be delegated to and performed by a management committee or body beyond local management that is empowered to oversee and supervise the local office (e.g. a regional risk management committee).

Roles and Responsibilities of the Board of Directors and Senior Management (Section 3.1)

3.15 Respondents commented that to maintain the independence of the third line of defence, the board of directors should be responsible for the appointment of the IT audit function instead of the senior management.

3.16 A respondent commented that the board of directors' responsibilities for technology risk management are too operational and onerous; and enquired whether such responsibilities could be delegated. Another respondent was of the view that the board of directors should oversee technology risks while the management of technology risks should be the senior management's responsibility.

3.17 Some respondents suggested that ongoing monitoring of the effectiveness of technology risk management practices be part of the board of directors' responsibilities.

MAS' Response

3.18 MAS agrees with the respondents' comment on the appointment of the IT audit function and has amended the TRMG to state that the FI's board of directors is responsible for appointing the IT audit function.

3.19 MAS also agrees that the management of technology risks should be the senior management's responsibility and has revised the TRMG.

3.20 Ongoing monitoring of the effectiveness of technology risk management practices and key IT risk should be part of the board of directors' responsibilities as senior management is expected to apprise the board of directors of salient and adverse technology risk developments and risk events that are likely to have a major impact on the FI.

Senior Executive Responsibility for Technology Risk Strategy (Section 3.1)

3.21 Respondents sought clarification on which senior executives in the FI should be given the responsibility to execute the FI's technology risk management strategy.

3.22 They also enquired about the level of authority that should be given to senior executives, and whether giving senior executives access to the board of directors means providing a direct reporting line to the latter.

MAS' Response

3.23 MAS expects the FI to appoint a senior executive, who is qualified, to execute its technology risk management strategy. This person could be the CIO, Chief Technology Officer, Head of IT or any other senior executive in the organisation.

3.24 The senior executive should have access to report or escalate any technology, including cyber, matters to the board of directors.

Scope of Technology Risk Strategy (Section 3.1)

3.25 Respondents requested MAS to provide more guidance on the expected scope of a technology risk strategy.

MAS' Response

3.26 MAS expects FIs to perform their own technology risk assessment and determine the actions and measures they need to implement to address the risks and ensure IT resilience.

Delineation of Responsibilities for Technology Risk Governance (Section 3.1)

3.27 A respondent sought clarification on the delineation of responsibilities in governing technology risks. The respondent was of the view that small FIs may not be able to implement the three lines of defence and enforce a clear segregation of roles and responsibilities for technology risk management.

MAS' Response

3.28 The TRMG provides general guidance and is not intended to prescribe a particular governance structure for all FIs. Broad guidance is provided on the responsibilities of senior managers that have oversight and management of technology risks, including cyber risks.

3.29 MAS recognises that in smaller firms, management oversight and control is generally less dispersed, and decision-making structures tend to be less complex. In these FIs, the directors and Chief Executive Officer usually directly oversee most or all functions in the FIs. While clear segregation of roles and responsibilities could not be enforced, MAS expects appropriate risk management processes and controls to be established to manage technology risks.

Policies, Procedures and Standards (Section 3.2)

3.30 Respondents highlighted that for FIs where IT activities and resources are governed at the group level, policies, procedures and standards at the group level may not fully meet the expectations in the TRMG.

3.31 Some respondents commented that additional guidelines should be provided on the areas which should be covered in the FIs' internal policies, procedures and standards minimally.

3.32 Another respondent enquired if MAS would allow for deviations from the TRMG if the FI has performed a risk assessment on such deviations and documented its risk acceptance and mitigating controls.

MAS' Response

3.33 The FI should perform a gap analysis of its global policies, procedures and standards against the TRMG and address gaps identified to ensure its technology risk management practices are commensurate with its technology risks. MAS does not prescribe the IT policies, procedures and standards that FIs are expected to implement.

3.34 Risks arising from deviations should be assessed and appropriately addressed. The risk assessment should be endorsed by the FI's senior management.

Compliance with Policies, Procedures and Standards (Section 3.2)

3.35 Some respondents commented that it will not be feasible for FIs to impose their policies, standards and procedures on third party service providers since the IT services support different customers. They sought clarification on the extent to which third party service providers, such as cloud service providers, are expected to adhere to the FI's policies, standards and procedures.

MAS' Response

3.36 The use of a third party service providers should not result in a deterioration of controls and compromise of risk management. FIs should ensure their third party service providers are able to meet regulatory standards expected of them.

Scope of Information Assets (Section 3.3)

3.37 Respondents proposed narrowing the scope of information assets to hardware, software and data, which have significant impact to the FI's operations in the event of failure.

3.38 Respondents sought clarification on whether information assets under third party vendors, such as cloud service providers, will fall within the scope of information assets. They commented that FIs may not have the visibility or ability to influence the controls over information assets, which are owned by third party service providers.

3.39 As an alternative, a respondent proposed allowing independent accreditation/ assessment of third party service providers' management of information assets as a form of assurance that the latter meets the expectations of the TRMG.

3.40 A respondent also suggested excluding data with little risk of exposure such as tokenised and anonymised data from the scope of information assets.

MAS' Response

3.41 The intent of the TRMG is for FIs to organise and manage its information assets i.e. hardware, software and data that they access and use, including those at third party service providers.

3.42 FIs should put in place processes and controls to manage information assets according to their security classification or criticality. MAS will not be limiting the scope of information assets.

Management of Third Party Services (Section 3.4)

3.43 A respondent commented that the guidelines on management of third party services are similar to the ones which have been proposed in the Consultation Paper on Outsourcing by Banks and Merchants, published on 7 February 2019. The respondent was of the view that MAS should not replicate the same expectations in the TRMG. Some respondents enquired whether the definition of outsourcing is consistent with the MAS Guidelines on Outsourcing.

MAS' Response

3.44 MAS would like to clarify "outsourcing arrangement" in the TRMG has the same meaning as that defined in the MAS Guidelines on Outsourcing.

3.45 The TRMG covers third party services that are used by FIs but may not constitute outsourcing arrangements. These third party services are provisioned or delivered using IT or may involve confidential customer information electronically stored and processed at the third party. Some examples of such third parties include firms that provide IT forensics, penetration testing and online marketing services.

3.46 FIs are expected to assess the technology risks posed by the third parties' services and mitigate the risks accordingly.

Scope of Employee Background Checks (Section 3.5)

3.47 Respondents sought clarification on the scope of background check that FIs are required to perform on their prospective employees.

3.48 A respondent commented that background checks on contractors and service providers by FIs may not be practical and it should primarily be the responsibility of contractors and service providers to ensure their staff are fit and proper.

3.49 A respondent highlighted that it may not be feasible to perform background checks for personnel who is based overseas, and such checks should be conducted in accordance with local jurisdictional requirements.

MAS' Response

3.50 As the TRMG applies to FIs of varying size and complexity, it is not practical for MAS to specify measures, such as the scope for background checks. The intent of the guidance is to ensure suitable and qualified people are engaged to manage the FI's information assets; and to protect such assets from insider threats.

3.51 We note the respondents' feedback that there may be situations where background checks on personnel could not be conducted. In such cases, FIs should assess the suitability of its personnel, such as through an interview, before engaging them.

Training for Board of Directors (Section 3.6)

3.52 A respondent enquired whether a board member who is cognisant of technology risk matters and practices could be exempted from training provided to the board of directors on technology risks.

3.53 Some respondents sought clarification on whether the training for the board of directors can be conducted by in-house technology risk professionals or external specialists.

MAS' Response

3.54 MAS expects FIs to put in place a training programme to raise staff, senior management and board of directors' awareness on risks associated with the use of technology, the evolving cyber threat landscape, and internal policies; as well as to enhance their understanding of technology risk management practices. The FI may assess whether the training is necessary for its board member based on his knowledge, experience and familiarity with the topics covered in the training programme.

3.55 The training programme can be conducted by in-house or external professionals.

Training for Service Providers (Section 3.6)

3.56 Respondents were of the view that it is not practical to expect FIs to ensure service providers undergo training, particularly for cloud service providers. They suggested that FIs should rely on service providers who already have robust training programs internally, or third party security certifications as evidence that the service providers' staff have undergone appropriate training.

MAS' Response

3.57 FIs should ensure their service providers and contractors have the requisite level of skills and competence required of them to carry out their work effectively. FIs should rely on service providers who are able to demonstrate that they have adequate training programs for their staff or that their staff have undergone the necessary training.

Training Based on Roles and Responsibilities (Section 3.6)

3.58 Respondents were of the view that the content and frequency of IT security awareness training and other training should be commensurate with the roles and responsibilities of the personnel handling the FI's IT systems.

MAS' Response

3.59 MAS agrees with the feedback. The purpose of a training programme is to raise awareness on risks associated with the use of technology, and the cyber threat landscape; as well as to enhance the understanding of technology risk management practices.

3.60 The training programme may be tailored, in terms of its content and frequency, to suit different audiences.

4 Technology Risk Management

Technology Risk Management versus Operational Risk Management (Section 4.1)

4.1 Respondents were of the view that the technology risk management framework should be a subset of the FI's enterprise or operational risk management framework. Since the technology and operational risk management practices are similar, the respondent recommended that technology risk management should not be singled out but be included as part of MAS' broader guidance on operational risk management.

MAS' Response

4.2 The FI's technology risk management framework can be part of the enterprise or operational risk management framework. The section on technology risk management framework was included in the TRMG to highlight that it is an important function in the oversight and governance of technology risks.

Risk Owner (Section 4.1)

4.3 Respondents sought clarification on the role and responsibilities of the risk owner and enquired whether the risk owner could decide on the type of IT security measures to implement but not be responsible for operationalising the measures.

4.4 A respondent enquired whether the FI's head office or regional office could be designated as the risk owner. Another respondent asked if the risk owner should be independent from the system owner.

MAS' response

4.5 As stated in the TRMG, the risk owner is accountable for ensuring proper risk treatment measures are implemented and enforced for a specific technology risk. Hence, the risk owner can decide or be part of the decision making in determining the IT security measures to be implemented. The operationalisation of these measures may be performed by another person or function.

4.6 The risk owner may be an individual or a function at the FI's head office or regional office. Depending on the type of risk, the risk owner can be the system owner.

Statement on Risk Appetite (Section 4.1)

4.7 A respondent proposed including guidance for FIs to develop a cyber risk appetite statement in the TRMG to facilitate the identification and reporting of key cyber risk exposures. The respondent also recommended covering the key components of the National Institute of Standards and Technology Cyber Security Framework in the cyber risk appetite statement.

MAS' Response

4.8 In Chapter 3 of the TRMG, it is stated that the FI's board of directors are expected to approve the risk appetite and risk tolerance statement. The board of directors and senior management are also expected to ensure key IT decisions are made in accordance with the FI's risk appetite. In establishing its risk appetite, the FI may refer to the guidance by international standards setting organisations.

Guidance on Risk Mitigation (Sections 4.4, 4.5)

4.9 Respondents sought clarification on MAS' expectations on the level of risks and mitigating controls that FIs should put in place before implementing a system or acquiring an IT service.

4.10 A respondent commented that Section 4.4 in the TRMG should include cyber exercises as one of the risk mitigation measures that FIs should implement.

4.11 Another respondent highlighted that the criticality of the FI's business or service is one of the determinants of an information asset's availability requirements. Hence, the criticality of the service or business should also be one of the considerations during the development of risk mitigation strategies.

MAS' Response

4.12 FIs are expected to implement controls that are effective in addressing or mitigating the risks for their systems and IT services. The objective of the guidance is to advise FIs not to implement systems or use IT services when the risks outweigh the benefits.

4.13 Section 4.4 of the TRMG is focused on the risk treatment approach instead of specific measures that FIs should implement for risk mitigation. Guidance on cyber exercises are included in Chapter 13 of the TRMG.

4.14 MAS agrees with the respondent's comment that the criticality of the business or service should be part of the FI's assessment criteria during the development of its risk mitigation strategies. Hence, it is stated in Paragraph 4.4.1 of the TRMG that the FI should develop and

implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance.

Continuous Feedback and Improvement in Risk Management (Section 4.4)

4.15 A respondent was of the view that the cyber threat landscape changes rapidly and assumptions made during an initial risk assessment may need to be adjusted.

4.16 The respondent proposed including significant events from threat intelligence, incidents and results from cyber exercises as triggers to initiate a review of existing risk mitigation and control measures. In addition, risk functions in the FI should play an active role in testing and validating the effectiveness of its IT controls and processes.

MAS' Response

4.17 MAS agrees with the respondent's views that FIs should actively monitor the cyber threat landscape and re-assess their risks, as well as test and validate the effectiveness of their controls and processes. However, MAS will not be prescribing the criteria for initiating a risk assessment. FIs are expected to develop their own criteria as part of their technology risk management approach.

Approval of Residual Risks (Section 4.4)

4.18 Respondents sought clarification on MAS' expectation on managing residual risks. They pointed out that FIs typically adopt a risk-based approach where only high risk issues will be reported to and approved by senior management. However, the TRMG appeared to imply that all residual risks should be formally approved by the FI's senior management.

MAS' Response

4.19 FIs can adopt a risk-based approach in managing residual risks. FIs are expected to monitor and report significant technology risks to their senior management and board of directors. We have revised the TRMG to reflect this intent.

Risk Register and Risk Metrics (Section 4.5)

4.20 Respondents commented that MAS should state the minimum requirements in the TRMG for the risk register so as to facilitate effective monitoring and reporting of technology risks.

4.21 A respondent sought clarification on the specific risk metrics that FIs are expected to develop for management reporting.

MAS' Response

4.22 A risk register is a record of the FI's identified risks, and should contain detailed information and actions to manage each risk. FIs are expected to determine the information that should be recorded in the risk register to facilitate the management of technology risks.

4.23 FIs are exposed to different types of technology, including cyber risks. The FIs should determine and establish the technology risk metrics based on the IT risks that they are exposed to.

5 IT Project Management and Security-by Design

Oversight of IT Project Risks (Section 5.1)

5.1 Respondents commented that the oversight of IT project risks should be in the remit of the FI's senior management and not the board of directors. This will be consistent with the responsibilities of board of directors and senior management delineated in Chapter 3 of the TRMG.

5.2 One respondent suggested that the project steering committee be specified as the party to report significant project risks and key decisions to the board of directors and senior management.

MAS' Response

5.3 MAS agrees with the respondents' comments. FIs are expected to establish a risk management process to identify, assess, treat and monitor risks throughout the project life cycle. Paragraph 5.1.4 in the TRMG has been amended to reflect this expectation.

5.4 MAS also expects risks and issues for large and complex projects, which cannot be resolved at the project management level, to be escalated to the project steering committee and senior management. This expectation on management oversight of IT project risks has been moved to Paragraph 5.2.2 of the TRMG.

