Annex A List of Respondents to the Consultation Paper

A total of 79 submissions were received of which 7 respondents requested confidentiality of their identity, 4 respondents requested confidentiality of their submission and 35 respondents requested confidentiality of both their identity and submission.

*Respondents who requested confidentiality of their identity
#Respondents who requested confidentiality for their submitted response

1. AIA Singapore
2. AIG Asia Pacific Insurance Pte. Ltd.
3. Allianz Global Investors Singapore
4. Alpha Advisory Pte Ltd
5. Aon Singapore Pte Ltd, Aon Singapore (Broking Centre) Pte Ltd, Aon Benfield Asia Pte Ltd, Aon Hewitt Wealth Management Pte Ltd
6. Asia Cloud Computing Association (ACCA)
7. Asia Pacific Exchange Pte. Ltd. and Asia Pacific Clear Pte. Ltd. (collectively referred to as "APEX")
8. ASIFMA
9. Aviva Ltd
10. Deloitte & Touche Enterprise Risk Services Pte Ltd
11. Depository Trust and Clearing Corporation
12. Holland & Marie Pte. Ltd.
13. HSK Resources Pte Ltd
14. IG Asia Pte Ltd
15. Investment Management Association of Singapore (IMAS)
16. KPMG Services Pte Ltd
17. Life Insurance Association
    i. AIA
    ii. Aviva
    iii. Etiqa
    iv. Friends Provident
    v. FWD
    vi. Manulife
    vii. Prudential
    viii. Tokio Marine Life
    ix. Transamerica Life
18. Life Insurance Association ISCCS
    i. AIA
    ii. AXA
    iii. GE
    iv. Income
    v. Manulife
    vi. MSIG
19. Microsoft Operations Pte Ltd.
20. MRS
21. MSIG Insurance (Singapore) Pte. Ltd.

22. Oliver Wyman
23. Prudential Assurance Company Singapore
24. Prusik Investment Management Singapore Pte Ltd
25. RBC Investor Services Trust Singapore Limited
26. REIT Association of Singapore
27. RHT Compliance Solutions
28. Schroder Investment Management (Singapore) Ltd
29. SingCash Pte Ltd and Telecom Equipment Pte Ltd
30. StarHub Ltd
31. SWIFT
32. The Association of Banks in Singapore
33. Transamerica Life Bermuda Ltd
34. Cleartrade Exchange Pte. Ltd #
35. JLT Asia Pte. Ltd. #
36. QBE Insurance (Singapore) Pte Ltd #
37. PayPal Pte. Ltd. (3PL) #
38. An entity *
39. An entity *
40. An entity *
41. An entity *
42. An entity *
43. An individual *
44. An entity *
45. An entity #*
46. An entity #*
47. An entity #*
48. An entity #*
49. An entity #*
50. An entity #*
51. An entity #*
52. An entity #*
53. An entity #*
54. An entity #*
55. An entity #*
56. An entity #*
57. An entity #*
58. An entity #*
59. An entity #*
60. An entity #*
61. An entity #*
62. An entity #*
63. An entity #*
64. An entity #*
65. An entity #*
66. An entity #*
67. An entity #*
68. An entity #*
69. An entity #*

70. An entity #*
71. An entity #*
72. An entity #*
73. An entity #*
74. An entity #*
75. An entity #*
76. An entity #*
77. An entity #*
78. An entity #*
79. An entity #*

Please refer to Annex B for the submissions.

Annex B Submissions to the Public Consultation

SUBMISSIONS FROM RESPONDENTS TO THE CONSULTATION PAPER ON PROPOSED REVISIONS TO THE MAS TECHNOLOGY RISK MANAGEMENT GUIDELINES

Note: This table below only includes submissions for which respondents did not request confidentiality of their submissions.

S/N	Respondent	Feedback from respondent
1.	AIA Singapore	Under para 3.1.2 of the proposed revisions to the MAS Guidelines, it is stated that "Both the Board of Directors and Senior Management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats." We will like to seek the MAS' views, if providing adequate cybersecurity awareness training to the Board and Senior Management to enhance their understanding and management of technology or cyber risks would suffice to address the MAS' requirement above, or would the FI need to ensure that both the Board of Directors and Senior Management have members with the knowledge to understand and manage technology risks, including risks posed by cyber threats.
2.	AIG Asia Pacific Insurance Pte. Ltd.	Comments on IT resilience: 8.1.1: The cost to implement system redundancy to achieve high system availability would need to be balance with the cost. Is MAS' expectation that the FI should implement system redundancy only for critical systems? 8.1.2: How often does MAS expect an FI to conduct a holistic review of its system and network architectures? 8.1.4: Please clarify if MAS' expectation of high system availability is only for critical systems which support the FI's business. 8.2.2: There are numerous disaster scenarios for each business function that is supported by IT. Please clarify if MAS' expectation is only to critical systems which support the FI's business. 8.2.3: There could be circumstances where a different disaster recovery plan needs to be adopted in view of the disaster event. There should be leeway given to the management of the FI to take a different approach if the event warrants such a decision.

		8.3.1: What is the MAS' expectation on the frequency of testing for the DR plan? As IT supports many different business functions, it would not be viable for IT to test all DR plans annually. Is MAS' expectation for FI to test DR plans for only critical IT systems annually? 8.3.4: What is the "extended period" which MAS expect FI to operate from its recovery site?
		Comments on operational infrastructure security: 11.1.1: For general insurers, we have agents who can represent up to 3 principals. The devices used by agents are usually not issued by the insurer. As the agents use the same device to service their business with all the principals, please clarify MAS' expectations in relation to the end point protection for data at rest in these devices and data transmitted by agents to the insurer. Does it suffice that the insurer has in place password protection for document protection and 2FA for access of its systems? 11.1.6: Sensitive data is referred to throughout the Guidelines. What is MAS' definition of sensitive data? Does it refer to credit card and bank account details and in the case of para 14.2.3, customer office and home address, email and telephone contact details?
		Comments on IT project management and security-by-design: 5.1.2: Please clarify MAS' expectation for projects which are driven by regional or home office where the involvement of the local team is limited. 5.3.4: Please clarify that a source code escrow agreement is expected only if the FI determine that the software is critical to the FI's business.

		Comments on technology risk governance and oversight: 3.1.2: Please clarify what is the extent of knowledge which MAS expects the board of directors to have. 3.1.3: Please clarify what amounts to "key IT decisions". Also, to what extent does the MAS expect the board of directors and senior management to be involved? 3.1.5: Please clarify that the committee delegated the responsibility does not need to be a board committee. It could be the IT Security and Risk Management Committee, which is not a board committee. Unlike the function of internal audit which must be independent of the management, the CIO, CTO or Head of IT of an FI is appointed by the management or the IT function of the home office. We propose that the appointment responsibility should be left to the discretion of the FI so long as the person has the requisite expertise and experience. In some FIs, the CISO or Head of IS could be a regional person and the appointment is made by the regional or home office. We propose that the appointment responsibility should be left to the discretion of the FI so long as the person has the requisite expertise and experience. 3.2.1: What is MAS' expectation on the regular review and update of the FI's policies, standards and procedures? We are cognizant of the fact that certain policies, standards and procedures should be reviewed and updated at once a year but there are others where review and update need only be done when there are material changes to how the FI is organized or operate. The FI should have the discretion to decide. Information assets are defined to also include data, hardware and software used by service providers to deliver their services to the FI. It would not be feasible for FI to

		impose their policies, standards and procedures on service providers where the information assets are used to support different customers. What is MAS' expectation of service providers to FI eg cloud service provider, to comply with the FI's policies, standards and procedures. 3.3.2: Is there a specific manner or are there specific information fields which MAS require the FI to maintain the inventory in? Will MAS be providing a template or will it be up to the FI to decide? 3.4.1: Please clarify the nature and extent of the assessment. Will MAS be providing any guidance on its expectations? Third party is defined to include standardized and non-standardised services and products (eg power supply, telecommunications lines, commercial hardware and software, etc), Interconnected counterparties such as other institutions (financial or not) and FMIs (eg payment and settlement systems etc). Is an FI required to conduct assessment on these services? It is unlikely that such service providers would even render any assistance to FI to enable it to conduct the assessment. 3.4.2: Please clarify MAS' expectation of service provider to have relevant certification or accreditation that is recognised by the industry. Many Fintech companies may not have these certifications or accreditations. 3.5.1: Even with the right level of competence and skills, there may potentially be situations of human oversight or error. How will the MAS regard these instances which happen notwithstanding the best practices and efforts by the FI? 3.5.2: Please clarify if MAS' expectation for background check on personnel of service providers are for those with access to large amount of data. If a service is outsourced to a third party, please confirm if

		it is sufficient if the FI imposes the obligations on the service provider to conduct background check on personnel with access to FI's data. What types of background check is MAS expecting FI and its service providers to conduct on personnel? 3.6.2: Is online training sufficient or does MAS require classroom training? 3.6.3: Please clarify that the frequency of training for the board of directors is also at least annually.
		Comments on IT service management: 7.2.2: Is MAS' expectation that the review and verification be done at least annually? 7.7.2: An FI would identify external resources as part of its incident management framework. Please clarify if the engagement of external resources needs to be in place as part of its incident management framework. 7.7.7: Please clarify if MAS requires a separate IT incident response management plan if the FI already has in place an incident management plan.
		Comments on cyber security assessment: 13.3.1: What is MAS' expectations on the frequency of such exercises?
		Comments on technology risk management framework: 4.1.2: In the case of multinational FIs, please clarify that the risk owner can be a function in the regional or global office. 4.1.4: Does MAS expect FIs to review their risk management framework annually? 4.4.5: In any system or IT service, there is certain amount of risks remaining despite the effort by an FI to put in place

		controls and security measures. Please clarify MAS' expectation in terms of "adequate control" to be place before implementing a system or acquiring an IT service. 4.4.8: Please clarify MAS' expectation for regular review and update.
3.	Allianz Global Investors Singapore	Comments on IT project management and security-by-design: (P19) on 5.3.4 which requires source code escrow should be in place based on criticality We suggest MAS to also consider the practicality that such might not be possible for every single case. Therefore suggest the following: ''escrow could be an option based on criticality of the acquired software to the FI's business, and the practicability." (P21) on 5.8.2 regarding independent quality assurance function, the definition here is not so clear to us We like to clarify with the MAS on the expectation for independent quality assurance function, also practicality depending on the size of the FIs.
		Comments on software application development and management: (P25) on section 6.5 regarding the End User Computing application, which should be approved by relevant businesses AND IT management Suggest the MAS to change to 'approved by the relevant businesses with oversight by IT management'
		Comments on technology risk governance and oversight: (P13) On section 3.6.2, it is mentioned FI needs to include contractors and service providers as part of our security awareness training as well as background review

		We suggest the MAS to revise the section as the service providers have the responsibility to ensure they are adhering to FI's contractual agreement in regards to information Security and security training would fall under that responsibility as well.
		Comments on IT service management: (P27) on 7.4.2 it is mentioned 'ALL' patches should be tested before production Suggest to remove the 'all' term as this is too board in terms of coverage and whether risk-based approach would be more practical
		Comments on access control: (P36) on 9.1.5 for multi-factor, we made the same feedback in the previous MAS consultation paper on cyber hygiene We suggest a clearer definition of 'critical systems'. In that way, we would be able to scope a more meaningful list of systems, to further determine and apply multi-factor authentication.
4.	Alpha Advisory Pte Ltd	Comments on cryptography: Our office wi-fi is encrypted.
		Comments on IT resilience: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on operational infrastructure security: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very

		basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on IT project management and security-by-design: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on software application development and management: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on cyber surveillance and security operations: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on IT audit: We don't have anything to audit.
		Comments on application security testing: All applications are global, typical products - Microsoft and Bloomberg

		Comments on BYOD security: We have office owned desktops and laptops only.
		Comments on mobile application security: We don't use any mobile applications. Staff may read their office emails using their own mobile devices but cannot access any office data.
		Comments on online financial services: We don't use any.
		Comments on technology risk governance and oversight: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		General Comments: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on IT service management: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.

		Comments on cyber security assessment: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
		Comments on access control: All of our email systems use typical email (POP3) passwords. There is no external access to our data servers.
		Comments on technology risk management framework: The issue at hand is not terribly relevant for us - we are a small team providing advisory services with only the very basic use of technology (email, web, Bloomberg). All emails and data is backed up real time. Beyond this, we have no critical reliance on any technology.
5.	Aon Singapore Pte Ltd, Aon Singapore (Broking Centre) Pte Ltd, Aon Benfield Asia Pte Ltd, Aon Hewitt Wealth Management Pte Ltd	Comments on IT project management and security-by-design: Section 5 (IT Project Management), 6 (Software application) and 7 (IT Management). Aon comments: For large multinational corporations, such IT activities and resources are typically governed at the global level. While the Singapore financial institution might be involved in an IT project or development of a software, the risk assessment and application testing could be done at the global level given the resource allocation, and these activities will have to abide by the global standards. Such global standards may or may not fully comply with MAS guidelines. In that respect, we suggest that MAS allows for deviations from the MAS guidelines if the Singapore financial institution performs a risk assessment

		on such deviations and document its risk acceptance and mitigating controls (if applicable).
		Comments on software application development and management: Section 5 (IT Project Management), 6 (Software application) and 7 (IT Management). Aon comments: For large multinational corporations, such IT activities and resources are typically governed at the global level. While the Singapore financial institution might be involved in an IT project or development of a software, the risk assessment and application testing could be done at the global level given the resource allocation, and these activities will have to abide by the global standards. Such global standards may or may not fully comply with MAS guidelines. In that respect, we suggest that MAS allows for deviations from the MAS guidelines if the Singapore financial institution performs a risk assessment on such deviations and document its risk acceptance and mitigating controls (if applicable).
		Comments on technology risk governance and oversight: Para 3.1.2 board of directors to have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. Aon comments: While this guideline may be possible to comply for large financial institutions, it may be not be possible for other financial institutions that have a small Board composition to comprise members that have specific knowledge to manage technology risks. We would suggest that this requirement be met if either (a) the board of directors are

		guided by senior management members who have knowledge or specialise in management of technology risk, or (b) the board of directors have been trained by in-house technology risk professionals or external specialists on managing technology risk. 3.5.2 Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who has access to the FI's data and systems, should be performed to minimise this risk. Aon comments: Could MAS clarify the extent of the background check to be performed e.g. search against criminal records database, ML/TF lists, civil litigations etc? This requirement may not be practical in situations where there are frequent personnel turnover at the contractors and services providers' end, as that would mean financial institutions are expected to obtain updated lists of personnel changes on an ongoing basis for screening purposes. We would suggest that MAS allows financial institutions to adopt a risk-based approach according to the level of risks posed by its staff, contractors and services providers.
		Comments on IT service management: Section 5 (IT Project Management), 6 (Software application) and 7 (IT Management). Aon comments: For large multinational corporations, such IT activities and resources are typically governed at the global level. While the Singapore financial institution might be involved in an IT project or development of a software, the risk assessment and application testing could be done at the global level given the resource allocation, and these activities will have to abide by the global standards. Such global standards may or may not fully comply with MAS guidelines. In that respect, we suggest that MAS allows for deviations from the MAS guidelines if the

		Singapore financial institution performs a risk assessment on such deviations and document its risk acceptance and mitigating controls (if applicable).
6.	Asia Cloud Computing Association (ACCA)	Comments on IT resilience: Section 8.3.5: Testing of Disaster Recovery Plan As per the Guidelines, "where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and verified to meet its business needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems." With regards to this section, we would like to highlight that it would not be possible for CSPs to commit to joint testing of their disaster recovery and business continuity plans with individual customers. The mandating of joint testing would not only be impractical for hyperscale CSPs to abide by, but it would also take away from the intended efficiency gained by outsourcing certain services to CSPs. Similarly, CSPs should also not be required to get involved with the business continuity management exercises of their FI customers. CSPs and FIs have their own business continuity plans, which they implement independently and therefore there are no components that require joint testing. Also, given the volume of customers, hyperscale CSPs will be unable to participate in the business continuity management exercises of all their FI customers.
		Comments on IT resilience: Section 8.3.5: Testing of Disaster Recovery Plan As per the Guidelines, "where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and verified to meet its business

		needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems." CSPs regularly test their business continuity plans to ensure its effectiveness and determine the organisation's readiness to execute the plan. While CSPs may be unable to share the outcomes of this testing due to security and confidentiality risks, these results are reviewed by independent third-party auditors. CSPs can also look to provide a number of disaster recovery tools, e.g. facilitating short recovery times, to assist FIs with their disaster recovery plans and procedures.
		Comments on IT resilience: Section 8.3.5: Testing of Disaster Recovery Plan As per the Guidelines, "where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and verified to meet its business needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems." Comment #5: With regards to this section, we would like to highlight that it would not be possible for CSPs to commit to joint testing of their disaster recovery and business continuity plans with individual customers. The mandating of joint testing would not only be impractical for hyperscale CSPs to abide by, but it would also take away from the intended efficiency gained by outsourcing certain services to CSPs. Similarly, CSPs should also not be required to get involved with the business continuity management exercises of their FI customers. CSPs and FIs have their own business continuity plans, which they implement independently and therefore there are no components that require joint testing. Also, given the volume of customers, hyperscale CSPs will be unable to participate in the business continuity management exercises of all their FI customers.

		Comment #6: CSPs regularly test their business continuity plans to ensure its effectiveness and determine the organisation's readiness to execute the plan. While CSPs may be unable to share the outcomes of this testing due to security and confidentiality risks, these results are reviewed by independent third-party auditors. CSPs can also look to provide a number of disaster recovery tools, e.g. facilitating short recovery times, to assist FIs with their disaster recovery plans and procedures.
		Comments on IT project management and security-by-design: Section 5.3: System Acquisition Section 5.3.4 states that "A source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI" We ask that MAS further clarify the section on system acquisition to determine which entities the requirements apply to. From the current discussion in the Guidelines, it is unclear whether the requirements in this section apply to ongoing IT service contracts, such as cloud computing services. If yes, then we would like to highlight that some of the provisions in this section will be challenging for CSPs to abide by. For instance, an escrow arrangement (as mentioned in Section 5.3.4) with a single FI is not feasible under a cloud services model because the source code is strictly confidential and may be used on a one to many basis to provide services to all of the CSP's customers. Furthermore, it may not be possible to put in place a source code escrow arrangement (even outside of the cloud services model) due to the potential intellectual property rights associated with the relevant software. Given this, the risks associated with the FI no longer being able to use the acquired software, is a matter that should be covered under the FI's due diligence and business continuity management practices.