Waterfall and Agile Approaches or Methodologies for System Development (Section 5.1)

5.5 Respondents commented that the TRMG appeared to emphasise a waterfall system development approach or delivery model. However, projects can also be delivered using other methodologies such as those related to Agile. The respondents proposed that references to Agile development approach or methodology should be included in Chapter 5.

MAS' Response

5.6 The intent of Section 5.1 of the TRMG is to address broad principles related to the management of project risks and is not specific to a particular type of IT project management methodology.

Project Management and Software Development Processes, Procedures and Plans (Sections 5.1, 5.2, 6.2)

5.7 Respondents commented that more details should be provided on project management and software development processes, procedures and plans, such as the following:

(a) the entry and exit criteria, at a project's major junctures, to facilitate decision making by key stakeholders of a project;

(b) the frequency of project steering committee meetings; and

(c) recommended practices and expected deliverables of each type of software development methodology.

MAS' Response

5.8 MAS' intent is to establish the key principles and best practices in project management and software development for FIs. We will not be prescribing specific controls in IT project management and software development processes, procedures and plans that may differ across FIs.

5.9 The FI should assess the complexity of its project and determine the criteria that are best suited for monitoring the progress of the project.

System Acquisition (Section 5.3)

5.10 A respondent commented that it is onerous to expect FIs to ensure software vendors have in place adequate software development, security and quality assurance practices as FIs may not be able to verify the information or conduct audits on such vendors.

5.11 Some respondents also commented that it is not practical to perform source code review and request for source code escrow agreement for commercial off-the-shelf software, such as MS Windows, MS Office, and Oracle database.

MAS' Response

5.12 As part of the system acquisition process, FIs may adopt a risk-based approach when assessing the robustness of their software vendors' software development, security and quality assurance practices.

5.13 We agree with the respondents that FIs may not have access to proprietary source codes of third party software and commercial off-the-shelf software. The FI is expected to assess whether an escrow arrangement should be in place based on the criticality of the acquired software to the FI's business.

5.14 To gain assurance that third party software is robust and secure, FIs may consider obtaining an undertaking from the software vendor on the software quality.

Security-By-Design Principle (Section 5.4)

5.15 One respondent proposed that MAS should allow FIs to take a risk-based approach and suggested that the security-by-design principle should be applied only to critical systems or systems with a higher risk exposure. The respondent also commented that the IT security function need not be involved in all phases of the system development life cycle (SDLC).

5.16 Another respondent suggested including an expectation for FIs to develop monitoring mechanisms to ensure the security-by-design principle is applied in each phase of the SDLC.

MAS' Response

5.17 The security-by-design principle should be applied for all IT projects.

5.18 As part of the SDLC framework, MAS expects FIs to establish security requirements in the early phase of system development or acquirement, as well as continuous security evaluation and adherence to security practices throughout the SDLC. MAS agrees that FIs should develop processes to ensure the security-by-design principles are consistently applied for their projects.

5.19 MAS expects FIs to involve their IT security function, where relevant, in each phase of the SDLC.

System Testing (Section 5.7)

5.20 A respondent suggested that system testing should not just be limited to a single testing phase but should be conducted across the entire life cycle of system development.

5.21 It was also suggested that resilience testing is included as part of the scope of system testing.

MAS' Response

5.22 MAS does not prescribe the types of testing and the number of times testing should be conducted. MAS expects FIs to establish a methodology for system testing which should cover business logic, system function, security controls and system performance.

Segregation of Development, Testing and Production Environments (Section 5.7)

5.23 A respondent commented that setting up separate environments for development, testing and production is operationally costly for FIs, and proposed that FIs be allowed the flexibility to determine the types of environments to conduct development, testing and production and the controls for securing these environments where required, as long as the

appropriate controls to ensure the integrity and security of the source code and compiled software programs are in place.

MAS' Response

5.24 The purpose of implementing different environments for development, testing and production activities is to protect the availability, integrity and confidentiality of data and systems in the production environment. It allows the FI to develop software and rigorously test its systems in other controlled environments and minimise risks to the production environment that could lead to unauthorised disclosure and modification of data, as well as system disruption.

5.25 The FI should perform an assessment of the setup of its development, test and production environments relative to its operations, and implement appropriate controls in the different environments.

6 Software Application Development and Management

Enforcement of Application Development and Management Practices on Third Parties (Section 6.1)

6.1 Respondents were of the view that it would be difficult to adhere to the software development and management principles in the TRMG when the software development function is outsourced or contracted to third parties.

6.2 In the area of training software developers, respondents proposed that the guidance be focused on ensuring software developers have adequate skills and competence for the job.

MAS' Response

6.3 MAS expects FIs to ensure the service provider or vendor employs a high standard of care in performing the outsourced service as if the service continued to be conducted by the FI. In this regard, MAS also expects FIs to apply standards and practices that are aligned with the principles of software development and management even if they contract or outsource software development to third parties.

6.4 MAS agrees with the respondent that apart from training software developers, the TRMG should also reflect that software developers should be skilled in applying secure coding and software development standards. The TRMG has been revised to better reflect MAS' policy intent.

6.5 As software development practices may vary across FIs, MAS expects FIs to assess the applicability of internationally recognised industry best practices on software development, adopt these practices and train their developers so that they have the skills that are commensurate with their job responsibilities.

Software Review and Security Validation Methods (Section 6.1)

6.6 Respondents opined that FIs should be permitted to use any source code review and security testing methods to validate the security of software applications.

6.7 They commented that the expectation to use a mixture of Static Application Security Testing, Dynamic Application Security Testing and Integrated Application Security Testing approaches is too prescriptive. The respondents proposed amending the TRMG to require FIs to establish a testing and validation strategy to assess the robustness and security of the software.

MAS' Response

6.8 Application security testing aims to identify and remediate vulnerabilities in software applications that could be exploited and result in data leakage, disruption to business operations, financial losses or reputational damage.

6.9 FIs are expected to perform source code review and adequate security testing. MAS would like to clarify that the TRMG is not recommending any specific methods to validate software security. The intent of the guidance is to provide some examples of common testing methods that are used for identifying security vulnerabilities in software applications.

6.10 MAS has amended the TRMG to incorporate the expectation on establishing a testing and validation strategy to ensure software robustness and security.

Remediation of Software Defects (Section 6.1)

6.11 The respondents were of the view that the phrase "remediated before production deployment" in the guidance imposes an unduly onerous expectation that does not consider the FI's business risk appetite.

6.12 Application security verification and testing activities may reveal a sizable number of issues and software defects of various severity levels, and not all identified issues necessarily exceed business risk appetite to require the same urgency of remediation. According to the respondents, as long as there are adequate risk assessment and mitigating measures in place, FIs should be allowed to deploy software to production even if there were outstanding software issues.

MAS' Response

6.13 MAS agrees with the respondents that software defects can vary in severity and not all uncovered software issues during testing must be resolved before the system is implemented in the production environment. FIs should perform risk assessment and address software weaknesses that pose significant risks to the confidentiality, integrity and availability of the system and data before its implementation.

Additional Guidance on DevOps (Section 6.3)

6.14 The respondents suggested that more guidance should be provided for different phases or stages of DevOps, i.e. regular operations, integration, infrastructure creation, image creation and hardening, as well as build. They also sought to clarify whether FIs are allowed to use a risk-based approach when applying DevOps for software development. One respondent suggested including clauses in the TRMG to support the use of DevOps practices.

6.15 Some respondents highlighted that DevOps is a means to structure the engineering and support functions and is not unique to software development and management. They proposed the guidance to be moved to another chapter.

6.16 Some proposed explicitly mentioning DevSecOps in the TRMG for completeness.

MAS' Response

6.17 MAS expects FIs to align its DevOps processes with its SDLC framework and IT service management processes. MAS' intent is to establish the key principles and best practices in software development and management for FIs. We will not be prescribing the specific approach that FIs should adopt.

6.18 MAS notes the respondents' comment that DevOps is not just for software development and management. However, our intent is to provide guidance on the use of DevOps as part of software development and delivery.

6.19 The term "DevOps" has been amended to "DevSecOps" in the TRMG to emphasise the importance of incorporating Security-by-Design principles and implementing security measures as part of DevOps.

Segregation of Duties in DevOps (Section 6.3)

6.20 Respondents sought clarification on the extent to which segregation of duties should be implemented for the development and operations functions in DevOps. They were of the view that the proposed segregation of duties for the development, testing and operations functions goes against the purpose of DevOps, which centres on automation and integration of traditionally separate processes.

6.21 Respondents suggested that apart from segregation of duties, MAS should consider allowing alternative controls such as automation of software releases and testing.

MAS' Response

6.22 MAS agrees with the respondents' comments that DevOps will facilitate continuous integration and continuous delivery by integrating and automating software development and IT operations. At the same time, MAS is also concerned that without applying security principles in

DevOps processes, FIs run the risk of having staff who have system access to change and deploy software without proper check and balance.

6.23 FIs are expected to apply security measures and segregation of duties principles at critical junctures in the DevOps processes, where relevant, even when these processes are automated.

Scope of Guidelines on Application Programming Interfaces (Section 6.4)

6.24 Respondents sought clarification on the scope of guidelines on application programming interfaces (APIs) in the TRMG. There are suggestions to include API security standards in the guidelines.

MAS' Response

6.25 The TRMG highlights the key aspects of securing the API development and provisioning to safeguard the integrity and security of FIs' systems and customer information. These include:

a) using strong encryption to securely transmit sensitive data;

b) building capabilities to monitor the usage of APIs; and

c) detecting suspicious activities and revoking any access in the event of a security breach.

6.26 Best practices on the implementation of APIs in FIs and organisations, common APIs for industry and cross-sectoral stakeholders, and guidance on information security standards and governance models for FIs and FinTech players could be found in MAS-ABS Financial World: API Conference 2016 E-book and ABS-MAS Financial World: Finance-as-a-Service API Playbook.

Vetting of Application Programming Interfaces (Section 6.4)

6.27 Respondents commented that the vetting process is beyond the scope of IT, and relevant business functions should perform the due diligence on third party API access.

6.28 Respondents sought clarification on the scope of vetting expected of third party APIs.

MAS' Response

6.29 MAS agrees with the respondents that IT and business functions should be involved in the vetting process of APIs. Hence, Paragraph 6.4.2 of the TRMG states that vetting criteria should take into account the third party's nature of business, industry reputation and track record amongst others.

6.30 The scope of technology risk assessment in the vetting process would largely depend on the nature of communication and interaction, and the sensitivity of information that is exchanged

between the FI and its third party via APIs. FIs are expected to apply similar security standards that are used to assess other types of technologies in their assessment of third party API access.

Acceptable Cryptographic Standards and Cryptographic Key Management (Section 6.4)

6.31 A respondent sought clarification on the cryptographic standards and cryptographic key management procedures that FIs are expected to use to secure APIs.

MAS' Response

6.32 FIs should refer to Chapter 10 of the TRMG on Cryptography as well as existing international standards when implementing encryption standards and cryptographic key management controls for securing APIs.

6.33 FIs can also refer to the ABS-MAS Financial World: Finance-as-a-Service API Playbook for information security standards and governance models.

Real-Time Monitoring of Application Programming Interfaces (Section 6.4)

6.34 Some respondents commented that technology solutions for performing real-time monitoring of APIs are limited and hence the expectation to have real-time monitoring and alerting capabilities will be onerous for FIs.

6.35 The respondents also highlighted that it would be challenging to detect suspicious activities on public cloud service providers' APIs.

MAS' Response

6.36 APIs provide a gateway for third parties into the FI's environment. The associated risks of an API being used as a conduit to compromise the FI's environment are not less than those present in other types of external connections.

6.37 FIs are expected to have robust measures in place to provide visibility of the usage and performance of APIs, and detect suspicious activities by performing real-time monitoring of its APIs.

6.38 MAS expects FIs to be aware of risks involved in consuming third parties' APIs and provisioning of APIs for third party access. Controls implemented should be commensurate with the sensitivity and criticality of the data being exchanged, as well as the FI's data confidentiality, integrity and availability requirements.

Inventory of End-User Developed Applications (Section 6.5)

6.39 A respondent proposed expanding Section 6.5 of the TRMG on Management of End User Computing and Applications to include guidelines on maintaining an inventory of end-user

developed applications. The respondent is of the view that it will be difficult to manage such applications without keeping proper records.

MAS' Response

6.40 MAS agrees that maintaining an inventory of end-user computing and applications is important to effectively manage the FI's information assets. Section 3.3 of the TRMG on Management on Information Assets and Section 7.2 on Configuration Management set out the expectations on maintaining an accurate and complete view of the FI's IT operating environment so as to have visibility and effective control of its systems.

Management of End-User Developed Applications (Section 6.5)

6.41 Respondents sought to clarify whether MAS expects FIs to apply software development and management practices on end user computing and applications.

6.42 Respondents suggested that applications that are developed and acquired by business users could be approved by business managers.

MAS' Response

6.43 As the risks present in such applications are no different from other applications that are used in the FI's environment, MAS expects FIs to establish a process to assess the risks of end user developed or acquired applications, ensure appropriate controls and security measures are implemented, perform testing and obtain approval for the use of these applications.

7 IT Service Management

Use of the Term "Information Assets" in the Guidelines on IT Service Management

7.1 Respondents were of the view that the use of the term "information assets" for the processes in IT service management is too broad, and proposed to replace the term with another term or phrase, such as "hardware and software", that describes the types of information assets which the guidelines on IT service management are applicable to.

MAS' Response

7.2 MAS agrees with the respondents' comments that the use of "information assets" is broad, and has revised the TRMG by replacing the term "information assets" with "IT systems" in Section 7.4 of the TRMG on Patch Management.

7.3 MAS will not be amending the term "information assets" for other areas, such as change management, as we expect FIs to review and ensure controls are in place for managing data that are electronically stored.

Guidelines on Information Asset Management and Configuration Management (Sections 3.3 and 7.2)

7.4 A respondent commented that the guidelines on management of information assets (Section 3.3) and configuration management (Section 7.2) are similar.

MAS' Response

7.5 MAS would like to clarify that Section 3.3 of the TRMG on Management of Information Assets stipulates the practices that should be in place to manage information assets. Section 7.2 on Configuration Management is an extension of Section 3.3, and it is about implementing a process to maintain and update information of the FI's hardware and software to have visibility and effective control of its systems.

Implementation of Controls to Secure Information Asset Inventory (Section 7.2)

7.6 A respondent highlighted that IT incidents could be the result of deficiencies in configuration management controls, and recommended MAS to include an expectation on FIs to put in place adequate controls to secure the configuration management process in the TRMG.

MAS' Response

7.7 MAS acknowledges the respondent's concerns that a poorly managed configuration management process and information asset inventory could result in IT incidents.

7.8 Similar to other IT processes, MAS expects FIs to ensure adequate controls are implemented to ensure the reliability and security of the configuration management process. MAS will not be prescribing the expectation specifically for configuration management in the TRMG.