		The ACCA therefore recommends that the Guidelines include a definition of the term "System Acquisition" to help FIs determine which types of IT vendors these requirements apply to. We also suggest that Section 5.3.4 be amended to propose that FIs continue to monitor the service provider's ability to provide services and establish an effective business continuity plan and/or exit strategy for instances where the service provider is no longer able to deliver services.
		Comments on IT project management and security-by-design: Section 5.3: System Acquisition Section 5.3.4 states that "A source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI" Comment #4: We ask that MAS further clarify the section on system acquisition to determine which entities the requirements apply to. From the current discussion in the Guidelines, it is unclear whether the requirements in this section apply to ongoing IT service contracts, such as cloud computing services. If yes, then we would like to highlight that some of the provisions in this section will be challenging for CSPs to abide by. For instance, an escrow arrangement (as mentioned in Section 5.3.4) with a single FI is not feasible under a cloud services model because the source code is strictly confidential and may be used on a one to many basis to provide services to all of the CSP's customers. Furthermore, it may not be possible to put in place a source code escrow arrangement (even outside of the cloud services model) due to the potential intellectual property rights associated with the relevant software. Given this, the risks associated with the FI no longer being able to use the acquired software, is a matter that should be covered under the FI's due diligence and business continuity management

		practices. The ACCA therefore recommends that the Guidelines include a definition of the term “System Acquisition” to help FIs determine which types of IT vendors these requirements apply to. We also suggest that Section 5.3.4 be amended to propose that FIs continue to monitor the service provider’s ability to provide services and establish an effective business continuity plan and/or exit strategy for instances where the service provider is no longer able to deliver services.
		Comments on technology risk governance and oversight: Section 3.3.1 requires an FI to establish an information asset management framework that includes the "identification of information assets that support the FI’s business and delivery of financial services”. However, the scope of “information assets” in this clause is too broad and may also include the information assets used by FIs to enable the provision of third-party services. We thus recommend that MAS clearly define the scope of information assets to include only those information assets that are owned by the FIs. This will help clarify the responsibilities of the FIs to comply with the requirements in the Technology Risk Management Guidelines. Regulations should recognise that different forms of outsourcing exist, and that taking the same approach towards all types of outsourcing, may not account for the unique features of hyper scale cloud services. These features include the following: (1) the services are highly scalable and provided on a one to many basis which means the services operate the same way for all customers; (2) the responsibility for maintaining the security of the services is shared between the service provider and the FSI; (3) FSIs retain full control and ownership over the content they store and process using the cloud services; and (4) the service features and offerings can be configured by the FSI to achieve its availability, redundancy and security requirements.

		Comments on technology risk governance and oversight: Section 3.4.1: Management of Third-Party Services This section states that "The use of certain third-party services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third-party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third-party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks." The ACCA recommends that the Guidelines also highlight that to conduct these assessments, FIs may adhere to international best practices, including the use of independent third-party audit reports. This allows FIs to validate that a CSP's services and security controls align with international standards and ensure that the confidentiality of the systems of the CSP and its customers (including FIs) is maintained.
		Comments on technology risk governance and oversight: Section 3.6.2: Security Awareness and Training As per this section, a comprehensive IT security awareness training programme "should be conducted at least annually for all staff, contractors and service providers who have access to FI's information assets." We would like to highlight that security and compliance is a shared responsibility between the service provider and customer. This shared model can help reduce a customer's burden as the service provider can operate, manage and control all components of the operating system, including the physical security of the facilities in which the services run. FIs can look to published independent third-party reports to conduct their due diligence on the security practices of a cloud service provider (CSP).

		We therefore propose that the MAS clarify that FIs can rely on independent third-party reports to assess the level of security awareness and training practices.
		Comments on technology risk governance and oversight: Section 3.3: Management of Information Assets Definition of information assets (Footnote 3 on P.11): “Information assets include data, hardware and software. Information assets are not limited to those that are owned by the FI. They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI.” Comment #1: Section 3.3.1 requires an FI to establish an information asset management framework that includes the "identification of information assets that support the FI’s business and delivery of financial services”. However, the scope of “information assets” in this clause is too broad and may also include the information assets used by FIs to enable the provision of third-party services. We thus recommend that MAS clearly define the scope of information assets to include only those information assets that are owned by the FIs. This will help clarify the responsibilities of the FIs to comply with the requirements in the Technology Risk Management Guidelines. Regulations should recognise that different forms of outsourcing exist, and that taking the same approach towards all types of outsourcing, may not account for the unique features of hyper scale cloud services. These features include the following: (1) the services are highly scalable and provided on a one to many basis which means the services operate the same way for all customers; (2) the responsibility for maintaining the security of the services is shared between the service provider and the FSI; (3) FSIs retain full control and ownership over the content they store and process using the cloud services; and (4) the service features and offerings can be configured by the FSI

		to achieve its availability, redundancy and security requirements.
		Comments on technology risk governance and oversight: Section 3.4.1: Management of Third-Party Services This section states that "The use of certain third-party services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third-party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third-party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks." Comment #2: The ACCA recommends that the Guidelines also highlight that to conduct these assessments, FIs may adhere to international best practices, including the use of independent third-party audit reports. This allows FIs to validate that a CSP's services and security controls align with international standards and ensure that the confidentiality of the systems of the CSP and its customers (including FIs) is maintained.
		Comments on technology risk governance and oversight: Section 3.6.2: Security Awareness and Training As per this section, a comprehensive IT security awareness training programme "should be conducted at least annually for all staff, contractors and service providers who have access to FI's information assets." Comment #3: We would like to highlight that security and compliance is a shared responsibility between the service provider and customer. This shared model can help reduce a customer's burden as the service provider can operate, manage and control all components of the operating system, including the physical security of the facilities in which the services run. FIs can look to published

		independent third-party reports to conduct their due diligence on the security practices of a cloud service provider (CSP). We therefore propose that the MAS clarify that FIs can rely on independent third-party reports to assess the level of security awareness and training practices.
		General Comments: Dear Sir/Madam, Re: Asia Cloud Computing Association (ACCA)'s Response to MAS' Consultation Paper on Technology Risk Management (TRM) Guidelines The Asia Cloud Computing Association (ACCA) would like to thank the Monetary Authority of Singapore (MAS) for the opportunity to provide comments on its Consultation Paper on Technology Risk Management (TRM) Guidelines. We commend the MAS for working towards providing a trusted and robust financial services environment. As the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem, we represent a vendor-neutral voice of the private sector to government and other stakeholders. Our mission is to accelerate the adoption of cloud computing throughout Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. We are committed to strengthening cybersecurity resilience, and developing a robust technology ecosystem which supports a vibrant digital economy. Following discussions with our member companies, we are submitting comments on the Consultation Paper. I would be happy to speak further with MAS on any of these items, or host a vendor-neutral discussion between MAS and other members of the industry from the ACCA, to provide feedback. Please feel free to contact me if this is of

		interest. I look forward to hearing from you, and welcome your response on the issues raised. Yours sincerely, Lim May-Ann Executive Director Asia Cloud Computing Association mayann@asiacloudcomputing.org
7.	Asia Pacific Exchange Pte. Ltd. and Asia Pacific Clear Pte. Ltd. (collectively referred to as "APEX")	Comments on technology risk governance and oversight: The reporting structure of CISO may affect the collaboration with other business departments, budgets and priorities of the security projects. May we suggest that MAS set some expectations on the reporting structure of CISO.
		Comments on access control: May we suggest that the monitoring of the use of system and service accounts to be only applicable if those system/service accounts can be used by users to logon to systems. For example, if certain service accounts do not allow user interactive logon, such monitoring is not necessary.
8.	ASIFMA	Comments on cryptography: • 10.1.1 The FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements. Cryptographic algorithms (e.g. 3DES, AES, etc.) are selected based on industry best practices or advisory papers issued by authoritative sources (e.g. NIST); instead of rigorous testing to be performed by FI of cryptographic algorithms, it would be more pragmatic to use industry recognized strong encryption standard (implied in 10.1.1) and keep abreast of encryption vulnerabilities (10.1.3)