Technology Refresh Management (Section 7.3)

7.9 A respondent sought to clarify the maximum period which the FI could seek dispensation from its management to continue using outdated and unsupported hardware or software.

MAS' Response

7.10 MAS expects FIs to perform risk assessments to evaluate the risks of continued usage of outdated and unsupported hardware and software. MAS does not prescribe the timeframe in which FIs could continue to use such hardware and software but they are expected to establish effective risk mitigation controls.

Validity Period for Management Dispensations (Section 7.3)

7.11 A respondent was of the view that exceptions approved by management are typically not re-assessed even though there are changes in the FI's IT control environment and risk appetite. The respondent proposed specifying the validity period for approved exceptions and management

dispensations in the TRMG so that FIs could re-assess the risk of continuing practices which are not aligned with the established policies, procedures and standards.

MAS' Response

7.12 MAS expects FIs to periodically review exceptions that have been approved by management to ensure the risks remain at an acceptable level. MAS has revised the TRMG for better clarity.

Scope of Guidelines on Patch Management (Section 7.4)

7.13 A respondent commented that patching is a key control in securing systems from cyber attacks and suggested that additional guidance on management and monitoring of patches should be included.

7.14 The respondent also suggested highlighting key procedures such as identification, categorisation, prioritisation and deployment as part of the system patch management process.

MAS' Response

7.15 The TRMG comprises a set of key technology and cyber risk management principles, and best practices which FIs could adopt based on the nature, size and complexity of their business. It is the responsibility of the FI to ensure it has adequate processes and controls in place that are commensurate with the technology risks that they are exposed to.

7.16 MAS does not prescribe the type of procedures and controls that FIs are expected to implement so that FIs could determine the practices that are suitable for addressing their technology risks.

Assessment of System Patches (Section 7.4)

7.17 A respondent was of the view that the applicability of functional system patches that are released by product vendors should be assessed. In addition, the decision to implement a functional patch should be driven by its functional impact and risk to the FI's production environment rather than the need to implement every functional patch.

7.18 Another respondent highlighted that apart from just considering criticality of patches when prioritising them for deployment, FIs should include the security classification of systems (e.g. whether a system is critical or internet-facing).

MAS' Response

7.19 System criticality can be one of the criteria to be considered in the risk assessment performed to determine the functional system patches' implementation timeline.

Guidelines on the Turnaround Time for System Patching (Section 7.4)

7.20 A respondent was of the view that current system patching practices are reactive, and vulnerabilities are typically not addressed in a timely manner due to delays in system patching.

7.21 The respondent commented that there is a need to shift the existing approach towards patch management newly given that discovered vulnerabilities are exploited faster than in the past. Systems facing the Internet or end-user computing stations are typically exposed to more cyber attacks, and yet their patching often remains challenging due to manual processes. To enhance the resilience of the financial ecosystem, FIs should be capable of patching their systems once the patch is available.

MAS' Response

7.22 MAS agrees with the respondent's comment that system patching should be performed in a timely manner. While we do not mandate patch management to be automated, MAS expects FIs to ensure applicable function and non-functional system patches are implemented within a timeframe that is commensurate with the criticality of the patches and the FI's IT systems.

Testing of System Patches (Section 7.4)

7.23 A respondent enquired whether patches for servers and network equipment should be tested in non-production environments before implementation.

MAS' Response

7.24 MAS expects FIs to perform testing in a non-production environment before any system changes are implemented in the production environment.

Scope of Guidelines on Change Management (Section 7.5)

7.25 A respondent was of the view that guidelines on change management could be clearer on the risks that FIs should assess as part of their risk and impact analysis for changes. It was proposed that inter-dependent components in the FI's IT infrastructure, including upstream and downstream systems, should be included as part of the risk and impact analysis of any change.

MAS' Response

7.26 MAS expects FIs to ensure the risk and impact analysis of changes covers factors such as security and implications of the change in relation to other information assets. We wish to clarify that the scope of "information assets" encompasses the IT components that will be impacted by the change.

Change Advisory Board (Section 7.5)

7.27 A respondent was of the view that small FIs that have slim organisational structures may face difficulties in forming a change advisory board and recommended that the TRMG should focus on the involvement of business and IT management in the approval and prioritisation of changes to the production environment.

MAS' Response

7.28 The TRMG is a set of key security principles and best practices which FIs could adopt based on the nature, size and complexity of their business. It is the responsibility of each FI to ensure it has adequate processes and controls in place that are commensurate with the technology risks that they are exposed to.

7.29 The focus of the guidelines is on the involvement of business and IT management in approving and prioritising changes to the production environment.

Software Migration (Section 7.6)

7.30 A respondent enquired whether FIs should apply the same security controls for software migration between non-production and production environments to software migration that is performed between other types of IT environments.

MAS' Response

7.31 MAS expects the FI to ensure the clear accountability, traceability and integrity of software codes when they are migrated from one IT environment to another. We have revised the TRMG to reflect this principle on software migration better.

Incident Management Framework (Section 7.7)

7.32 A respondent commented that the TRMG should include clauses to emphasise the importance of collaboration across business, operations and IT functions in the response and recovery of IT incidents.

7.33 The respondent also proposed defining the roles and responsibilities as well as monitoring performance of staff and external parties who are responsible for incident management.

MAS' Response

7.34 MAS agrees with the respondent's comments. Hence, we have outlined in the TRMG that FIs should identify and establish the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents as part of its incident management framework.

External Assistance to Manage IT Incidents (Section 7.7)

7.35 A respondent enquired whether FIs are required to engage a permanent third party service provider to provide incident management services or FIs will be allowed to engage such third party services on a "need-to" basis.

7.36 Another respondent enquired whether the external assistance that FIs could engage include resources from their intra-group entities, such as their head office.

MAS' Response

7.37 FIs can engage external parties, including those from intra-group entities, to augment their resources to manage IT incidents. FIs should assess and determine whether the additional resources and expertise are required on a permanent or "need-to" basis.

Configuration of Security Events for Monitoring (Section 7.7)

7.38 A respondent was of the view that the guidelines on active monitoring of system events and alerts to address issues before they become incidents should be confined to critical systems as defined in the MAS Notice on Technology Risk Management.

MAS' Response

7.39 The intent of the guidance is for FIs to establish a comprehensive set of system events and alerts for monitoring, as well as a process and procedures to actively monitor and respond to system events and alerts. FIs may take a risk-based approach to identify systems that require active monitoring.

Incident Notification (Section 7.7)

7.40 A respondent was of the view that the TRMG should include regulators as one of the stakeholders to be notified of major incidents.

7.41 Another respondent suggested that the "Instructions on Incident Notification and Reporting to MAS" should be incorporated as part of the TRMG.

MAS' Response

7.42 The notification of incidents to the MAS is a requirement in the Notice on Technology Risk Management. Please refer to the applicable notice for your FI.

7.43 The "Instructions on Incident Notification and Reporting to MAS" is a guide for FIs on reporting the type of incidents as defined in the MAS Notice on Technology Risk Management to MAS. It will not be incorporated into the TRMG as the purpose of the two documents is different.

Additional Guidelines on Problem Management (Section 7.8)

7.44 Respondents commented that MAS should include additional guidance on the best practices in problem management that should be adopted by FIs.

MAS' Response

7.45 MAS' expectations on problem management are in Section 7.8 of the TRMG. Problem management is a continuation from incident management.

7.46 The problem management framework should encompass the process and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents, as well as the roles and responsibilities of staff and key stakeholders in problem management.

8 IT Resilience

System Availability (Section 8.1)

8.1 A respondent highlighted that the TRMG should emphasise the importance of designing systems for scalability, stability and resilience, and continuous system monitoring. It was also proposed to include system capacity requirements as part of the assessment on system scalability and recovery in technology refresh plans.

MAS' Response

8.2 MAS agrees with the respondent's comments. The TRMG provides guidance on designing systems that are scalable and resilient, and continuous system monitoring to facilitate prompt response to system events.

8.3 In the TRMG, FIs are expected to establish a technology refresh plan for the replacement of hardware and software. FIs may include system capacity considerations when planning for technology refresh. MAS will not be prescribing the assessment criteria for technology refresh in the TRMG.

High Availability (Section 8.1)

8.4 Respondents commented that the guidelines appear to imply that system redundancy or fault-tolerant solutions should be implemented for all the FI's systems to achieve high system availability. This would contradict the Notice on Technology Risk Management where the high availability requirement is only applicable for critical systems.

8.5 A respondent also highlighted that the term "high availability" should be defined as the interpretation of the term may differ for each FI. For example, an "active-passive" configuration may also be considered as "high availability" setup.

MAS' Response

8.6 MAS expects FIs to design and implement systems that will achieve the level of system availability that is commensurate with their business needs. We have revised the guidance to clarify on our intent.

Guidelines on the Review of System and Network Architectures (Section 8.1)

8.7 A respondent sought clarification on the scope of review that should be covered for system and network architectures in order for the review to be holistic.

MAS' Response

8.8 The review should include an assessment of the system and network design and controls; as well as an analysis to identify any potential single point of failure.

Guidelines on Capacity Management (Section 8.1)

8.9 A respondent sought clarification on whether guidelines on capacity management in the MAS Guidelines on Technology Risk Management, published in 2013, were moved to Section 8.1 of the TRMG.

MAS' Response

8.10 The guidelines on capacity management has been moved to Section 8.1 of the TRMG.

Approval of Disaster Recovery Plan (Section 8.2)

8.11 A respondent sought clarification on the term "management". The respondent highlighted that "management", who is responsible for approving the DR plan appeared to be different from "senior management" whose roles and responsibilities are defined in Chapter 3 of the TRMG.

8.12 It was suggested that MAS should consider including the board of directors or its delegated committee to provide oversight of DR planning of the FI, as well as review and endorse the recovery objectives of critical systems. This will align with the MAS Guidelines on Business Continuity Management which stated in Section 4.3 that the board of directors should "review and endorse, at least annually, the FI's critical business functions, business continuity objectives and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place".

MAS' Response

8.13 The IT DR plan and procedures may be approved by senior management, whose roles and responsibilities are defined in Chapter 3 of the TRMG or by a manager who is delegated by the senior management to oversee IT DR planning.

8.14 We agree with the respondents' feedback on aligning the expectations in the TRMG on the oversight of IT DR planning, as well as the review of recovery objectives, with the MAS Guidelines on Business Continuity Management.

Business Impact Analysis (Section 8.2)

8.15 Respondents sought clarification on whether the business impact analysis (BIA) mentioned in Section 8.2 of the TRMG is referring to the BIA that the FI is expected to conduct for business continuity management or a separate BIA to be performed for IT systems by the IT function.

8.16 A respondent also enquired whether the outcome of the BIA is expected to be used to identify critical systems as defined in the MAS Notice on Technology Risk Management.

8.17 Respondents commented that the expectations on BIA are already covered in MAS Guidelines on Business Continuity Management and they should not be replicated in the TRMG.

MAS' Response

8.18 FIs are expected to ensure the recovery objectives of IT systems are aligned with business objectives. This is facilitated by a BIA which is conducted as part of business continuity planning.

8.19 The results from the BIA can be used by FIs to assess and identify critical systems.

8.20 MAS agrees with the respondents' comments that the expectations on BIA in the TRMG are the same as the MAS Guidelines on Business Continuity Management and have removed them from the TRMG.

Disaster Recovery Scenarios (Section 8.2)

8.21 Respondents sought clarification on the scope of DR scenarios which should be included in an IT DR plan. One respondent enquired whether having procedures to cover site failure and single system failure will meet MAS' expectations on DR planning.

8.22 A respondent sought further guidance on MAS' expectations on the types of scenarios that will lead to "large scale disruption" and should be considered during DR planning.

MAS' Response

8.23 MAS does not prescribe the DR scenarios that should be included in the FI's IT DR plan. Depending on each FI's business needs, set up of IT environments and system inter-dependencies, the disaster scenarios that should be covered in the DR plan may differ from one FI to another.

8.24 MAS expects FIs to identify the disaster scenarios which could disrupt their businesses and operations, as well as delivery of services to customers. FIs should establish and test the recovery procedures for their systems based on the disaster scenarios.

8.25 The DR plan should cover the scenario of site failure. In addition, the FI should also consider other failure scenarios, such as outage of utilities and cyber attacks. In this regard, the FI should refer to its BIA when designing its DR plan.

Recovery Objectives (Section 8.2)

8.26 A respondent sought guidance on the recovery time objective (RTO) of critical systems.

8.27 Respondents commented that the definitions of RTO and recovery point objective (RPO) should be aligned with the MAS Guidelines on Business Continuity Management.

MAS' Response

8.28 Paragraph 6 of the MAS Notice on Technology Risk Management states that the FI shall establish an RTO of not more than 4 hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The bank shall validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing.

8.29 MAS noted the respondents' comment on the definitions of RTO and RPO. The terms used in the TRMG are aligned with the MAS Guidelines on Business Continuity Management.

Change in Recovery Approach (Section 8.2)

8.30 Respondents commented that there could be circumstances in an actual disaster where the FI may need to deviate from its DR plan and procedures, and were of the view that FIs should be allowed to take a different approach should the situation warrant it.

MAS' Response

8.31 The intent of the guidance is for FIs to adhere to their DR plan and procedures, which have been approved by their management and tested. This is to minimise the risk of using unfamiliar procedures to recover systems, which if unsuccessful could exacerbate the incident and prolong recovery efforts.

8.32 MAS agrees with the respondents that there may be circumstances that a deviation from the established plan and procedures may be necessary. FIs should then ensure any deviations in the recovery approach are assessed and approved by senior management before changes are made. MAS has revised the TRMG to include this guidance.

Scope of Disaster Recovery Testing (Section 8.3)

8.33 A respondent sought clarification on the scope of DR testing that the FI is expected to conduct. For instance, whether testing should cover all applications across multiple data centres (DCs). Another respondent enquired whether the expectations on DR planning are applicable only for critical systems.

8.34 One respondent highlighted that there is no consistent definition of the term "partial shutdown or incapacitation" among FIs and sought clarification on MAS' expectations when testing such a scenario.

8.35 Other respondents highlighted that it is not practical to require FIs to ensure DR arrangements for information assets that are managed by service providers are properly tested and verified to meet their business needs. This is because third party service providers are unable to commit to joint testing with individual customers. In addition, given the volume of customers they have, cloud service providers will not be able to participate in the DR exercises of all their customers.

8.36 Respondents commented that while service providers may not share their test results due to security and confidentiality concerns, the results are reviewed by independent third-party auditors. Some service providers also provide tools to assist FIs in establishing and testing of their DR plans and procedures.

MAS' Response

8.37 FIs should perform risk assessment to determine the criticality of their systems based on business requirements before deciding on the scope of DR testing.

8.38 The term "partial shutdown and incapacitation of primary site" is used as an example of a plausible scenario which could be included in DR testing.

8.39 MAS wishes to clarify that the intent of the guidance is for FIs to ensure adequate DR arrangements are established for the recovery of systems, regardless if they are outsourced or not. FIs may need to engage or involve its third party service providers as part of their DR testing if they are essential in providing support during a disaster. We have revised the TRMG to reflect this expectation.

Frequency of Disaster Recovery Testing (Section 8.3)

8.40 Respondents sought clarification on MAS' expectation on the frequency for DR testing.

MAS' Response

8.41 The objectives of conducting regular DR testing is to ensure staff and relevant stakeholders are sufficiently familiar with their roles, responsibilities, and activities that they are

expected to perform when DR is activated, and to verify that the technical measures implemented operate as planned during a disaster.

8.42 The frequency of DR testing should be determined based on these objectives and the FI's assessment of the criticality of its IT systems.

Disaster Recovery Test Scripts (Section 8.3)

8.43 A respondent sought clarification on the term "test scripts" in relation to the DR test plan.

MAS' Response

8.44 Test scripts are technical instructions used in system recovery. They would include the list of activities to be performed on systems to validate the recovery objectives.

Ability to Operate from Recovery, Secondary or Alternate Site (Section 8.3)

8.45 Respondents commented that the guidance for FIs to operate critical systems from the recovery or secondary site as part of DR testing should only apply for critical systems and sought clarification on MAS' expectation on the duration for operating at the recovery, secondary or alternate site.

MAS' Response

8.46 MAS' intent is for FIs to ensure systems that are hosted at the recovery or secondary site are able to continue to support their business needs as close to normal operations as possible during a disaster.

8.47 FIs should determine the duration which they should operate from the recovery, secondary or alternate site.

Stakeholders to Engage in Disaster Recovery Testing (Section 8.3)

8.48 A respondent sought clarification on the "key stakeholders" who should be involved in the DR testing.

MAS' Response

8.49 "Key stakeholders" refer to the management, relevant employees, vendors and anyone who should be involved in the DR activities and those who are responsible for making decisions during a disaster.

Testing of Backup Media (Section 8.4)

8.50 Respondents sought clarification on MAS' expectations on the scope and frequency of tests on backup media.

8.51 One respondent enquired whether the guidance to test backup media is applicable only for backup media that are stored offsite.

MAS' Response

8.52 MAS expects FIs to verify that all their systems and data backups can be effectively restored to meet their business needs regardless of whether the storage media are kept onsite or offsite.

8.53 FIs may take a risk-based approach and perform backup media testing based on a frequency that is commensurate with the criticality of the data.

Protection of Data in Backup Media (Section 8.4)

8.54 A respondent was of the view that encryption acts as an access control, since it secures data from unauthorised "read" operations. It was proposed that apart from data encryption, MAS should also include the need for physical access controls to be in place. The respondent highlighted that encryption also raised the need to outline the controls for cryptographic key management.

MAS' Response

8.55 FIs are expected to implement controls to protect confidential data in backup media from unauthorised access and modification, including physical access controls. Cryptographic key management is outlined in Chapter 10 of the TRMG.

Selection of Data Centres (Section 8.5)

8.56 A respondent enquired whether distance between the primary and secondary DCs should be a key criterion in the selection of the DCs' locations, given the limited number of telecommunications and DC service providers in Singapore.

8.57 The respondent also sought clarification on whether FIs are expected to use different service providers for the primary and secondary sites.

MAS' Response

8.58 The rationale for having DCs at different locations is to avoid the situation where a disruption could impact both the primary and secondary DCs due to the proximity of their physical locations. This is an area which the FI should take into consideration when selecting its locations to host its primary and secondary DCs.

8.59 FIs may engage the same service providers for both main and secondary sites.

Responsibility for Performing Threat Vulnerability Risk Assessment (Section 8.5)

8.60 Respondents enquired whether the threat vulnerability risk assessment (TVRA) for DCs should be performed by FIs, DC service providers or DC owners.

MAS' Response

8.61 FIs are responsible for ensuring that TVRAs are performed for their DCs. The FI may appoint a third party or its employees with the requisite knowledge and qualifications to perform a TVRA on the DC facility.

Scope of Threat Vulnerability Risk Assessment (Section 8.5)

8.62 Respondents suggested that MAS should provide more guidance on the scope of TVRA.

8.63 Some respondents enquired the scope of DCs which should be included in a TVRA. For instance, whether a TVRA is needed for a virtual DC i.e. a cluster of hypervisors on a server rack that are virtualised DC functions.

8.64 Respondents also enquired whether MAS expects a TVRA to be performed on both onshore and offshore DCs, and DCs hosting non-critical systems.

MAS' Response

8.65 MAS expects FIs to perform a TVRA on their DC before procuring the DC services and to ensure identified risks are adequately addressed. This can be achieved by obtaining and reviewing a current TVRA report from the DC service provider.

8.66 MAS expects FIs to perform TVRA on DCs regardless of whether they are located in Singapore or overseas, as long as the DCs support the FIs' Singapore operations.

8.67 MAS does not prescribe an exhaustive set of specifications on TVRA as the scope of assessment is dependent on many factors such as the criticality and the type of systems hosted at the DC. FIs may consider including the DC's perimeter, physical and environmental security, natural disasters, and the political and economic climate of the country in which the DC resides as part of the TVRA.

Network Diversification for Data Centres (Section 8.5)

8.68 A respondent commented that network resilience through the diversification of network paths is not necessarily guaranteed by engaging different external telecommunications service providers. From the FI's experience, it is acceptable to engage with the same external service provider to request for separate networks using different technologies and separate network paths to ensure network resilience.

MAS' Response

8.69 MAS agrees with the respondent's comments and has revised the TRMG by removing the expectation on FIs to engage different external telecommunications service providers for diversifying network paths.

9 Access Control

Definition and Applicability of Terms (Section 9.1)

9.1 Several respondents sought clarity on the definitions of the principles of 'never alone', 'segregation of duties', and 'least privilege'. Some requested the definitions of "user access" and "user management activities".

9.2 Some respondents highlighted that "critical system functions" may be confused with "critical systems" as defined under the MAS Notice on Technology Risk Management. A few respondents sought guidance on the criteria to identify critical system functions.

9.3 One respondent highlighted that the principles of 'never alone', 'segregation of duties', and 'least privilege' may not be applicable to all systems. Another respondent suggested modifying the expectation to apply these principles only to staff with access to perform critical system functions.

9.4 One respondent suggested extending the requirements on access control to contractors who are granted access to FIs' systems.

MAS' Response

9.5 MAS noted the feedback to request the definitions of the principles of 'never alone', 'segregation of duties', and 'least privilege'. The TRMG has been revised to include definitions on these terms.

9.6 MAS would like to clarify that "user access" refers to access for any types of users, including end user accounts as well as administrative accounts. "User management activities" refers to activities pertaining to user administration (e.g. creation, modification, deletion of user accounts).

9.7 MAS agrees that FIs may associate "critical system functions" with "critical systems". We wish to clarify that such critical system functions are not limited to those that exist within "critical systems" but also system functions that are of a sensitive nature, such as system initialisation and configuration, PIN generation and creation of cryptographic keys. MAS has replaced "critical system functions" with "sensitive system functions".

9.8 The principles of 'never alone', 'segregation of duties', and 'least privilege' should apply to sensitive system functions in all information assets. MAS would also like to clarify that these

principles should apply to staff, including contractors and service providers, who have access to at least one sensitive system function.

User Access Management (Section 9.1)

9.9 Some respondents asked whether FIs are allowed to use role assignment for the purpose of user access provisioning.

9.10 One respondent suggested that MAS should recommend the implementation of automated user access review.

9.11 Several respondents sought clarity on the parties responsible for authorising, approving and reviewing user access rights. Some suggested allowing delegates of the information asset owner, such as line managers to assume the responsibilities of the information asset owner to perform duties such as authorising, approving and reviewing access rights. Another respondent asked whether system owner or data owner should be the responsible party, and commented that access rights are typically approved by the system owner.

MAS' Response

9.12 FIs can adopt role-based access rights to grant users access to systems.

9.13 MAS does not prescribe the mechanisms for user access management or the party to perform access rights review. FIs should perform their own risk assessment to identify the appropriate party to authorise, approve and review user access rights.

Capturing and Retaining Logs (Sections 9.1 and 9.2)

9.14 Some respondents asked whether the requirement on logging of user access and user management activities applies to all systems, regardless of their criticality and functionalities.

9.15 A few respondents sought clarification on the expected retention period for system logs that record user and privileged access, as well as user management activities.

MAS' Response

9.16 FIs may take a risk-based approach to determine the user access and user management activities to be logged and maintained.

9.17 FIs are expected to determine the retention period of system logs based on the criticality of the system or service.

Strong Password Controls (Section 9.1)

9.18 A respondent highlighted that guidance on password controls issued by international standards setting bodies such as NIST or GCHQ (CESD) no longer recommended password complexity and maximum validity period controls.

9.19 One respondent suggested that the expectation on password controls should not apply to multi-factor authentication (MFA) where one of the factors is based on what the user knows.

9.20 Another respondent suggested amending the expectation on password controls given that some organisations no longer use passwords for authentication.

9.21 One respondent suggested adding an expectation to enforce a minimum password length of 20 alphanumeric character for service accounts, and recommending FIs to use Microsoft Managed Service Accounts or enterprise password vaulting solutions to manage privileged users, where possible.

9.22 A respondent commented that to reduce the risk of improper implementation of access control systems, FIs should aim to standardise their authentication and authorisation systems.

MAS' Response

9.23 MAS noted the respondent's feedback and would like to clarify that the controls are given as examples. We also noted the feedback that some organisations have progressed to non-password authentication methods. As many FIs still use passwords as a form of authentication, the guidance on password controls will remain in the TRMG.

9.24 MAS does not prescribe the design of controls or endorse any IT solutions. FIs should determine the appropriate authentication practices or solutions.

Applicability of Multi-factor Authentication (Section 9.1)

9.25 Respondents sought clarification on whether the expectation on MFA applies to only critical internet facing systems, or it includes critical systems that are not connected to the Internet.

9.26 A few respondents asked whether the expectation on MFA applies to staff and the FI's customers.

9.27 Several respondents highlighted that legacy systems such as AS400 may not have built-in support for MFA, and asked whether these systems could be exempted.

9.28 One respondent commented that alternative measures that are as effective as MFA should also be considered for critical systems, such as privileged access management solutions for password vaulting.

9.29 Another respondent asked if One-Time-Password (OTP) via the short-message-service (SMS) could be used as one of the factors for MFA.

MAS' Response

9.30 MAS would like to clarify that FIs are expected to implement MFA for access to sensitive system functions, regardless of whether the system is Internet-facing or otherwise.

9.31 The expectation on MFA in this section applies only to staff, including contractors and service providers who are given access to the FI's systems. The expectation on MFA for customer authentication is in Chapter 14 of the TRMG.

9.32 MAS noted the potential challenges in the implementation of MFA on legacy systems. FIs could utilise a third-party software application or appliance to implement MFA to control access to their legacy systems.

9.33 The use of privileged access management solutions will not fulfil the expectation of MFA if the authentication to the sensitive system functions relies on only one factor. Two or more unique and independent authentication factors must be implemented. Examples of authentication factors include an OTP that is generated from a hardware or software token or delivered through SMS, biometrics, unique device identity, digital certificate, and password.

Scope of User Access Review (Section 9.1)

9.34 One respondent suggested replacing the words "incorrectly provisioned access rights" with "inappropriate access rights" for the scope of user access review.

MAS' Response

9.35 MAS agrees with the feedback and has updated the TRMG accordingly.

Expectations on Third Party Service Providers and Scope of Monitoring (Section 9.1)

9.36 One respondent sought clarification on whether the expectations on user access management apply to third party service providers regardless of materiality and the nature of services subscribed by FIs.

9.37 Another respondent requested guidance on the expected level of monitoring for access to the FI's information assets.

MAS' Response

9.38 MAS would like to clarify that the expectations apply to third party services subscribed by FIs.

9.39 MAS does not prescribe the approach for monitoring. The FI is expected to conduct its own risk assessment to determine the appropriate scope and approach for monitoring.

Revocation of Privileged Access (Section 9.2)

9.40 One respondent sought clarification on whether the revocation of privileged access should be covered under Section 9.2 of the TRMG on Privileged Access Management.

MAS' Response

9.41 Revocation of user access has been covered under Section 9.1 of the TRMG on User Access Management, which includes privileged user access.

Applicability of Privileged Access Controls (Section 9.2)

9.42 One respondent asked whether legacy systems could be exempted from the expectations on privileged access management, such as granting access on a need-to-use basis, and logging and reviewing privileged user activities.

9.43 Another respondent sought clarification on whether FIs could determine the scope of privileged access review based on system criticality.

MAS' Response

9.44 FIs are expected to implement strong access controls to manage all privileged system access. The FI will have to assess the risks and implement appropriate mitigating controls should there be any constraints to meet our expectations.

9.45 FIs are expected to determine the scope of review based on the criticality of the system and may take a risk-based approach to review the privileged system access logs.

Potential Abuse of Privileged System Access (Section 9.2)

9.46 One respondent suggested rephrasing the line on "users granted with privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment", as it implied that all privileged users will end up abusing their privileged access.

MAS' Response

9.47 MAS would like to clarify that the paragraph is intended to highlight the potential scenario in which privileged user accounts are misused; as well as the controls that FIs are expected to implement to mitigate such a risk.

Review of Privileged Activities (Section 9.2)

9.48 One respondent commented that FIs have put in place preventive and detective controls (e.g. on-boarding background checks, strong access and authentication controls, logging of user activities) to limit the risk exposure of the organisation to employees and contractors performing privileged activities. The respondent further added that monitoring of privileged activities may not provide 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.

MAS' Response

9.49 The review of privileged activities serves as a detective control to identify unauthorised or unintended changes. FIs should ensure that the system logs capture adequate details to facilitate such reviews.

System and Service Accounts (Section 9.2)

9.50 One respondent commented that the term "system and service accounts" should be defined for better clarity.

9.51 One respondent suggested that the monitoring of the use of system and service accounts should only be applicable to interactive accounts.

MAS' Response

9.52 The term "system and service accounts" has been defined as accounts that are used by operating systems, applications and databases to access other systems' resources.

9.53 Malware are known to bypass controls and leverage on system and service accounts to perform malicious activities. MAS expects FIs to monitor such accounts to detect malicious activities and act promptly upon such detection.

Enhanced Privileged Access Controls (Section 9.2)

9.54 One respondent suggested including an expectation on establishing a process to periodically change passwords and digital certificates used by system and service accounts.

MAS' Response

9.55 The guidance on password policy and management of digital certificates are in Section 9.1 and Section 10.2 of the TRMG respectively.

Multi-factor Authentication for Remote Access to Externally Hosted Platforms (Section 9.3)

9.56 One respondent sought clarification on whether the use of MFA applies to externally hosted platforms (e.g. Software-as-a-Service) and internal platforms, and suggested that this expectation should be commensurate with the criticality of the external services.