		• 10.2.1 A cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established. FIs are unlikely to need a policy for cryptography, just a technical standard. Suggest rephrasing section to "a cryptographic key management policy or technical standard and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established. • 10.2.4 The FI should ensure the systems that store the cryptographic keys and authenticate customer passwords are hardened and tamper resistant, e.g. hardware security module. Outside the payment card applications, password authentication is not an activity typically performed by HSMs. To reduce ambiguity, separate treatment should be given to password authentication versus payment card applications.
		Comments on IT resilience: • 8.1.2 A holistic review of the FI's system and network architectures should be performed to identify any potential single point of failure, and implement appropriate measures to address and mitigate the risk of disruption. Suggestion for MAS to provide guidance on the meaning of "a holistic review".
		Comments on IT resilience: • 8.1.3 It is particularly important for an FI which operates systems that support real-time transactions to proactively measure and monitor the utilisation of its system and network resources against a set of pre-defined thresholds 15. Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs, or to identify

		anomalous system or network behaviour for prompt investigation. The 2013 TRM Guidelines included capacity management under ITSM framework. 2019 TRM does not include capacity management. Is this an intentional omission? Is capacity management intended to be covered by 8.1.3 under IT Resilience?
		Comments on IT resilience: • 8.2.1 The FI should perform a business impact analysis to determine its business resumption and system recovery priorities in events where an IT incident leads to large scale service disruption. The FI's systems' recovery time objectives (RTO) and recovery point objectives (RPO), should be defined according to its business needs. We request for the MAS to provide clarity whether this clause should be read on top of the MAS Business Continuity Management (BCM) Guidelines. We suggest that alignment to new requirement from MAS BCM consultation paper should be included or referenced for clarity.
		Comments on IT resilience: • 8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management, and avoid taking untested recovery measures which are likely to carry higher operational risks. • We suggest there is no need to mention the option of taking untested recovery measures. and suggest rephrasing to "8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management." • Could MAS clarify what it means by "untested recovery measures"

		Comments on IT resilience: • 8.3.2 A disaster recovery test plan should include the test objectives and scope, test scenarios, test scripts with details of the activities to be performed during and after testing, test scripts with details of the activities to be performed during and after testing, system recovery procedures, and the criteria for measuring the success of the test. With reference to “criteria for measuring the success of the test”, there is currently no industry-wide methodology to measure the success of an RPO. Therefore, we would recommend that further guidance be issued on this in consultation with FIs.
		Comments on IT resilience: • 8.3.3 The testing of disaster recovery plans should comprise: a. Various plausible disruption scenarios, including full and partial shutdown or incapacitation of the primary site and major system failures; and b. Recovery dependencies between information assets, including those managed by third parties. Further clarification is requested for "partial shutdown or incapacitation" and if the definition is consistent among all FI's. For example, partial shutdown could include high availability cluster fail testing within the same data center or partial loss of a data center requiring failover to another data center.
		Comments on IT resilience: • 8.3.4 If the system and network architectures support load balancing and high availability, the FI should operate from its recovery site for an extended period as part of disaster recovery testing to gain the assurance and confidence that its recovery site is able to support business needs.

		Further clarification is requested on the “extended period”. Does this mean a few hours or one day?
		Comments on IT resilience: • 8.4.3 The FI should periodically restore its system and data backups to validate the effectiveness of its backup restoration procedures... We recommend that this requirement reads: “periodically test the ability to restore its system and data backups to validate the effectiveness of its backup restoration procedures.” The test is up to the FI and should not particularly require the live production environment.
		Comments on IT resilience: • 8.5.1 The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats. In addition, the TVRA should consider the political and economic climate of the country in which DCs is located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC’s environment. Clarification on whether TVRA should be done by an independent entity or can it be done in-house.
		Comments on IT resilience: • 8.5.6 The DC should have adequate physical access controls including: (a) access granted to staff should be on a need-to-have basis, and revoked immediately if access is no longer required. Propose to replace the word “immediately” with “promptly”

		(d) access to equipment racks should be recorded, monitored and supervised at all times; • Can MAS clarify what kind and to which extent the monitoring of access to equipment racks is expected? • Suggestion to reword the “recorded, monitored, and supervised” as it is redundant, to “Access to equipment racks should be adequately controlled and have adequate surveillance in place.”
		Comments on operational infrastructure security: • 11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following: a. data in motion - data that traverses a network or that is transported between sites; and b.data at rest - data in computing endpoints such as notebooks, personal computers, portable storage devices and mobile devices, as well as files stored on servers, databases, backup media and storage platforms (e.g. cloud). Clarity on the scope of "Endpoints" for "Data at Rest" required as these guidelines should be limited to devices owned and/or managed by FI as FI cannot manage personal devices used by FI resources from an endpoint perspective (11.1.1) Alternatively, consider including “FI to encrypt when confidential data resides within the end point devices owned by personnel”
		Comments on operational infrastructure security: • 11.1.2 The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI’s service providers.

		Suggest adding ", where feasible" at end of paragraph 11.1.2 as there could be systemic and procedural restrictions on implementing firm tools in the endpoints or appliances provided/managed by service providers.
		Comments on operational infrastructure security: • 11.1.3 Databases, systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in databases, systems and endpoint devices should be encrypted and protected by strong access controls. • It is not always technically feasible to encrypt confidential information stored in databases due to the constraints on performance and search functions which such encryption cause. Encryption protects against the physical theft of information; however, most attacks on database contents are made by compromising user accounts of persons who have access to unencrypted database information. Physical theft concerns can be mitigated by encrypting the underlying media on which databases are stored. • We suggest the MAS also clarifies if backup media and storage platforms (for instance cloud databases) would fall within the scope of 11.1.3. • Confidential data stored in- Company managed infrastructure will be governed by authorized user access and hence encryption of such data should not be mandated. Requiring encryption of data should focus on non-Company managed infrastructure. •Suggestion to use the term 'safeguarded' instead of encryption. Please see suggested minor edits as: "11.1.3 As such, confidential data stored in databases, systems and endpoint devices, should be safeguarded and protected by strong access controls."

		Comments on operational infrastructure security: • 11.1.4 The FI should ensure only authorised mediums are used to communicate, transfer, or store confidential data. Strong access controls should be implemented to protect the information from unauthorised disclosure. It is unclear what 'medium' is. Suggested edits below: "The FI should ensure only authorized delivery channels and storage devices are used to communicate, transfer or store confidential data"
		Comments on operational infrastructure security: • 11.1.7 The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of... Confidential data should be purged not only prior to asset destruction but also prior to asset transfer/re-assignment. As such, we propose the following suggested edits to provide a more comprehensive approach in handling confidential data. Suggested edits below: "The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of or redeployed for other use."
		Comments on operational infrastructure security: • 11.2.2 To minimise the impact of the security exposure originating from third party or overseas systems, as well as from internal trusted network, the FI should deploy firewalls, or other similar measures, within internal networks to segregate information assets within the FI's internal networks. Information assets could be grouped into network segments based on the criticality of the business that they support, their functional role (e.g. database and applications) of the sensitivity of the information.

		Suggestion to replace “segregate information assets” with “protect information assets”
		Comments on operational infrastructure security: • 11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet. Clarification is needed on the expectation – only systems handling critical business and system functions or containing sensitive data should have Internet surfing separation implemented, or should it be implemented on all end-user computers and devices? The requirement to implement internet surfing separation is too prescriptive and should be left to the FI to assess and determine the most appropriate and holistic approach / solution (e.g. browser and email isolation, content threat removal, micro-VMs, AI/ML, etc) to safeguard online services from cyber threats. Suggested amendments below. “the FI should perform a risk assessment to ensure such systems are adequately ringfenced and segregated to mitigate likelihood of exploitation from Internet. “ Suggested amendments reasons: Guidelines should be less-prescriptive, instead of recommending to isolate system and data from internet “[…] the FI should perform a risk assessment and implement Internet surfing separation by isolating systems or have strong controls in place that effectively reduce the risk of cyber threats from the internet.”

		Comments on operational infrastructure security: • 11.3.2 The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner. Deviation from standard does not necessarily constitute a risk. It is a non-conformity. Suggested edits below. "The FI should establish a process to verify that standards are applied. Non-conformities arising from deviations should be addressed in a timely manner."
		Comments on operational infrastructure security: • 11.3.5 To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform real-time scanning of indicators of compromise (IOCs), and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities. We suggest that para 11.3.5 be reworded: "To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities." As the Guidelines should be less-prescriptive. Real time scanning may cause performance issues and we would like to suggest that an FI can adjust the scanning frequency based on the risk assessment (11.3.5)