MAS' Response

9.57 MAS would like to clarify that Section 9.3 of the TRMG refers to users connecting to the FI's internal network via an external network. Strong authentication, such as MFA, should be implemented for remote access to the FI's information assets.

Hardening of Devices (Section 9.3)

9.58 Some respondents proposed taking a risk-based approach in hardening devices that are allowed to access the FI's information assets remotely.

9.59 A few respondents asked whether the use of personal or non-corporate managed device and Virtual Desktop Infrastructure (VDI) solution to access the FI's information assets remotely should be disallowed.

9.60 Several respondents asked whether employees' personal devices are expected to be hardened if FIs have put in place protection measures such as encryption and MFA.

9.61 One respondent sought to clarify whether the guidance applies to insurance agents' devices.

9.62 Some respondents commented that other than hardening devices, approaches such as using a secure proxy (e.g. Citrix) and VDI can also secure remote access to the FI's information assets. Another respondent commented that instead of hardening devices, the focus should be on securing data.

9.63 One respondent suggested blocking off remote access to critical or sensitive information assets to minimise the possibility of data leakage and other security breaches.

MAS' Response

9.64 Remote access from an unsecured device to the FI's information asset could be used by attackers to gain a foothold into the FI's network, which may heighten the risk of unauthorised access to the FI's systems and data. In this regard, remote access to the FI's information assets should only be allowed from devices that have been secured according to the FI's security standards.

9.65 MAS would like to clarify that it is not our intent to prohibit the use of personal and non-corporate managed devices and VDI solutions. FIs are expected to implement data loss prevention measures on personal computing or mobile devices that are used to access the FI's information assets. This could be achieved through the use of mobile device or application management, as well as virtualisation solutions.

9.66 MAS expects FIs to perform their own risk assessment to ascertain the effectiveness of controls that are put in place to secure remote access to information assets.

Remote Access by Third Parties (Section 9.3)

9.67 One respondent recommended providing guidance for remote access to the FI's information assets by third-party service providers.

9.68 Another respondent commented that cloud service providers, who have remote access to FIs' information assets, will not be able to adhere to every customer's security standards. The respondent suggested that FIs should assess the service provider's security standards, controls and policies, and determine whether they are adequate.

MAS' Response

9.69 The expectations under Section 9.3 on Remote Access Management are applicable to remote access by third parties.

9.70 MAS agrees with the respondent that the FI should assess the adequacy of the service provider's security standards and controls. The FI should ensure the service provider's security standards and controls meet the FI's requirements.

10 Cryptography

Expectations on Cryptographic Algorithms (Section 10.1)

10.1 One respondent suggested replacing "sufficient length and randomness" for the seed or random number used in a cryptographic algorithm with the term "high entropy".

MAS' Response

10.2 MAS is of the view that the term "sufficient length and randomness" adequately reflects our expectation on securing the seed in cryptographic algorithms.

Testing or Vetting of Cryptographic Algorithms (Section 10.1)

10.3 Several respondents sought clarification on the scope of the testing or vetting process for cryptographic algorithms.

10.4 Some respondents suggested eliminating the need to perform testing or vetting, since FIs are expected to use cryptographic algorithms from well-established international standards.

10.5 A respondent enquired on the party who should be responsible for performing the testing or vetting of cryptographic algorithms. Another respondent asked whether cryptographic algorithms could be tested or vetted by third parties.

MAS' Response

10.6 MAS expects FIs to perform a risk assessment to determine the scope of testing or vetting. The rigour of the testing or vetting process should be commensurate with the criticality of the data that the cryptographic algorithms are used to protect.

10.7 While FIs are expected to use cryptographic algorithms from well-established international standards, they should determine the appropriateness of the cryptographic

algorithms, including the choice of ciphers, key sizes and key exchange control protocols. FIs should exercise judgment when reviewing the assessment provided by external parties and address any concerns before implementation.

Third Party Cryptographic Key Management Solutions (Section 10.2)

10.8 Some respondents enquired about MAS' views on the use of cryptographic key management solutions provided by third party vendors, including cloud service providers.

MAS' Response

10.9 FIs are expected to use cryptographic algorithms from well-established international standards. They should evaluate the appropriateness of the cryptographic algorithms and exercise judgment when reviewing the assessment provided by external parties.

Generation and Distribution of Cryptographic Keys (Section 10.2)

10.10 A respondent commented that the generation and distribution of cryptographic keys should be automated.

10.11 Some respondents sought clarification on whether asymmetric public keys should be distributed via an out of band channel or other secure means.

MAS' Response

10.12 MAS does not prescribe the means to manage cryptographic keys. FIs are expected to establish processes and procedures that ensure cryptographic keys are managed securely.

10.13 The objective of distributing cryptographic keys via either an out-of-band or secure channel is to minimise the risk of interception, and should be applied only to sensitive keys such as private keys. MAS notes the feedback and has revised Paragraph 10.2.5 of the TRMG.

Scope of Cryptographic Key Management Policy and Procedures (Section 10.2)

10.14 One respondent suggested including cryptographic key management standards as one of the key documents that FIs have to establish.

10.15 Another respondent suggested including key recovery within the scope of cryptographic key management policy and procedures.

MAS' Response

10.16 MAS has accepted the respondents' suggestions and revised the TRMG to include guidance for FIs to establish cryptographic key management standards. We have also included key recovery as part of the scope of cryptographic key management.

Destroying Cryptographic Keys (Section 10.2)

10.17 A respondent commented that the expectation to destroy sensitive materials that are used to derive the cryptographic keys prevents FIs from using key derivation functions (e.g. Diffie-Hellman or Elliptic Curve Diffie-Hellman) as mechanisms to generate (session) keys, which are based on long term key materials or passphrases.

10.18 The respondent opined that such long term keys should not be destroyed.

MAS' Response

10.19 MAS agrees with the respondent's feedback and has revised the TRMG to allow sensitive materials used to generate or derive keys to be either protected or securely destroyed after the cryptographic key has been generated. This allows FIs the flexibility to determine the appropriate approach to manage cryptographic keys based on the cryptographic algorithms used.

Lifespan of Cryptographic Keys (Section 10.2)

10.20 One respondent sought clarification on whether the term "lifespan" in Paragraph 10.2.3 of the TRMG is referring to the lifespan of the asset that the cryptographic key is used for.

10.21 One respondent highlighted that leading industry standards typically do not consider the sensitivity of data when determining the lifespan of cryptographic keys because such data is not available to the general industry. The respondent also commented that cyber threats that impact the lifespan of cryptographic keys are generally independent of data sensitivity levels.

MAS' Response

10.22 The term "lifespan" in Paragraph 10.2.3 of the TRMG refers to the lifespan of the cryptographic key.

10.23 MAS is of the view that the sensitivity of the data is a factor in determining the lifespan of a cryptographic key, but agrees that it is also important to consider the threats and risks that the data or system may be exposed to. The TRMG has been revised to include additional criteria for determining the cryptographic key's lifespan.

Authentication of Customer Passwords (Section 10.2)

10.24 One respondent suggested taking into account the shift towards authenticating customer passwords on server runtime instead of in the hardware security module, and commented that password authentication is not an activity typically performed by the hardware security module other than that for payment card applications.

MAS' Response

10.25 MAS has revised the TRMG to remove the expectation to authenticate customer passwords in the hardware security module.

Replacement or Renewal of Cryptographic Keys (Section 10.2)

10.26 One respondent commented that not all cryptographic keys should be generated independently from the previous key when replacing or renewing a cryptographic key. For example, identity-based encryption requires deterministic key derivation.

10.27 Another respondent suggested specifying in the TRMG the types of cryptographic keys that should be replaced after the compromise of a cryptographic key. The respondent is of the view that the scope should exclude cryptographic keys that are not reusable such as session keys used in past session negotiations.

MAS' Response

10.28 MAS agrees that not all cryptographic keys can be generated independently from the previous keys associated with them as some cryptographic algorithms derive one or more keys based on a single key such as a master key. We have revised paragraph 10.2.9 of the TRMG to state that when replacing or renewing a compromised or expiring cryptographic key, the FI should ensure any adversary who has knowledge of part or whole of the previous key will not be able to derive the new key from it.

10.29 We wish to clarify that the expectation on replacement of cryptographic keys applies only to those that FIs have assessed to be necessary for replacement or renewal.

Backup of Cryptographic Keys (Section 10.2)

10.30 Some respondents commented that it may not be necessary to maintain backups of all cryptographic keys due to the nature of the keys. For example, asymmetric signature keys that are generated in smart cards, can be easily replaced if corrupted or lost.

10.31 One respondent highlighted that the loss of cryptographic keys could be interpreted as either data loss or theft, and highlighted that restoring backups for recovery purposes is not an appropriate risk response in the case of data theft. The respondent proposed replacing the word "lost" with "deleted" for clarity.

MAS' Response

10.32 As a best practice, FIs should maintain backups of cryptographic keys for recovery purposes. FIs should perform a risk assessment and determine the types of keys that will adversely affect their operations if there are no recovery provisions.

10.33 MAS agrees with the respondent's comment on the potential misinterpretation of the loss of cryptographic keys. The term "lost" has been replaced with "unintentionally deleted" in Paragraph 10.2.10 of the TRMG.

11 Data and Infrastructure Security

Additional Guidance on Malicious Software, Phishing and Advanced Persistent Threat

11.1 A respondent proposed providing more guidance to FIs on security measures to protect against malware, phishing and advanced persistent threat (APT).

MAS' Response

11.2 The security principles and best practices in the TRMG are measures to guide FIs to protect against different types of cyber threats. MAS will not be prescribing the security measures to address the specific types of cyber threats.

Definition of Terms (Section 11.1)

11.3 Several respondents requested definitions of the terms "strong access controls", "confidential data", "sensitive data" and "mediums". Some proposed replacing "mediums" with "channels and devices" or "delivery channels and storage".

MAS' Response

11.4 Chapter 9 of the TRMG on Access Control states MAS' expectations on implementing strong access controls to protect systems and data.

11.5 Generally, customer information and transaction data are considered as "confidential" or "sensitive". As different FIs store and process different types of data, MAS expects FIs to determine the information which is deemed "confidential" or "sensitive".

11.6 MAS has replaced the term "medium" in Paragraph 11.1.4 of the TRMG with "data storage media, systems and endpoint devices" to provide better clarity on the devices that should be authorised for communications, transfer and storage of confidential data.

Scope of Endpoint Devices (Section 11.1)

11.7 Some respondents sought clarification on the scope of "endpoint devices" under the point on "data at rest", and commented that the TRMG should be limited to devices owned or managed by the FIs as FIs will not be able to manage personal devices.

MAS' Response

11.8 MAS wishes to highlight that the scope of endpoint devices include notebooks, personal computers, portable storage devices and mobile devices as stated in Paragraph 11.1.1 of the TRMG. These devices can either be issued by the FI or personal devices owned by the staff.

11.9 FIs should implement equivalent safeguards to personal computing devices that are used to access the FI's information assets.

Security Measures to Protect Data at Rest (Section 11.1)

11.10 One respondent asked whether there is a need to implement encryption at file level to protect data at rest.

11.11 Another respondent sought to clarify MAS' expectations in relation to the endpoint protection for data at rest in devices and data transmitted by general insurers' agents, who can represent up to three principals, to the insurers. The respondent also asked whether it is sufficient for insurers to have in place password protection for their documents and two-factor authentication for access to their systems.

MAS' Response

11.12 FIs may take a risk-based approach to determine the appropriate strategy and measures to meet the security principles. File level encryption is one of the security measures to protect data at rest.

11.13 Endpoint devices belonging to insurance agents may contain confidential and sensitive data. Hence, insurers should ensure these data are adequately protected.

Management of Systems and Endpoint Devices by Service Providers (Section 11.1)

11.14 One respondent sought clarification on whether the expectation on preventing and detecting data theft, as well as unauthorised modification in systems and endpoint devices applies to all service providers.

11.15 Several respondents expressed that FIs are unable to directly implement measures to prevent or detect events or breaches in information systems owned by their service providers.

MAS' Response

11.16 FIs should ensure they have adequate processes and controls in place that are commensurate with the technology risks that they are exposed to. Hence, FIs should exercise due diligence in ensuring their service providers implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices.

Data Theft (Section 11.1)

11.17 One respondent asked whether data theft is focused only on electronic theft and if it includes data theft via means such as photo-taking, screenshots, photocopying or hardcopies.

11.18 Another respondent commented that it will be challenging to detect and prevent all data theft. The respondent further added that this expectation could imply the need for a digital rights management solution to track digital records.

11.19 A respondent proposed using the term "deter" instead of "prevent" for data theft.

MAS' Response

11.20 The TRMG is focused on the management of technology risks, and theft of hardcopy files and data theft committed via photo taking and photocopying is not in scope.

11.21 The TRMG is intended to provide broad guidance and is not meant to be prescriptive. FIs are expected to determine the appropriate solutions to implement in order to adequately prevent and detect data theft.

11.22 MAS' view is that adequate preventive and detective controls should be implemented for data theft, and "deter" is not an appropriate term to reflect our intent.

Database-level Encryption (Section 11.1)

11.23 Several respondents expressed concern about the implementation of database-level encryption. One opined that database-level encryption is a recognised technical constraint and proposed the term "encrypted" to be replaced with "safeguarded". Another commented that database-level encryption could not be implemented for legacy databases.

11.24 Some respondents also commented that apart from encryption and access controls, other compensating controls are able to protect confidential data in databases, systems and end points.

11.25 Respondents suggested a risk-based approach in applying data encryption.

MAS' Response

11.26 Databases usually store large amount of data, including confidential and sensitive information. If compromised, it can result in serious consequences to the FI. FIs may apply a risk-based approach when determining the level of protection to be put in place to safeguard the database, as long as the controls are suitable and sufficient to address the risks.

Encryption of Data-in-use (Section 11.1)

11.27 One respondent asked whether data-in-use is expected to be encrypted.

MAS' Response

11.28 FIs are expected to implement strong controls to protect confidential and sensitive data. A risk assessment should be performed to determine if data-in-use needs to be protected when the data is being processed by applications. Data should only be in the clear when it is processed in a secure environment.

Unauthorised Internet Services (Section 11.1)

11.29 One respondent commented that depending solely on IT controls to prevent data loss is unlikely to be effective since not every endpoint device connected to the internet can be continuously inspected. The respondent further added that Paragraph 11.1.5 of the TRMG does not explicitly define who should authorise the type of internet services that the FI staff are allowed to use.

11.30 Another respondent commented that as public cloud matures in the Unified Communications and Collaboration space, many FIs will see this as an opportunity to deploy collaborative tools (MS Office 365 and One Drive, Gmail and Google Apps, etc.) to their users. The respondent suggested inserting "unapproved" or "unauthorised" before the terms "cloud-based internet storage sites" and "web-based emails".