		Comments on operational infrastructure security: • 11.3.6 Security measures, such as application white-listing, should be implemented to ensure only authorised software is allowed to be installed on the FI's systems. We suggest in para 11.3.6 the words ", such as application white-listing" should be deleted because application white-listing may not be a viable approach for all FIs due to the large and complex environment. Additionally, the decision to implement additional security measure (or not) should be derived from assessment. Suggested edits below. "The FI should consider additional security measures, to ensure only authorized software is allowed to be installed on the FI's systems."
		Comments on operational infrastructure security: • 11.5.1 Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which are connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, the networks which they are connected to and their physical locations. References to specific computing techniques such as hypervisor / virtualisation / IoT / BYOD can never be comprehensive. We respectfully propose MAS remove Section 11.5 as IoT is a technological trend. IoT can be treated similarly as untrusted devices, e.g. customer-owned devices, kiosks and BYOD, and there should be no need to prescribe additional controls against IoT devices. Alternatively, we suggest "maintain an inventory of all its IoT devices" be replaced with "maintain an inventory of FI owned IoT devices" for the Guidelines to provide clarity on the scope of IoT. Can the MAS also clarify whether or not BYOD devices

		considered IOT and are the FI's required to maintain an inventory of all BYOD's that end users may use? Access control can be accomplished by various methods. We propose that multifunction printers may not be IOT if they are only connected to the internal networks; however, they should have adequate security, patching, and updates. Some IoT related devices are not part of an FI's network but connected to the Internet (For instance, CCTV cameras owned by the building management, Mobile devices used for building management, WiFi routers provided by the building management for guests). We would seek clarification with regards to whether such IoT devices listed above which are not connected to FIs network but on the Internet, are out of scope and therefore not required to maintain an inventory as part of the FIs inventory management framework.
		Comments on operational infrastructure security: • 11.5.2 Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with function and criticality of the data that, collected, stored and processed by the IoT devices. We respectfully propose amending paragraph 11.5.2: "Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with the business process/function and

		criticality of the data that is transmitted, collected, stored and processed by the IoT devices." Comments on operational infrastructure security: • 11.5.3 The network that hosts IoT devices should be secured using strong authentication and network access controls to limit the cyber attack surface. For instance, restrict the inbound and outbound network traffic to and from IoT device. The FI may consider hosting IoT devices in a separate network segment from the network that hosts the FI's systems and confidential data. We suggest to make the paragraph less prescriptive and take into account that some devices can be less or more secure than others. Comments on operational infrastructure security: • 11.5.4 The FI should manage the administrator access to the IoT devices where feasible to minimise the risk of unauthorised access. We respectfully propose amending paragraph 11.5.4: "The FI should manage the administrator access to the IoT devices where feasible to minimise the risk of unauthorised access. Where access control is not provided by the IoT device, the FI may select an alternative control, such as restricting traffic as outlined in 11.5.3." Amendments reasons: The guidelines should acknowledge that not all devices may allow for administrator access configuration. Comments on operational infrastructure security: • 11.5.5 The FI should log and monitor the system activities of IoT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours.

		There are IOT devices that are purpose-built to be active outside normal working hours e.g. security cameras, and such 'behaviour' should not necessarily be deemed as anomalous. If Section 11.5 still remains - Suggested edits below. "The FI should log and monitor the system activities of IOT devices for suspicious or anomalous system activities or user behavioural patterns."
		Comments on operational infrastructure security: •Section 11 in general • Any device connected to an FI's network must adhere to acceptable Network Security Standards. IoT brings into scope a large variety and number of devices and FI's should be aware of that. The MAS should consider removing this section, as it is essentially covered throughout the other sections of this document. • Would an employee's own personal device that connects to corporate Wifi be considered an IoT device and subject to monitoring?
		Comments on IT project management and security-by-design: • 5.1.2 Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan. We suggest that MAS refrains from prescribing how FI's should run IT projects based on the prescriptive nature of 5.1.2 and 5.2.1. We suggest that this should be left to FI's to determine who is required for such projects within their organisation. FIs may define and use Agile framework that applies to both Project Lifecycle and Software Development Lifecycle (while ensuring that secure coding, source code review and

		application security standards are applied during Agile Software Development). By requiring the use of Waterfall project management and System Development Lifecycle (SDLC) framework for agile projects, this would negate the commercial gains FI seek with Agile, such as reduction of risk, increase quality and faster solution delivery time.
		Comments on IT project management and security-by-design: • 5.1.4 As project risks, such as an ill-defined project scope and poor cost management, can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle. For large and complex projects that impact the business, the FI should report significant project risks to its board of directors and senior management. For IT project management, we would assume it is applicable to those IT projects that will follow the SDLC methodology. Project management should not mandate Agile Development to adhere to the SDLC way. We would like to seek clarification on what is meant by "large and complex projects". Suggestion to use terminology which provide guidance for project-centric and product-centric delivery alike.
		Comments on IT project management and security-by-design: • 5.3.4 A source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. The feasibility of having a company providing its intellectual property to its customers is questionable.

		Applicability of escrow agreement guidelines across all critical software vendors requires further clarification as vendors like SAP, Oracle may not agree with such an agreement. The stability of the vendor, as well as the criticality of the software should also be considered in the decisions to require a software escrow agreement. For example, many FIs rely on critical software from Microsoft, however it will not be a good use of time and resources to require software escrow agreement in this case. Smaller scale IT service providers tend not to have escrow agreements due to cost and intellectual property considerations. MAS may like to consider providing more flexibility in choosing alternative mitigating measures in the absence of an escrow arrangement from such service providers (e.g. adequate contractual clauses with third party contracts). In addition, we suggest MAS clarifies the scope of the agreement as some of the front end digital technologies require open source code, hence implementing escrow would not be relevant. We also want to seek clarification required for type source code escrow agreement, especially for propriety software from vendor verses software that an FI purchases for use in-house.
		Comments on IT project management and security-by-design: • 5.4.2 The security-by-design principle requires the design and implementation of security in every phase of the SDLC in order to develop an IT system that is reliable and resilient to attacks. This includes incorporation of security specifications in the system design, continuous security evaluation and adherence to security practices throughout the SDLC. The principle should be adhered to such that security requirements are clearly specified in the early

		phase of system development. The security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling. • Security requirements may vary depending on the threat and risk to information assets and we suggest that MAS does not mandate these minimum-security requirements in all development projects. • Suggestion to reword that "The security requirements are commensurate with project scope and complexity…."
		Comments on IT project management and security-by-design: • 5.4.3 The SDLC should, where relevant, involve the IT security function in each phase of the life cycle. The wording "involve IT security function in each phase of the life cycle" seems too prescriptive. We suggest MAS to consider using "where relevant, the IT security function should be involved as part of the SDLC framework".
		Comments on IT project management and security-by-design: • 5.5.1 Functional requirements, key requirements such as system performance, resiliency and security controls, should also be established and documented. We respectfully propose amending paragraph 5.5.1: "Functional requirements, key requirements such as system performance, resiliency and security controls, should also be taken into account"

		Comments on IT project management and security-by-design: • 5.7.4 The FI should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing system to validate that the system continues to function properly after the changes have been implemented. We request more clarity on the scope of change that requires regression testing, and if it is the intention it will apply to all functional changes. Generally, executing regression test is a standard approach for major functional changes and is non-standard for small enhancements. (e.g. minor bug fixes which would be also considered as change) and we recommend this is reflected in 5.7.4.
		Comments on IT project management and security-by-design: • 5.8.2 Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI's policies, procedures and standards, and achieve the project objectives. • It would be helpful if MAS can provide clarification on the independent quality assurance function. Would this include members within the Quality Assurance function of the project phase? • Suggestion to use terminology which provide guidance for project-centric and product-centric delivery alike. Suggested edit as follows: "Quality assurance should be performed by an independent quality assurance function to ensure technology delivery activities and deliverables comply with the FI's policies, procedures and standards, and achieve the delivery objectives."

		•Can MAS please clarify the scope (i.e. all system build-outs or only critical / major systems?
		Comments on software application development and management: • 6.1.1 Software bugs or vulnerabilities are typically targeted and exploited by hackers to compromise an IT system, and they often occur because of poor software development practices. To minimise the bugs and vulnerabilities in its software, the FI should establish standards on secure coding, source code review and application security testing, and ensure the standards are applied and adopted throughout the SDLC. We propose that the standard should be risk based.
		Comments on software application development and management: • 6.1.6 The FI should ensure issues and software defects discovered from the source code review and application security testing, which affect the confidentiality, integrity and availability of information and the IT system, are tracked and remediated before production deployment. We would recommend for the remediation requirement to be based on materiality as some software defects may not affect the confidentiality, integrity and availability of information and the IT system. For issues and software defects discovered from the source code review which affect the confidentiality, integrity and availability of information: We recommend that remediation is performed on a risk based approach rather than expecting all software defects to be remediated before production, given that certain software defects come with mitigation controls which manage risks to an acceptable level.

		Comments on software application development and management: • 6.3.2 The FI should enforce segregation of duties for the development, testing and operations functions in its DevOps processes, and ensure the respective DevOps activities are logged and reviewed in a timely manner. MAS should consider allowing alternative controls that mitigate risks when segregation of duties control is not in place within DevOps teams as that may undermine the value the methodology brings. An example of this would be automating releases and aspects of testing. Strict segregation of duties between development, testing and operations would stop the efficient flow of information across the lifecycle of service that DevOps is meant to deliver.
		Comments on software application development and management: • 6.4 Application Programming Interface Development This section applies to direct application-to-application interfaces using request-reply internet-based standards. Clarification is required if the browser-applications (e.g. the use of HTML/JavaScript to request information and perform actions) and other styles of API (e.g. messaging (MQ,EMS), web streaming, file transfer) are included in the scope of this section.
		Comments on software application development and management: • 6.4.1 Application programming interfaces (APIs) (including foot note 12) enable various software applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIs that provide developers with programmatic access to a proprietary software application or web service. FIs collaborate with FinTech companies and develop open APIs, which are used by third parties to implement products

		and services for customers and the marketplace. Hence, it is important for the FI to establish adequate safeguards to manage the development and provision of APIs for secure delivery of such services. Paragraph 6.4.1 seems to suggest that FIs always collaborate with FinTech firms to develop open APIs. This is not always the case, as many FI's have in-house technology development centres working on developing APIs. Para 6.4.1 should be accordingly amended and adequate safeguards should be established to manage the development and provision of APIs, irrespective of whether the APIs are built by FI independently or in partnership with a FinTech firm.
		Comments on software application development and management: • 6.4.3 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. The vetting criteria should take into account the third party's nature of business, security policy, industry reputation and track record amongst others. • If the third party is a start-up, it is unlikely that FI can vet its industry reputation or track record. Suggested edit below. Suggest rephrasing to "A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third-party API access. FI should vet and assess third party's suitability based on applicable criteria under 'Section 3.4 Management of Third Party Services'. • Vetting criteria may be dynamic depending on the nature of API connectivity. We suggest revising such that the FI defines the vetting process based on the nature of the API functionality and its data security. • We request clarification on whether approved API access

		is only required for third party governance or more on general terms.
		Comments on software application development and management: • 6.4.7 A robust security screening and testing of the API should be performed between the FI and third party before it goes into production. The FI should have the ability to log the access sessions by the third party, such as the identity of the third party making the API connections, and the data being accessed. Further clarification is required whether this refers to the 'penetration testing' of external facing APIs, or to end-to-end testing of the APIs and back-end supporting applications. Where there are multiple third-parties (e.g. end clients) it is not feasible to test each third-party individually.
		Comments on software application development and management: • 6.4.8 Real-time monitoring and alerting capabilities should be instituted to provide visibility of the usage and performance of APIs and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach. We request further clarification on the requirement to perform real-time monitoring of APIs. E.g. What kind of suspicious activities need to be monitored? Is this required only for critical APIs or based on the classification of data that the API handles?

		Comments on software application development and management: • 6.5.1 The prevalence of common business application tools and software on the Internet has enabled end user computing, where business users develop or use simple application to automate their operations, such as perform data analysis and generate reports. Any application developed or acquired by end users should be approved by the relevant business and IT management, and managed as part of the FI's information assets. We request further clarification on what is the scope of impact and definition of application developed or acquired by end user that requires approval from business and IT management. We propose this be risk based for all end user management guidelines in this section.
		Comments on cyber surveillance and security operations: Suggest adding footnote on these terminologies 'situational awareness', cyber alerts' and 'cyber events' for additional clarity. Refer to FSB Cyber Lexicon (http://www.fsb.org/wp-content/uploads/P121118-1.pdf), released on November 2018, for these terminologies. We also added a suggested footnote below. 12.1.1 To maintain good cyber situational awareness1 …. Cyber-related information would include cyber alerts2, cyber events3, cyber threat intelligence and information on system vulnerabilities. Footnote 1. Situational Awareness is the ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. 2. Cyber Alert is notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems.

		3. Cyber Event refers to any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. Adapted from FSB Cyber Lexicon published on 12 November 2018.
		Comments on cyber surveillance and security operations: • 12.1.2 The FI could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties. Could MAS further clarify whether procuring cyber intelligence monitoring services is considered as "outsourcing" or "third party services"
		Comments on cyber surveillance and security operations: • 12.1.5 The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation. We respectfully propose amending paragraph 12.1.5: “The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services to facilitate evaluation and identification of online misinformation.” Suggested amendments reasons: Guidelines should not suggest mandating the use of specific technology in the regulations, instead focus on the control objectives that need to be achieved. Detect and respond to 'Misinformation' is a broad statement; a clearer understanding of the intention and scope of this guideline would be useful (12.1.5).

		Comments on cyber surveillance and security operations: • 12.2 Cyber Monitoring and Security Operations We suggest that the way anomalous user behaviour is detected shouldn't be tied to a particular methodology. Profiling individual users and their behaviour leads to legal/privacy/regulatory concerns. This relate to how the data can be used, how it is shared and protected, and what country specific regulatory requirements will need to be addressed when storing this type of information considering many FIs operate in many different countries.
		Comments on cyber surveillance and security operations: • 12.2.2 As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be tell-tale signs of intrusions. Suggested amendments below for clarity: As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block call-backs, which can be intrusions indicators of attempted intrusions.
		Comments on cyber surveillance and security operations: • 12.2.6 To facilitate identification of anomalies, the FI should establish a baseline profile of each system and user's routine activity. The profiles should be regularly reviewed and updated. Establish a baseline profile of each system and user's routine activity; applicability in its current form is too broad and clarity should be provided if this can be limited to critical systems / services (12.2.6). We also request further clarification if this is intended for external customers.

		Comments on cyber surveillance and security operations: • 12.2.7 User behavioural analytics is the use of machine learning algorithms in real time to analyse system logs, establish a baseline of normal user behaviour and identify suspicious or anomalous behaviour. The FI should consider applying user behavioural analytics to enhance the effectiveness of security monitoring. Further clarification if this is intended for external customers.
		Comments on cyber surveillance and security operations: • 12.3.3 The cyber incident response plan should be reviewed, updated and tested at least annually. Lesson learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan. The testing of the cyber incident response plan is covered in section 13.3 (Cyber Exercises) and hence can be removed from here. To follow a risk-based approach, we recommend this requirement to be periodic as determined by FI rather than annual and suggest the following amendment: "12.3.3 The FI's cyber incident response plan should be periodically reviewed and/or updated based on current cyber threat intelligence, information-sharing and lessons learned following a cyber event."
		Comments on BYOD security: Annex B.1(b) Mobile device do not cover the full scope of devices that staff use to gain on demand access to enterprise computing resources and data via virtualisation. Non-mobile devices such as personal computers are also used. Recommendation to MAS to consider using the term "devices" instead to reflect the coverage of staffs' devices used in this process.

		Comments on mobile application security: "Annex C.1(e) implement a secure in-app keypad security measures to mitigate against malware that captures keystrokes; and " This provision is quite prescriptive, suggest rewording to use security measures instead.
		Comments on online financial services: Please clarify if Section 13 (2013 TRM) - Payment Card Security (Automated Teller Machines, Credit and Debit Cards) is now under Online Financial Services. If yes, which subsection in Section 14 covers this? If it is not under Online Financial Services, then which section should it be under in the revised TRM?
		Comments on online financial services: • 14.1.1 Online financial services refer to banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. In delivering online financial services, the FI should implement security and control measures which commensurate with the risk involved to ensure data confidentiality and integrity, and the security, availability and resilience of the online services. Would applications created to enhance client's experience (e.g. Virtual Reality) be included as part of the scope? These are the applications not created for financial/payment services but its usage is for events whereby clients are required to download the mobile application for a better client experience. Are read-only applications included as part of the scope for paragraph 14.1.1?

		Comments on online financial services: • 14.1.5 Distribution of mobile applications or software to customers should only be performed through official mobile application stores or other secure delivery channels. FIs do not distribute mobile banking application to customers but rather customers choose to download FI's mobile banking application from official mobile application stores. Suggested edit below. FIs should only make available mobile applications or software to customers through official mobile application stores or other secure delivery channels.
		Comments on online financial services: • 14.1.6 The FI should actively monitor the internet, mobile application stores, social media websites, emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report the phishing attempts to the service providers and law enforcement agencies to facilitate removal of the malicious content. The FI should alert its customers of such campaigns. We suggest that the guideline should be less-prescriptive. Monitoring of SMS and e-mail of customers is not feasible as it takes place outside the FI's infrastructure. It may not be practical to alert customers of every instance of Phish sites identified as there are many discovered each day. We suggest that the paragraph be reworded as follows: "14.1.6 The FI should actively monitor the Internet, mobile application stores and social media websites for phishing campaigns targeting the FI and its customers. Timely action should be taken to report the impactful phishing campaigns to the service providers and law enforcement agencies as appropriate to facilitate removal of the malicious content."

		Comments on online financial services: • 14.1.7 Rooted or jailbroken mobile devices should be blocked from accessing the FI's mobile applications to perform financial transactions as such devices are more susceptible to malware and security vulnerabilities. This point should also be linked to Section 14.4 – Customer Education and Communication. It is important for customers to be aware about the risks of using devices which are more susceptible to malware and security vulnerabilities.
		Comments on online financial services: • 14.2.1 Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on any two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. OTP generator) and who you are (e.g. Biometrics). ASIFMA members suggest that a risk based approach be taken vis a vis multi-factor authentication. We suggest that multi-factor authentication should only be required before a high risk function is performed. For non-high risk functions (such as login), multi-factor authentication should be optional. This is in line with the HKMA Supervisory Policy Manual for the Supervision of E-banking item 4.1.2, which states that two-factor authentication is expected for "transactions with higher risk" such as unregistered third-party transfers or large-value transactions. Further clarification needed for the practice and requirement for OTP. Is classification required for first time login and mask? As of now all banks are showing the masked information on login without 2FA. Please clarify if this be added in the text.