MAS' Response

11.31 MAS expects FIs to implement appropriate processes and controls in managing data loss prevention, and not limited to IT solutions.

11.32 FIs may adopt the guidance outlined in Annex B Bring-Your-Own Device Security for devices that are not owned by the FI but are able to access the FI's network and systems.

11.33 MAS wishes to clarify that the intent of Paragraph 11.1.5 of the TRMG is about implementing safeguards to detect and prevent data from being moved to and stored on "unauthorised internet services". In this regard, if FIs deploy collaborative tools such as cloud-based internet storage sites and web-based emails for use within the organisation after obtaining management approval, such internet services would not be deemed as "unauthorised".

Use of Sensitive Production Data in Non-Production Environment (Section 11.1)

11.34 One respondent suggested excluding pseudo-production environment from the definition of "non-production environment" as controls for such environments are equivalent to production environments. The respondent clarified that the use of such environments is typically for pre-production mock run or testing for data conversion, data migration or full regulatory reporting, which would require production data to be included for verifications.

11.35 Some respondents also suggested specifying that sensitive production data should be prohibited from use in non-production environments where controls are less stringent than those in the production environments.

MAS' Response

11.36 The use of sensitive production data in any non-production environments should be restricted. Where production data need to be used in a non-production environment, proper approval has to be obtained from senior management. The FI should also ensure appropriate controls are implemented to prevent data leakage, and where possible, such data should be masked.

Removal of Data (Section 11.1)

11.37 Some respondents suggested that the TRMG should state that confidential data should be purged from any storage media or systems before the storage media or systems are destroyed, reassigned or transferred.

11.38 One respondent sought clarification on the minimum standards that FIs should adopt in order to irrevocably remove confidential data.

11.39 One respondent asked whether the expectation on removal of confidential data is applicable to vendors operating a multi-tenant environment (e.g. Office 365, AWS, etc.)

MAS' Response

11.40 MAS has revised the TRMG to include the expectation on the removal of confidential data prior to the destruction of the hardware.

11.41 FIs may adopt a risk-based approach in determining the most appropriate methods to irrevocably remove confidential data so that the data can no longer be recovered.

11.42 FIs should ensure that processes and controls are in place to remove confidential data from the vendor's environment when necessary.

Multi-tier Firewall or Web Application Firewall (Section 11.2)

11.43 A respondent asked whether there are any mandatory requirements to implement network security controls such as multi-tier firewall or web application firewall (WAF).

MAS' Response

11.44 MAS does not prescribe the type of network security controls that should be put in place. FIs should perform their own risk assessment and determine the appropriate strategy to adequately secure their network.

Alternative Network Security Measures (Section 11.2)

11.45 A respondent proposed adding guidance for FIs to specifically include network forensics and monitoring of network traffic within the internal network as part of network security capabilities.

MAS' Response

11.46 FIs should implement appropriate security measures to monitor the network traffic in its internal network to detect suspicious or anomalous traffic pattern.

Segregation of Information Assets (Section 11.2)

11.47 One respondent proposed replacing the phrase "segregate information assets" with "protect information assets" in Paragraph 11.2.2 of the TRMG.

11.48 A respondent commented that FIs should be allowed to assess whether they should implement internal segregation of information assets.

11.49 Another respondent commented that proper segmentation of the network is better achieved by segmenting by business function rather than by system criticality. Critical systems that support different business functions should not be hosted in the same segment in order to reduce lateral movement risk. Additionally, the respondent commented that FIs should consider the implementation of micro-segmentation or "zero trust network".

MAS' Response

11.50 MAS agrees with the respondent and has amended Paragraph 11.2.2 of the TRMG, which states that "To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets".

11.51 FIs should determine the most appropriate approach to manage its network security, which includes network segregation of systems, micro segmentation or the implementation of a "zero trust network".

Segregation of Information Assets (Section 11.2)

11.52 One respondent asked whether insecure network protocols, such as TELNET, can be used, granted that there are adequate compensating controls in place.

MAS' Response

11.53 Insecure protocols may heighten FIs' exposure to cyber threats. FIs should assess the risk of the continued usage of insecure protocols within its IT environment, and evaluate whether risks have been reduced to an acceptable level after applying the compensating controls and security measures.

Internet Surfing Separation (Section 11.2)

11.54 Several respondents expressed concern that prescribing Internet surfing separation (ISS) in the TRMG is overly prescriptive. A few of them opined that there are other ways to protect sensitive data, for example, anonymisation, encryption, MFA, content threat removal, micro virtual machines, etc.

11.55 Another respondent expressed concerns on the proposed "isolation" approach and suggested that MAS should consider other approaches which may be more sophisticated, effective and efficient. They recommended replacing the term "isolating" with "insulating" which explicitly allows for more sophisticated forms of isolation such as "isolating security zones" and similar concepts.

11.56 A few respondents sought clarification on the expectation of the ISS strategy, in particular whether either physical or logical separation would fulfil Paragraph 11.2.6 of the TRMG.

11.57 Some respondents asked whether the implementation of ISS applies to only systems handling critical business and system functions or containing sensitive data, or on all end-user computers and devices. There were further requests for guidance on the examples of systems that should be subject to ISS given the broad range of systems with internet access which handle critical business and system functions or contain sensitive data.

11.58 One respondent asked whether the expectation in Paragraph 11.2.7 of the TRMG would be similar to the mandatory control requirement on network segregation/isolation under the SWIFT Customer Security Controls Framework v2019.

11.59 A respondent highlighted that for such a limited applicability of ISS to be effective, it must be supplemented by equally strong controls to prevent lateral movement to the Internet-isolated systems using privileged credentials from other Internet-accessible systems.

MAS' Response

11.60 MAS advocates a defence-in-depth approach in cyber resilience and wishes to clarify that the implementation of ISS is meant to complement existing security controls and further enhance FIs' cyber defence capabilities.

11.61 The intent of the guidance on implementing controls for internet web browsing is to mitigate the risk of cyber attacks delivered to end users over the internet, which provides a conduit for cyber criminals to access the FI's IT systems.

11.62 FIs may consider isolating internet web browsing activities from its endpoint devices by using other devices that are not connected to their internal network or restricting the activities in a virtualised environment on devices that are connected to their internal network. FIs should assess and decide on the approach to protect its network and systems from cyber threats coming from the internet.

Denial of Service (Section 11.2)

11.63 A respondent suggested replacing the term "denial of service solution" with "denial of service protection" to reinforce the concept of protecting the FI's network from denial of service attacks.

11.64 Another respondent recommended including distributed denial of service (DDoS), to guide FIs in developing leading capabilities for technology risk management.

MAS' Response

11.65 MAS has revised the TRMG to replace "denial of service solution" with "denial of service protection".

11.66 MAS wishes to clarify that DDoS is listed as one of the examples of DoS attacks in the footnote.

Risks Arising from Deviations (Section 11.3)

11.67 Some respondents commented that deviations from standards do not necessarily constitute a risk.

MAS' Response

11.68 MAS wishes to clarify that while deviations from standards do not necessarily constitute a risk, the expectation is to ensure any risks arising from deviations are addressed adequately and in a timely manner.

Endpoint Protection (Section 11.3)

11.69 One respondent recommended including other practices and controls in the TRMG that can achieve the same objectives for endpoint protection. For instance, the implementation of endpoint detection and response (EDR) capabilities could facilitate forensics investigation.

11.70 A respondent suggested listing the different types of malware, such as adware, spyware, virus, ransomware and keylogger, in the TRMG.

11.71 One respondent asked whether Paragraph 11.3.3 of the TRMG is applicable to end user computers and devices which have direct access to critical systems.

11.72 A respondent suggested including the expectation to regularly scan systems for suspicious activities in the TRMG.

MAS' Response

11.73 FIs should determine the most appropriate strategy and controls to manage endpoint security.

11.74 The term "malware" in the TRMG refers to all types of malicious software and FIs should implement controls and processes to protect their network and systems against malware.

11.75 Paragraph 11.3.3 of the TRMG is applicable to all endpoint devices.

11.76 MAS agrees with the respondent that systems should be scanned regularly for suspicious activities, and has revised the TRMG.

Scanning of Indicators of Compromise (Section 11.3)

11.77 Several respondents commented that real time scanning of indicators of compromise (IOCs) may cause performance issues and suggested allowing FIs to adjust the scanning frequency based on their risk assessment.

MAS' Response

11.78 MAS agrees with the respondents that it may be operationally challenging to perform real time scanning of IOCs, and has revised the TRMG to clarify that such scanning should be performed in a timely manner.

Security Measures on Installation of Authorised Software (Section 11.3)

11.79 A few respondents sought clarification on whether "application white-listing" is just one example of the security measures that FIs should implement to ensure only authorised software are installed in systems.

11.80 A respondent commented that "application white-listing" may not be a viable approach for all FIs due the large and complex environments that many FIs operate in. Another respondent commented that application white-listing could be operationally onerous, as the range of software in systems may change over time; and the underlying components of the software could also change due to patching and version upgrade. As a result, it may require constant fine-tuning of the whitelist. Alternative measures such as advanced malware detection software should also be considered.

11.81 One respondent suggested expanding the examples of security measures to include blocking of portable extension files as they are potential sources of malicious codes.

MAS' Response

11.82 FIs should implement security measures to restrict installation of unauthorised software. Application white-listing is cited as an example of security measures to ensure only authorised

software are installed on the FI's systems. FIs may implement other measures that achieve the same objective.

Bring Your Own Device (Section 11.3)

11.83 One respondent suggested replacing the term "Bring-your-own-device (BYOD)" with "remote computing", as the underlying security principle is to ensure adequate security controls are in place before any devices, either owned by the user or the FI, to access the FI's corporate network remotely.

MAS' Response

11.84 MAS notes the respondent's comments and would like to clarify that it is MAS' intent to cover the security principles and best practices for managing BYOD and remote access in the TRMG.

Guidance on Virtualisation (Section 11.4)

11.85 A respondent commented that a hypervisor does not have an operating system interface, a controller feature or an operating system controller. Hence, it may not be possible to restrict administrative access as the configuration of virtual machines is performed via web interface on a remote client.

MAS' Response

11.86 A virtualisation solution could be made up of the following components: hypervisor, the host operating system and the guest operating system. MAS expects FIs to adopt the guidance outlined in Chapter 9 of the TRMG on Access Control to secure these accounts.

Scope of Internet-of-Things (Section 11.5)

11.87 Respondents commented that the scope of Internet-of-Things (IoT) covers a broad range of electronic devices. They were of the view that IoT standards are still being developed and suggested that the financial industry should develop a set of industry guidelines before security principles and best practices are included in the TRMG. One respondent commented that it is not necessary to include guidance specifically for IoT as the best practices in the rest of the TRMG are adequate for securing such devices.

11.88 Some respondents suggested that MAS defines the list of IoT devices that the TRMG is applicable to. They commented that FIs should be allowed to take a risk-based approach in managing IoT devices.

MAS' Response

11.89 The objective of including a section on IoT in the TRMG is to highlight specific risk areas and the associated best practices for securing IoT.

11.90 MAS notes respondents' comments that IoT security standards will need time to mature. MAS would not be providing an exhaustive list of IoT devices, as FIs are expected to implement processes and controls that are commensurate with the risks of using any type of IoT devices.

11.91 As IoT devices can access and transmit data to the internet, FIs should assess and manage the risks of using IoT devices.

Internet-of-Things Security (Section 11.5)

11.92 Respondents commented that it may not be possible to implement strong access controls for IoT as such controls may not be available or limited in these devices.

11.93 Respondents commented that it is challenging to maintain records on the physical locations of mobile devices and sought clarification on MAS' expectation.

11.94 Respondents also highlighted that not all IoT devices provide system activity logs and sought further guidance on MAS' expectations on performing log review for IoT devices.

11.95 Respondents suggested that the guidance should be revised to allow FIs to implement other measures to secure IoT devices.

MAS' Response

11.96 FIs should ensure the IoT devices that are connected to their networks are secure. Communication from IoT devices should be monitored so that FIs could detect and respond to suspicious activities in a timely manner. Information that will facilitate FIs in tracking or locating the IoT devices should be maintained.

11.97 If IoT devices do not have or have minimal security controls, FIs should assess whether they should allow such devices to be connected to their network, and implement appropriate processes and controls to mitigate the risks arising from such devices.

12 Cyber Security Operations

Management of Misinformation (Section 12.1)

12.1 Respondents highlighted that management of misinformation goes beyond technology risk management and should be managed as an enterprise risk. Some respondents were of the view that monitoring misinformation in cyberspace is too onerous on FIs.

12.2 Respondents also sought clarification on the definition of "misinformation" and enquired whether this is related to the Protection from Online Falsehoods and Manipulation Act.

12.3 A respondent enquired whether FIs are expected to take additional actions beyond those stated in the TRMG, for instance, notification of misinformation published about the FI to MAS.

12.4 Respondents enquired whether the engagement of external media monitoring services is a form of outsourcing.

MAS' Response

12.5 "Misinformation" refers to false statements of facts. The guidance on the management of misinformation is proposed to be included in the revised TRMG because misinformation may be easily propagated via the internet. Hence, as part of technology risk management, we expect FIs to establish a process to detect and respond to misinformation propagated on the Internet, so that the misinformation can be dealt with appropriately.

12.6 It is neither appropriate nor possible for MAS to exhaustively list specific actions that FIs should take when responding to online misinformation, as the assessment is dependent on many factors, including the nature of the misinformation. MAS expects FIs to ensure their actions are commensurate with the potential impact of the online misinformation. We will also be using the term "Internet", instead of "cyberspace" in the revised TRMG.

12.7 The guidance on mismanagement of information is independent of the Protection from Online Falsehoods and Manipulation Act 2019. Notwithstanding this, FIs should ensure they comply with the relevant laws and regulations in Singapore.

12.8 In assessing whether the procurement of media monitoring services is a form of outsourcing, FIs may wish to consider if the arrangement in which the services are procured is an "outsourcing arrangement" as defined in the MAS' Guidelines on Outsourcing.

Cyber Intelligence Sharing with Stakeholders (Section 12.1)

12.9 A respondent commented that as part of FIs' measures to raise cyber situational awareness, the TRMG should include guidance for the establishment of a cyber threat intelligence and information sharing process to share cyber threat intelligence with their counterparties and external stakeholders.

MAS' Response

12.10 The guidance recommended by the respondent is already in the TRMG. It is stated in Paragraph 12.1.1 of the TRMG that the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment and in Paragraph 12.1.2 of the TRMG that the FI should participate in cyber threat information-sharing arrangements with trusted parties.

Subscription of Cyber Intelligence Monitoring and Sharing Services (Section 12.1)

12.11 A respondent enquired whether there are any specific cyber intelligence monitoring and sharing services which FIs are expected to subscribe to.

12.12 Some respondents sought clarification on whether subscription of cyber intelligence monitoring and sharing services is a form of outsourcing.