		Comments on online financial services: • 14.2.2 E2E encryption at the application layer should be implemented for the transmission of customer passwords so that they are not exposed at any intermediate nodes between the customer mobile application or browser and the system where passwords are verified. Browser script-based password encryption is an implied requirement novel to Singapore. Where possible, requirements enabling equivalent protection of credentials should be achievable without FIs producing bespoke cryptographic methods, structures and code.
		Comments on online financial services: • 14.2.3 The FI should implement transaction-signing (e.g. digital signatures) for authorising high risk activities to protect the integrity of customer accounts' data and transaction details. High-risk activities include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details, high value funds transfer and revision of funds transfer limits. Suggestion to take account of PayNow which does not require any transaction signing. Also, it is better to clarify whether merchant/bill payment is out of scope.
		Comments on online financial services: • 14.2.6 Where biometric technologies and customer passwords are used for customer authentication, the FI should ensure the biometrics information and authentication credentials are encrypted in storage and during transmission. • 14.2.7 The performance of the biometrics solution, based on false acceptance rate and false rejection rate, should be calibrated to commensurate with the risk associated with the online activity. Clarification is required on both 14.2.6 and 14.2.7

		requirements applicability where FIs rely on biometric capabilities on the device used by customer. In such cases, it is proposed that FIs conduct due diligence on the solution offered by device manufacturers to evaluate if the biometric technologies are suitable to be used for customer authentication in online financial services. Suggestion that where feasible, FIs work with and share their technical / security standards with device manufacturers to improve the biometrics solution. However, the device manufacturer should remain responsible and accountable to its customers with regard to the performance of the biometrics solution and the security of the biometric information stored in the user's device.
		Comments on online financial services: • 14.2.12 Where alternate controls and processes (e.g. maker-checker function) are implemented for corporate or institutional customers to authorise transactions, the FI should perform a security risk assessment to ascertain these controls or processes commensurate with the risk of the activities that are being carried out. We would like to request for more clarity on this paragraph. Usually, alternate controls are determined after a risk assessment and controls testing. The paragraph indicates that a security risk assessment is required "after the fact". By this paragraph, are we expected to relook at our alternate controls to assess whether the controls are commensurate with the risk of the activities?
		Comments on online financial services: • 14.3.1 The FI should implement real-time fraud monitoring or surveillance systems to identify and block suspicious or fraudulent online transactions We request further clarification from MAS on what is meant with online transactions.

		Comments on online financial services: • 14.4 Customer Education and Communication Suggestion for FI to alert their customers to cyber threats and incidents, and the risks of using rooted or jailbroken mobile devices. The FI should educate their customers, other than professional and institutional customers, of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services.
		Comments on technology risk governance and oversight: 3.1.2 Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. While the organization should have members with the knowledge to understand and manage technology risks, the Board should have access to the knowledge and expertise needed to manage this risk. It is not clear from clause 3.1.2 if the requirement is for the Board to change the composition of its members to include someone with this specific skill set. We recommend that the focus should be on access to the right knowledge and expertise, instead of requiring changes to the composition of the Board. Indeed, depending on the size and type of the local business, it may be disproportionate to have a tech expert on the Board and it may be more appropriate for the Board to delegate to the relevant Senior Management including for example regional management for Tech.
		Comments on technology risk governance and oversight: • 3.1.5 The board of directors or a committee delegated by it, is responsible for: (c) appointing a Chief Information Officer, Chief Technology Officer, or Head of Information Technology with the requisite expertise and experience, to be responsible for Information technology and computer systems that support enterprise goals; (d) appointing a

		Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme • We would like to bring to the MAS attention that generally, the board of directors does not appoint these roles. Instead, this is usually the responsibility of the senior management of an organization. Also, individuals that are accountable for information security and information technology can have many titles. Thus, instead of listing a number of titles, we suggest MAS consider outlining the role attributes (e.g., expertise, experience, accountable, empowered) rather than the titles. • It should be up to FI's board of directors to designate/delegate relevant committees where necessary, instead of just one committee. Suggest rephrasing section 3.1.5. to "The board of directors or a relevant committee delegated by it, is responsible for…" • There is overlap with the MAS proposal for Individual Accountability and Conduct (IAC). In the draft IAC Framework, it is clearly indicated that these senior persons can be located outside Singapore and can dual/triple hat these roles and we request clarification on this matter.
		Comments on technology risk governance and oversight: • With respect to section 3.1.5(d), we would like to seek clarification on the required competence level, and if there are any expectations on the level of experience and industry certifications required within the technology and cyber security risk domains.
		Comments on technology risk governance and oversight: • 3.1.5 The board of directors or a committee delegated by it, is responsible for: (h) undertaking regular reviews of the technology risk management strategy for continued relevance In line with our suggestion for clause 3.1.2, we suggest it should be clarified that the focus is for the board to have

		access to necessary knowledge and expertise, instead of changing the board's composition.
		Comments on technology risk governance and oversight: • 3.2.1 The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards to manage technology risks and safeguard information assets in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape We would like to seek clarification from the MAS on what would be the recommended industry standards. For example, some of the industry standards that could be mentioned in the guidance are NIST Cybersecurity Framework for Cybersecurity framework or ISO 27017/18, SOC1/2/3 for Cloud. The recommended industry standards would be especially useful for emerging technologies such as API.
		Comments on technology risk governance and oversight: • 3.2.3 Compliance processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner The required 'monitoring and review' processes could be carried out by any independent team with the relevant subject matter expertise and not necessarily the Compliance team. We recommend that the MAS accordingly changes this requirement such as – "Monitoring and Review processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner. These monitoring and review processes could be carried out by any independent

		team with relevant subject matter expertise such as an internal control unit or compliance.”
		Comments on technology risk governance and oversight: • 3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes. We recommend that the requirement of registration by an FI of all information assets, establishment of its ownership and the roles and responsibilities of the staff managing the information assets should be limited to the information assets which are categorised as ‘material’ based on its security classification or business impact criticality. Otherwise, we are concerned that documentation and risk management requirements may lead to disproportionately high operational and compliance burdens for FIs. This is particularly so for global FIs. Our understanding is that this requirement also applies to any shared information assets that may be critical for the delivery of services. This should be clarified. MAS should clarify if this requirement also applies to any shared information assets not limited to those within the FI’s environment (e.g. on cloud infrastructure). We understand that MAS has expanded the definition of information assets as compared to 2013. It will be helpful to provide clarity on inventorying data as information assets. Would this include both hard copy and soft copy formats? (foot note for 3.2.1 , Information assets include data, hardware and software)

		Comments on technology risk governance and oversight: • 3.4 Management of Third Party Services It would be helpful if MAS can provide examples of the type of certification and accreditation which are recognised by MAS. For industry recognised certification and accreditation, these would include ISO 27001, SOC1, SOC2, NIST.
		Comments on technology risk governance and oversight: • 3.4.2 Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognised by the industry, before entering into a contractual agreement or partnership with the service provider. We encourage MAS to allow FIs to adopt separate but comparable due diligence processes applicable to FinTech firms given that the FinTech industry landscape is rapidly evolving. Traditional third party due diligence considerations such as track record may not fully apply to FinTech firms. For example, the due diligence performed for FI's partnership with Fintech start-up firms to develop a Proof-of-Concept innovation solution (without customer information) will differ from the FI's engagement of a third-party service provider for outsourcing arrangement.
		Comments on technology risk governance and oversight: • 3.5.2 Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who has access to the FI's data and systems, should be performed to minimise this risk. The requirement of a background check on personnel, who has access to an FI's data and systems could represent a significant task; especially for FIs who have a large global

		footprint or where the technology processes or systems are sub-outsourced. We would therefore recommend for the background check requirement to be limited to all personnel who has access to critical data or information assets in the production and data recovery environment. This combined with a strong Operational Infrastructure Security framework (section 11) should minimise the risk of theft of confidential, sabotage of systems or fraud by staff, contractors or service providers. We, therefore, recommend that para 3.5.2 be changed to – "Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who need access to the FI's sensitive and confidential data or information assets in the production and data recovery environment, should be performed where permitted by law to minimise this risk."
		Comments on technology risk governance and oversight: • 3.6 Security Awareness and Training • It may be unreasonable to require "all service providers" to have their staff participate in the FI's training program due to the fact that service providers generally have many customers. Part of the due diligence process for new vendors should involve determining that they have a suitable security awareness program for their staff. • Generally, a service provider has clients from the same industry – which would face the same set of risks. Hence it would alternatively be reasonable for the MAS to expect that the vendor staff should be trained on suitable security awareness program. Additionally, para 3.5.1 requires that service providers have the requisite level of competence and skills to manage technology risks. So, training would be useful to make sure they are aware of the technology risks. • Further clarification is needed on whether this can be global training programme with a Singapore supplement.