MAS' Response

12.13 It is not MAS' intent to require FIs to subscribe to any specific cyber threat intelligence monitoring and sharing services. FIs are expected to assess and determine the appropriate measures to adopt to maintain cyber situational awareness.

12.14 FIs should assess whether the procurement of cyber intelligence monitoring and sharing services meets the definition of "outsourcing" in the MAS Guidelines on Outsourcing.

Scope of Cyber Monitoring (Section 12.2)

12.15 Respondents were of the view that real-time monitoring of cyber events should not be limited to only critical systems or internet facing systems as malicious actors will often identify the weaker links and easier targets, hence system monitoring should cover all systems.

12.16 Some respondents highlighted that the scope of system logs to review is too broad and proposed allowing FIs to determine the types of system logs or events to review using a risk-based approach.

MAS' Response

12.17 MAS agrees that monitoring of cyber events should not be limited to critical systems and updated the TRMG accordingly. FIs should assess and ensure the scope of cyber monitoring is commensurate with the risks to which a system is exposed to, as well as the criticality of the system.

12.18 FIs should identify the appropriate scope of system logs or events for continuous monitoring of cyber events and to facilitate prompt detection and response to cyber incidents.

User Behavioural Analytics (Section 12.2)

12.19 Respondents enquired whether FIs are expected to implement tools or solutions with capabilities, such as machine learning, to baseline system and user activities.

12.20 A few respondents were of the view that not all FIs have the capabilities or skills to implement user behavioural analytics and suggest that the guidance be revised to allow FIs the flexibility to determine how they should perform cyber monitoring.

12.21 Some respondents expressed their concern that profiling individual users could have legal, regulatory and privacy concerns that are not within the remit of technology risk management. There will also be jurisdictional requirements that need to be addressed, in particular for multinational FIs.

12.22 A respondent enquired whether the guidance also applies to the FI's customers.

MAS' Response

12.23 The TRMG is not meant to be prescriptive. FIs are expected to assess and determine the appropriate strategy and measures to ensure timely identification of suspicious activities in their IT environments.

12.24 User behaviour analytics is one of the security measures in the TRMG that FIs can implement.

12.25 MAS notes the respondents' concerns about the expectation to baseline user activities. MAS' intent is that FIs should implement controls to identify suspicious user behaviour and this could be achieved via user behaviour analytics.

12.26 The guidance does not cover FIs' customers. For the guidance on fraud monitoring on customer transactions, please refer to Section 14.3 of the TRMG.

Management of System Logs (Section 12.2)

12.27 Respondents requested for guidance on the retention period of system logs and how the relevant events in the system logs are to be reviewed. One respondent enquired whether the guidance is applicable only for production systems.

MAS' Response

12.28 MAS does not prescribe the log retention period. FIs should perform a risk assessment and determine appropriate retention period for its system logs.

12.29 We also do not prescribe specific actions that FIs should take when reviewing system logs, as the assessment is dependent on many factors, including the criticality and type of systems.

12.30 FIs are expected to identify and establish the controls, processes and procedures to manage system logs in production and other non-production systems. The controls, processes and procedures should be commensurate with the criticality of the FI's systems.

Cyber Incident Response and Management Plan (Section 12.3)

12.31 Respondents enquired whether the cyber incident response and management plan could be part of the IT incident response and management plan.

12.32 Some suggested including guidance on establishing a framework to categorise cyber incidents into different criticality levels, based on the severity and impact of the incident, which could facilitate incident response and escalation.

12.33 In addition, the respondents suggested including more details about the cyber scenarios that should be covered as part of cyber response, as well as the expectations on collaboration and coordination among various stakeholders.

12.34 The respondents opined that in order to improve its cyber incident response and management plans, the FI should assess and monitor the efficacy of the plan, as well as incorporate lessons learnt from cyber incidents in the plan.

MAS' Response

12.35 The cyber incident response and management plan can be part of the FI's incident management plan. FIs may take a risk-based approach to determine the coverage of its cyber incident response and management plan, as well as the appropriate strategy and measures to ensure timely response to cyber incidents.

Testing the Cyber Incident Response and Management Plan (Section 12.3)

12.36 A respondent sought clarification of the scope of tests expected on the cyber incident response and management plan.

12.37 Another respondent highlighted that testing has already been covered in Chapter 13 of the TRMG on Cyber Assessment and suggested removing the guidance on testing in Chapter 12.

MAS' Response

12.38 We agree with the respondent's suggestion to remove the part on testing the cyber incident response and management plan as it is covered in Chapter 13 of the TRMG.

13 Cyber Security Assessment

Cyber Security Assessment (Sections 13.1, 13.3)

13.1 Respondents enquired whether FIs must conduct cyber security assessments that are stated in Chapter 13 of the TRMG.

13.2 Respondents also sought clarification on whether the assessment could be conducted at a global level involving the relevant stakeholders in Singapore, or MAS expects the cyber security assessment to be performed by the Singapore office.

13.3 Another respondent asked whether the expectation in Paragraph 13.1.2 of the TRMG to identify "services that are not approved" as part of vulnerability assessment refers to the identification of system processes.

13.4 Some respondents proposed confining the guidance on vulnerability assessment to critical systems and web-based or internet-facing systems.

MAS' Response

13.5 Risk assessment of its IT environment should be integral to the FI's efforts in mitigating security threats and systems' security vulnerabilities. FIs may take a risk-based approach in determining the type and scope of cyber security assessment to conduct. FIs are expected to assess and determine the appropriate strategy and measures to identify security vulnerabilities in their IT environment.

13.6 FIs should conduct cyber security assessment, such as penetration testing, of its IT environment so as to obtain an accurate assessment of the robustness of their security measures.

13.7 The cyber security assessment may be conducted by the FI, its head office or a qualified external service provider.

13.8 The "services" in Paragraph 13.1.2 of the TRMG refers to system processes that are enabled but have not been approved by business, IT and other stakeholders in the FI.

Cyber Exercise and Business Continuity (Sections 13.1, 13.3)

13.9 Respondents commented that cyber exercise has been included as part of business continuity test and enquired whether FIs should still continue the practice, or MAS expects cyber exercises to be conducted separately.

MAS' Response

13.10 FIs are expected to conduct cyber exercises to validate its response and recovery, as well as communication plans against cyber threats. Such exercises may be conducted as part of the FI's business continuity plan test.

Tools for Cyber Security Assessment (Sections 13.1, 13.4)

13.11 A respondent pointed out that a combination of automated tools and manual techniques should be used to perform a comprehensive vulnerability assessment.

13.12 Another respondent enquired whether the adversarial attack simulation exercise could be conducted using automated and agent-based attack simulation software.

MAS' Response

13.13 FIs may use a combination of tools and techniques, either automated or otherwise, for vulnerability assessment and adversarial attack simulation exercise.

Penetration Testing and Red Team Exercises (Section 13.2)

13.14 Respondents were of the view that performing red team exercises and penetration tests in a production environment raises the operational risk of an FI as any IT disruptions could adversely impact the FI's operations. They commented that if the risks of conducting such tests outweigh its risk appetite, the FI should be allowed to conduct these tests in a non-production environment that is similar to the production environment.

13.15 The respondents also sought clarification on the scope of red teaming and penetration testing.

MAS' Response

13.16 MAS is of the view that penetration testing should be conducted in the production environment as a best practice in order to obtain a more accurate assessment of the robustness of the FI's security measures.

13.17 As the TRMG applies to FIs of varying size and complexity, it is not practical for MAS to prescribe the scope of red teaming and penetration testing. The intent of the guidance is to ensure adequate coverage in order to obtain an accurate evaluation of the robustness of the FI's cyber defences.

Adversarial Attack Simulation and Intelligence-Led Exercises (Sections 13.3, 13.4)

13.18 Respondents were of the view that the sections on adversarial attack simulation and intelligence-led exercises should be combined if intelligence-led exercise is also referring to adversarial attack simulation exercise.

MAS' Response

13.19 MAS has amended the heading of the section. Any cyber exercise can be conducted using intelligence-based scenarios.

14 Online Financial Services

Payment Card Security

14.1 A respondent sought clarification on the sections in the TRMG that cover the guidance on payment card security.

MAS' Response

14.2 The guidance on payment card security has been removed. The card issuing banks in Singapore have already fully migrated to chip cards. Measures to secure ATMs, payment card systems and networks are covered under Section 11.2 and 11.3 on Network Security and System Security respectively, as well as Chapter 14 on Online Financial Services.

Scope of Online Financial Services (Section 14.1)

14.3 One respondent asked whether online applications that are created to enhance customers' experience are included in the scope of "online financial services". In addition, the respondent asked whether informational online services are in-scope.

MAS' Response

14.4 Any online applications which provide information on and offer financial services are in the scope of online financial services. This also includes applications that are created to enhance customers' experience.

Protection against Code Injection Attacks and Cross-site Scripting (Section 14.1)

14.5 One respondent highlighted that controls to address malicious code injections and cross-site scripting are sufficiently covered by Paragraph 6.1.2 of the TRMG, such as input validation and output encoding. The respondent proposed removing references to malicious code injection and cross-site scripting in Paragraph 14.1.3 of the TRMG.

MAS' Response

14.6 The intent of the guidelines in Chapter 6 and Chapter 14 of the TRMG is different. Paragraph 6.1.2 of the TRMG provides examples of security controls to be covered in the secure code review of an application, while Paragraph 14.1.3 of the TRMG highlights the common cyber threats targeting Internet-facing applications, and FIs should assess and mitigate against such threats.

Distribution of Mobile Application or Software (Section 14.1)

14.7 One respondent commented that FIs do not distribute mobile banking applications to customers but rather, customers choose to download the FI's mobile banking application from the official mobile application stores.

MAS' Response

14.8 MAS agrees with the respondent's feedback. The intent of the guidance is about FIs making available mobile applications or software to customers through official mobile application stores, or other secure delivery channels. Paragraph 14.1.5 of the TRMG has been amended.

Phishing Campaigns (Section 14.1)

14.9 Some respondents asked whether FIs are required to report to law enforcement agencies on phishing attempts that impersonate the FIs and target the FI's customers. There were also other clarifications on the types of government agencies (e.g. Cyber Security Agency of Singapore, Singapore Police Force) as well as channels and avenues for FIs to notify government agencies of incidents arising from phishing campaigns.

14.10 Several respondents sought clarification on the extent which FIs 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.

14.11 A few respondents commented that it is impractical for FIs to monitor customers' emails or text messages as these take place outside the FIs' infrastructure. The respondents added that FIs are only able to take actions after they have received feedback from customers or through their own sources of intelligence.

14.12 Respondents highlighted that it may not be feasible for FIs to alert customers of every instance of phishing sites identified as numerous sites could be discovered daily.

14.13 Some respondents asked whether there is any requirement on the timeframe and channels (e.g. the FI's public website) to notify customers of phishing campaigns.

14.14 One respondent suggested that FIs should be encouraged to implement anti-phishing controls, such as Domain-based Message Authentication, Reporting and Conformance (DMARC) for emails.

MAS' Response

14.15 FIs should contact service providers to facilitate removal of phishing content from websites, or suspension of hosting services. FIs should also alert their customers of such campaigns and advise them of security measures to adopt to protect against phishing. MAS has removed the expectation of FIs reporting phishing incidents to law enforcement agencies (i.e. Singapore Police Force) from the TRMG.

14.16 FIs should assess and determine their strategy and protection measures to defend against various forms of phishing attacks, as well as the approach (i.e. guiding principles, timeframe and communication channels) for notifying customers of phishing campaigns as soon as practicable. FIs should use channels that are effective in communicating to their customers, such as their public websites, mobile applications, email and social media.

14.17 MAS agrees with the respondents' feedback that it is not practical for FIs to monitor their customers' emails or text messages. We have removed this guidance from the TRMG.

Rooted or Jailbroken Mobile Device (Section 14.1)

14.18 One respondent requested MAS to make a distinction between jailbroken devices and devices used for fraudulent transactions. The respondent opined that not all users who "jail break" their mobile devices are fraudsters as many users may choose to root their devices to attain greater flexibility while using their devices. The respondent suggested that MAS should revise the guidelines such that the FI is responsible for implementing security measures to safeguard their mobile applications against various scenarios where their users' devices have been compromised.

14.19 One respondent commented that the FI may not have the right to block its users from downloading and launching its mobile application on the users' devices. Another respondent suggested that apart from blocking rooted or jailbroken mobile devices, other controls could be implemented to mitigate the risk of malware and security vulnerabilities. For example, FIs could perform a risk analysis of devices which have been identified to be rooted or jailbroken. Based on the result of the risk analysis, the FI could determine whether further authentication is required before any transaction is allowed or to block the use of the application on the user's mobile device.

MAS' Response

14.20 MAS is of the view that while users may root their device for non-malicious purposes, these devices are more susceptible to malware and security vulnerabilities. Hence, as a best practice, FIs are expected to disallow rooted or jailbroken devices from downloading or accessing their mobile applications.

14.21 If the FI decides to allow its customers to use its applications on rooted or jailbroken devices, it should evaluate the risks and implement mitigating measures to address the risks.

Multi-Factor Authentication (Section 14.2)

14.22 One respondent asked whether FIs are expected to implement MFA for all customer authentication and whether the implementation can be based on the risk level of the financial activities.

14.23 Some respondents suggested that a risk-based approach should be taken with regard to the implementation of MFA for online financial activities. They recommended that MFA should only be required for high risk financial activities.

14.24 A respondent sought clarification on the use of OTP. The respondent further commented that many banks are showing full account information after login without two-factor authentication.

MAS' Response

14.25 FIs offer a variety of online financial services to their customers. The authentication factors or mechanisms implemented by FIs may vary depending on the type and risk assessment

of online financial services. For example, high risk or high value transactions typically require a higher level of identity assurance and authentication.

14.26 FIs may implement appropriate risk-based or adaptive authentication mechanisms that are commensurate with factors such as the risk level of the transaction and sensitivity of the information.

End-to-end Encryption (Section 14.2)

14.27 One respondent commented that customer authentication relying on OTPs, and PINs is inadequate in today's digital payment ecosystem. In order to prevent online fraud, the respondent recommended the use of real-time and multi-layered validation services to validate the security cryptograms used at various stages to secure the transaction (i.e. authentication, authorisation, clearing).

14.28 Another respondent commented that browser script-based password encryption is novel to Singapore. Where possible, requirements enabling equivalent protection of credentials should be achievable without FIs producing bespoke cryptographic methods, structures and code.

MAS' Response

14.29 The TRMG is technology agnostic and is not meant to be prescriptive. As stated in Paragraph 14.1.1 of the TRMG, FIs should implement security and control measures which are commensurate with the risks of online financial services.

Sensitive Customer Data (Section 14.2)

14.30 One respondent sought clarification on whether MAS' interpretation of "sensitive customer data" includes customer office and home address, email and telephone contact details. The respondent further commented that they may not necessarily identify them as sensitive data individually if the information cannot be used to uniquely identify an individual.

MAS' Response

14.31 The types of sensitive customer data listed are examples for FIs to consider as part of their risk assessments. The list is not exhaustive, and FIs should define and assess what constitutes sensitive customer data, as well as the potential impact to the FIs and their customers if the data is compromised.

Transaction signing (Section 14.2)

14.32 One respondent suggested taking into account PayNow which does not require any transaction signing. In addition, the respondent sought to clarify whether Paragraph 14.2.3 of the TRMG is applicable to merchant/bill payment.

14.33 A few respondents requested MAS to provide guidance on the criteria for determining activities as "high risk" so as to facilitate FIs' assessment on whether to implement transaction signing. One respondent highlighted that the examples provided in the TRMG may not necessarily be considered as high risk transactions that need transaction signing, for example, change of office address or email address.

14.34 Another respondent asked whether MAS is recommending any thresholds for high value funds transfer which requires transaction signing.

MAS' Response

14.35 MAS wishes to clarify that "transaction signing" is required for PayNow transfers that exceed the limit set by the participating FIs. Examples of high risk transactions include adding of beneficiary and changing of personal particulars.

14.36 In determining the manner of authentication, FIs should identify the types of transactions and the assessment criteria for each type of transaction that would qualify the transaction as "high risk". They may adopt a risk-based approach and implement appropriate measures (e.g. fund transfer limit, transaction signing, risk-based or adaptive authentication mechanisms, alternate controls and processes, etc.) that are commensurate with the risk level of the transaction and sensitivity of the information.

Adaptive Authentication (Section 14.2)

14.37 Some respondents requested MAS to provide examples of adaptive authentication.

MAS' Response

14.38 Adaptive authentication refers to authentication mechanisms that assess the risk of each transaction attempts and present customers with authentication options appropriate to the risk level. This gives FIs the ability to initiate "stepped up" authentication (e.g. by requiring additional authentication factors or mechanisms) for high risk transactions or activities.

Validity Period of One-Time Password (Section 14.2)

14.39 Several respondents sought guidance on the expected validity period of OTP.

MAS' Response

14.40 FIs are expected to assess and determine the validity period of OTP that is most appropriate for their online financial services. FIs should establish a time window that is as short as practicable to minimise the exposure of the OTP.

Biometric Solutions (Section 14.2)

14.41 Several respondents asked whether biometric solutions include those implemented by mobile phone manufacturers.

14.42 They opined that the protection of biometric information on users' mobile devices is not within the control of FIs. Therefore, they suggested that the expectation to secure biometric information should only be applicable to information that is managed by FIs. The respondents also commented that the device manufacturer should be primarily responsible and accountable to its customers with regard to the performance of the biometrics solution and the security of the biometric information on the device.

14.43 Some respondents sought clarification on whether FIs are expected to test the performance of the biometric solution, such as the false acceptance rate (FAR) and false rejection rate (FRR), or they could accept the performance of the biometric solution as represented by the vendor.

MAS' Response

14.44 FIs should perform their due diligence and assessment to ensure the third party biometric solutions they plan to acquire or use meet their security requirements. This includes biometric solutions that are installed on the devices by the device manufacturers.

14.45 The performance of the third party biometric solutions can be assessed based on the FI's internal testing or attestation from vendors. FIs are expected to assess the appropriateness and adequacy of the attestation provided by their vendors.

Software Token Provisioning Process (Section 14.2)

14.46 As part of the software token provisioning process, a respondent commented that the FI should verify whether its customer is using a rooted or jailbroken mobile device.

14.47 Another respondent suggested that the FI should alert the customer and verify the identity of the individual who requests for the software token to be provisioned before the completing the provisioning process.

MAS' Response

14.48 MAS does not prescribe the FI's operational procedures for provisioning software tokens. In paragraph 14.2.8 of the TRMG, verifying the identity of the individual is suggested as a control measure that the FI could implement during software token provisioning. FIs are expected to determine the appropriate approach to manage their software token provisioning process.

Issuance and Enrolment of Authentication or Transaction Signing Mechanism (Section 14.2)

14.49 Some respondents commented that no single control or process can address risks that are beyond the FI's control, e.g. a customer providing his login credentials to unauthorised parties.

MAS' Response

14.50 MAS agrees with the respondents' comments. The issues to address are about phishing and online scams targeting the public, and a holistic approach is needed to address these issues.

Pre-defined Session Time (Section 14.2)

14.51 Some respondents asked whether a session timeout should be implemented for all customers' logins since there are customers who need to keep their login sessions active for a long period of time.

14.52 Another respondent suggested that MAS should define the minimum requirement for the session timeout.

MAS' Response

14.53 MAS is of the view that as a best practice, a session timeout should be established. Online financial applications and customers should be required to periodically authenticate themselves. This will minimise the risk of idle sessions being hijacked and used for unauthorised activities.

14.54 FIs should assess the abovementioned risk and determine the appropriate approach to meet this security best practice, including the session timeout duration that is most appropriate for their services.

Operational Controls on Fraud Monitoring (Section 14.3)

14.55 One respondent suggested that MAS provides more guidance in the TRMG on fraud monitoring controls, processes and procedures to manage suspicious transactions or payments.

14.56 A respondent suggested including techniques such as artificial intelligence and machine learning to identify fraudulent activities. Another respondent sought clarification on whether this requirement covers all online transactions on all channels.

14.57 A respondent opined that it may be challenging to design rules to identify and block suspicious or fraudulent online transactions based on each customer's online behaviour. The respondent suggested that it would be more practical to formulate one set of rules for all customers.

MAS' Response

14.58 The TRMG is principle-based and not meant to be prescriptive. The guidance should be adopted where appropriate by the FI based on its operating environment.

14.59 FIs should assess and determine the fraud monitoring techniques and rules to monitor, identify and prevent suspicious or fraudulent online transactions. A "one-size-fits-all" set of fraud monitoring techniques and rules for all customers may not be effective in identifying suspicious or fraudulent online transactions. FIs could tailor rules for each customer or group of customers that are of similar risk profile for effective fraud monitoring.

14.60 Online financial services include banking, trading, insurance and payment services that are provisioned via the Internet. In this regard, FIs are expected to implement fraud monitoring controls for all online financial transactions.

Definition of Online Transactions (Section 14.3)

14.61 A respondent sought clarification on the definition of "online transactions" mentioned in Paragraph 14.3.1 of the TRMG.

MAS' Response

14.62 The term "online transactions" refer to transactions under the list of online financial services. The definition of "online financial services" has been provided in Paragraph 14.1.1 of the TRMG.

Platform to Share Information on Fraud (Section 14.3)

14.63 One respondent commented that it would be beneficial to have a platform for FIs to share information on fraud and mitigating actions as other FIs will be able to take the necessary measures to prevent similar fraud.

MAS' Response

14.64 FIs may make use of commercial or public cyber threat intelligence and information sharing platforms for this purpose.

Notification of Suspicious Activities (Section 14.3)

14.65 A respondent asked whether meeting the expectations on transaction notification that are stipulated in the MAS E-Payments User Protection Guidelines (EUPG) will fulfil the expectations on notification of suspicious activities in Paragraph 14.3.3 of the TRMG.

MAS' Response

14.66 The transaction notification guidelines in EUPG are for payment transactions. Paragraph 14.3.3 of the TRMG covers a broader scope of financial activities, including non-payment transactions such as change of address, email address and mobile number.

Customer Communication (Section 14.4)

14.67 Several respondents sought clarification on the types of changes to the security features of online financial services which FIs should inform their customers.

14.68 Some respondents asked whether it is sufficient to inform customers of such changes by including them as part of the general terms and conditions of the online financial services.

14.69 One respondent requested for more details on the types of cyber threats and incidents which the FI is expected to alert its customers. Another respondent asked if it is sufficient for the FI to inform its customers only if there is any incident impacting their accounts.

14.70 A respondent asked about the communication modes that FIs should use to alert and educate their customers.

14.71 A respondent proposed that efforts to raise customer awareness on the risks and security measures of online financial services should be organised at the industry level.

MAS' Response

14.72 FIs are expected to notify their customers of significant changes to the security features of their online financial services, such as those that impact customer authentication, transaction authorisation and transaction notification.

14.73 As stated in Paragraph 14.4.3 of the TRMG, FIs should educate their customers on their responsibilities in using online financial services and the appropriate security measures to protect their electronic devices which are used to access online financial services. FIs should also publish information on prevalent cyber threats (e.g. phishing and other forms of social engineering) targeted at online financial services.

14.74 FIs should use channels that are effective in communicating to their customers, such as their websites, mobile applications, email and social media websites.

14.75 MAS agrees with the respondent that customer education to raise awareness of cyber security should go beyond an individual FI. MAS, the Singapore Police Force (SPF), the National Crime Prevention Council (NCPC) and FIs have been making a concerted effort to proactively educate the public about the latest cyber developments, such as newly observed modus operandi of cyber threat actors. For the purpose of the TRMG, the focus is on the scope of customer education which FIs are expected to put in place.

15 IT Audit

Group IT Audit (Section 15.1)

15.1 A respondent sought clarification on whether IT auditors from the FI's head office could audit the FI's IT functions, processes and controls.

MAS' Response

15.2 MAS does not prescribe the composition of the IT audit team that should review the FI's IT functions, processes and controls. IT auditors from the FI's head office could audit the FI as long as they have the requisite qualifications and knowledge to provide an independent and objective assessment of the effectiveness of the FI's IT processes and controls.

Assessing the Competency of IT Auditors (Section 15.1)

15.3 A respondent sought clarification on the party, who is considered as appropriate for assessing the competency of IT auditors.

MAS' Response

15.4 FIs are responsible for conducting due diligence prior to the appointment of their staff. The FI's senior management should ensure the appropriate processes and procedures are in place to assess the competency and skills of its IT auditors.

15.5 When assessing the competencies of IT internal auditors, work experience and professional certifications can be taken into account.

IT Audit for Small FIs (Section 15.1)

15.6 A respondent suggested that MAS should provide other alternatives for small FIs, such as those with a headcount of less than 10, on fulfilling the audit expectations in the TRMG.

MAS' Response

15.7 FIs may adopt a risk-based approach when adopting the guidance in the TRMG. For FIs that do not have an IT audit function, they may engage external parties who are qualified to audit the IT processes and controls that support their operations.

Scope and Frequency of IT Audit (Section 15.1)

15.8 A respondent suggested that the scope and frequency of IT audit should be proportionate to the size and type of FIs.

MAS' Response

15.9 The scope and frequency of IT audits should be commensurate with the criticality of, and the risks from the extent that IT is used by the FI. The FI should perform a risk assessment of its IT universe to determine the frequency and scope of IT audit.

16 Annex A Application Security Testing

Application Security Testing

16.1 A respondent enquired whether it is mandatory to conduct Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST), as part of application security testing.

16.2 The respondent also enquired if DAST and IAST are required if a penetration test on the application has been performed.

MAS' Response

16.3 The types of application security testing listed in Annex A are examples for FIs to adopt. The list is not exhaustive, and FIs should assess and determine the types of application security testing to perform.

17 Annex B Bring-Your-Own-Device Security

Scope of Bring-Your-Own-Device

17.1 A respondent sought clarification on the types of electronic devices that are considered as BYOD.

17.2 Respondents enquired whether Mobile Application Management (MAM) could be considered as a substitute for Mobile Device Management (MDM) solution.

MAS' Response

17.3 BYOD refers to personal computing devices including notebooks, laptops, tablets and phones. It does not include corporate owned devices. MAS has revised "personal mobile devices" to "personal computing devices" in the TRMG.

17.4 MAM can be considered as an MDM-equivalent measure at the application level. MAS has revised the TRMG to include MAM in Annex B.

Virtualisation versus Mobile Device Management

17.5 A respondent highlighted that certain virtualisation and containerisation solutions are equivalent to MDM solutions in securing devices in BYOD arrangements.

MAS' Response

17.6 MAS does not mandate any specific measures to secure BYOD arrangements. FIs may adopt one or more of the recommended measures, or implement other equivalent safeguards to personal computing devices that are used to access the FI's information assets.

18 Annex C Mobile Application Security

Applicability of Mobile Application Security

18.1 Respondents sought clarification whether Annex C of the TRMG applies only to FIs offering online financial services to customers via mobile applications.

MAS' Response

18.2 The guidelines are not limited to online financial services offered to customers via mobile applications. This annex applies to all mobile applications developed or commissioned by the FIs.

Use of Sandbox or Container to Secure Mobile Application

18.3 Respondents sought clarification whether MAS supports the use of sandbox or container technology to secure mobile applications. They were of the view that it would be easier to secure mobile applications that are implemented in a container or sandbox.

MAS' Response

18.4 There is a variety of ways to implement "containers" or "sandboxes" for mobile applications. Rather than using generic terms, the TRMG covers the security mechanisms, of which some can be implemented within a "container" or "sandbox".

Storage or Caching of Data in Mobile Applications

18.5 In the TRMG, it was recommended that FIs avoid storing or caching data in their mobile applications to mitigate the risk of data security breaches on mobile devices. Respondents enquired whether the use of cookies would be considered as a form of data caching.

18.6 Respondents also enquired whether the guidance would be applicable to software token and secure storage on the mobile device.

MAS' Response

18.7 It is possible to store data in cookies and hence FIs should put in place measures to secure cookies. The Annex applies to all mobile applications developed or commissioned by FIs.

Clarification about In-App Keypad

18.8 Respondents sought clarification on the definition of the term "in-app keypad". A respondent also enquired whether all FIs' mobile applications must have their own build-in keypads or if the in-app keypad is only mandatory for keying in sensitive information.

18.9 A respondent was of the view that this guidance is prescriptive and suggested rephrasing the term "in-app keypad" to "security measures" to represent the mitigation against key logging malware.

MAS' Response

18.10 The term "in-app keypad" refers to keypad or software keyboard provided by the mobile applications for user inputs instead of relying on the keypad or keyboard mechanism provided by the mobile device.

18.11 MAS would like to clarify that Annex C sets out examples of mobile application security measures for FIs to consider and is not meant to be exhaustive. In-app keypad is one of the security measures that could be implemented to protect against keystroke capture.

Security Measures against Man-in-the-Middle Attack

18.12 A respondent was of the view that certificate pinning is not always possible in a micro-service architecture which involves multiple services.

MAS' Response

18.13 MAS would like to clarify that Annex C sets out the list of mobile application security measures for FIs to consider. Certificate pinning is one of the security measures that could be implemented to protect against MITM attack. The TRMG is not meant to be prescriptive. The guidance should be adopted, where appropriate, based on the FI's operating environment.

RESPONSE TO FEEDBACK RECEIVED ON PROPOSED REVISIONS TO TECHNOLOGY RISK MANAGEMENT GUIDELINES

JANUARY 2021

Monetary Authority of Singapore