		General Comments: • ASIFMA welcome the opportunity to respond to the draft Guidelines on Technology Risk Management (TRM) and we are pleased to set out our comments in what follows. • To encourage the adoption of certain emerging technologies, a less-prescriptive approach will allow financial institutions (FIs) flexibility to determine and design appropriate technologies, guidelines, controls and frequency that best meet business needs and better align with the supervisory objectives at the discretion of the FIs. • Issuing specific local requirements pose challenges to FIs that operate in multiple jurisdiction and markets. Implementing different standards will also create technical challenges and economic impact for FIs to establish controls. To achieve effectiveness, multinational FIs create consistent frameworks and standards that span across different jurisdictions. This drives effective reduction in risk to FIs in accordance with global nature of the threat landscape, while still meeting regulatory requirements. We suggest that MAS cooperate with comparable foreign regulators to agree common standards for the regulation of technology risk so that FIs that operate across borders have the benefit of a seamless or at least aligned regulatory structures or that it is possible to rely on substantively equivalent foreign regulatory regimes (e.g. of home jurisdiction regulators).
		General Comments: • We suggest that MAS consider allowing FIs to substitute and leverage existing industry standard technology risk management frameworks to meet the MAS's supervisory requirements. Allowing FIs to demonstrate compliance with the use of existing industry framework increases efficiency by enabling FIs to focus on control improvement rather than competing framework implementation. • To ensure MAS's supervisory requirements are met in a considered and globally-harmonized manner, we

		recommend that MAS allow a two-year phase-in period so FIs of different sizes have sufficient time to comprehensively identify material gaps, and establish and implement additional controls where required. • Given the considerable number of footnotes in the consultation paper, we suggest at glossary for definition of terms to be utilised instead. • The definition of information assets has been updated with the inclusion of End User Application (EUA) and data. The applicability of all Technology Risk Management (TRM) guidelines across this broad definition requires further clarification. • There are some potential challenges in implementation for smaller local entities that are part of a significantly larger and complex global entity.
		Comments on IT service management: • 7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g., fixes for security vulnerabilities and software bugs are implemented within a timeframe that is commensurate with the criticality of the patches to the FI's systems. • Prioritization of patch deployment should take into consideration if FI's systems are mission-critical and accessible from Internet hence more susceptible to exploitation. Suggest section is rephrased as following. Suggest rephrasing to "7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with patch criticality and in accordance to security classification and asset placement of the FI's systems."

		Comments on IT service management: • 7.4.2 All patches should be tested before they are applied to the information assets in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system. The definition of 'Information asset' is too wide under Page 11 as it covers customer-owned and third-party systems of which an FI does not have access to their production environment. Suggest section is amended to: "All patches should be tested before they are applied to the FI's systems in the production environment."
		Comments on IT service management: • 7.5.4 A change advisory board, comprising of relevant key stakeholders including business and IT management should be formed to approve and prioritise the changes after considering the stability and security implications of the changes to the production environment. • Not all IT changes will have business impacts and business does not necessarily have the knowledge to assess every IT change. Generally, businesses are engaged as needed. • What is the expectation of business involvement in the change advisory board? Would this be for the purpose of providing approval and sign off? Or would the change advisory board serve as an avenue to promote awareness, and solicit feedback from the business?
		Comments on IT service management: • 7.5.7 Audit and security logs contain useful information which facilitates investigations and trouble-shooting. As such, the FI should ensure the logging facility is enabled to record activities that are performed during the change process. Suggested to add "where feasible" at the end of para 7.5.7

		when incorporating the control as there maybe parts of the change process that could not be logged.
		Comments on cyber security assessment: • 13.1 Vulnerability Assessment The 2013 TRM guidelines included that Vulnerability Assessment (VA) should have a combination of automated tools and manual techniques to perform a comprehensive VA. Is this a mandatory requirement in the latest 2019 guidelines?
		Comments on cyber security assessment: • 13.2.1 The FI should carry out penetration testing (PT) to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services. We suggest that PT may not necessarily provide in-depth evaluation of security posture, rather helps in identifying gaps in cybersecurity defences and suggest the following amendment: "13.2.1 The FI should carry out penetration testing (PT) to identify gaps in cybersecurity defences of its IT environment. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT."
		Comments on cyber security assessment: • 13.2.3 To obtain a more accurate assessment of the robustness of the FIs security measures, penetration testing should be conducted on the production environment. Proper safeguards should be implemented when penetration testing is conducted on the production environment. The guideline may lead to significant risk to an FI and we recommend this to include production-like environment as

		well. The production-like environment should have similar hardware/software/application configuration as that of Production. As a result, we suggest the edit below: "13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production or equivalent production-like environment. Proper safeguard should be implemented when PT is conducted on the production environment." We suggest to allow a mechanism to defer production penetration testing in favour of interim non-production penetration testing where risks have been identified. Known risks under remediation may result in PT of the underlying production asset posing an undue risk to operational stability leading to potential production impact.
		Comments on cyber security assessment: • 13.5.1 To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on real cyber incidents. Suggest adding a footnote for red team using 'Section 4 Definition' on 'Attacker (Sometimes referred to as 'Red Team')' in line with the 'ABS Guidelines for the Financial Industry in Singapore, Red Team: Adversarial Attack Simulation Exercises' which was referenced by MAS under Section 13.4. Footnote on Red team 1 Attacker (sometimes referred to as Red Team) is an individual or a team who is employed or contracted by an organisation to simulate the attack tactics of a real-world adversary based on intelligence about prevailing and/or probable cyber threats and incidents. Adapted from ABS Guidelines for the Financial Industry in Singapore, Red Team: Adversarial Attack Simulation Exercises, version 1, November 2018.

		Comments on access control: • 9.1.2 The FI should establish a user access management process to provision and revoke access rights to information assets. Access rights should be authorised and approved by the information asset owner. Organizations Line manager is accountable to ensure that staff is granted with user access relevant to his/her role and responsibilities. Suggesting edits below. "Access rights should be authorized and approved by information asset owner and or user's line manager or delegate."
		Comments on access control: • 9.1.4 The FI should establish a password policy and a process to enforce strong password controls (including footnote 18) for users' access to IT systems. This requirement and footnote risk quickly becoming outdated given that some organisations don't use passwords for authentication. MAS should consider amending requirement to ""The FI should establish a standard for authentication that mitigates brute force attacks to IT systems".
		Comments on access control: • 9.1.5 Multi-factor authentication19 should be implemented for users with access to critical system functions20 to safeguard the systems and information from unauthorised access In addition to implement multi-factor authentication on specific users, we encourage MAS to consider allowing FIs to alternatively implement multi-factor authentication based on factors such as user's purpose of use, system criticality and user's login location.

		Comments on access control: • 9.1.6 The FI should ensure information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as incorrectly provisioned access rights. Exceptions noted from the user access review should be resolved as soon as practicable. Information asset owners are not in a position to determine appropriateness of user access e.g. internal transfer, redeployment by line manager to perform different functions, etc. Suggested edits below. "The FI should ensure line managers perform periodic user access review to verify the appropriateness of privileges that are granted to their staff and contractors users"
		Comments on access control: • 9.2.1 Users granted with privilege system access have the ability to inflict severe damage on the stability and security of the FIs IT environment. Access to privileged accounts should only be granted on a need-to-know basis; activities of these accounts should be logged and reviewed as part of the FIs ongoing monitoring. Organizations have implemented multiple controls from onboarding background checks, strong access and authentication controls, to the logging of user activities. These layered controls are in place to limit the organizations' exposure to employees and contractors conducting activities which requires privileged access. While it is agreed that accounts should be granted on a need-to-use basis, the additional activity of monitoring activities then conducted by the use of these accounts may not provide the additional security benefits when compared to the cost of implementation. The activity of reviewing log entries and tying these activities back to a change description may, in many cases, be inconclusive as log entries to application activities may not provide

		sufficient information to determine all activities conducted by a user.
		Comments on access control: • 9.3.1 Remote access allows users to connect to the FIS's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connection should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment. Clarification on whether BYOD email such as Blackberry be classified as remote access assets since they do not have access to internal networks
		Comments on access control: 9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. • Virtual Devices (e.g., VDI) that are accessed through secure channels including from BYOD should be allowed. • FI cannot harden employee-owned personal mobile devices used for remote access, hence BYOD security policy applies. As such, we propose to draw reference to the Annex B in the draft consultation paper. Suggested edits below. • "The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. For personal-owned mobile devices, please refer to Annex B: BYOD Security." • This control is impractical as FIs cannot enforce its security expectations on the non FI-owned equipment

		personnel may use to access the FI's information assets. This completely defeats the purpose and benefits of a BYOD strategy. Instead, FIs should be allowed to rely on its own security measures regarding how those assets are accessed, if the device may not have the strongest security measures in place. Given the extensive guidance provided in the revised TRM (e.g. multi-factor authentication, data leakage controls, disallow mobile applications on jail-broken devices, etc.) we believe adequate measures are already in place to mitigate this risk.
		Comments on technology risk management framework: • 4.1.1 The FI should establish a risk management framework to manage technology risks in a consistent and systematic manner. As part of the framework, effective risk management practices and internal controls should be instituted to achieve data confidentiality (including footnote 5) and integrity, system security and reliability, as well as resilience in its IT operating environment. • Suggest that this paragraph include proportionality and we ask the MAS to consider this drafting language: "The FI should establish a risk management framework consistent with the level of risk and complexity inherent to its business to manage technology risks…" • The technology risks terminology varies across chapters. For example - In section 7.1, there is reference to "stability of the production IT environment" but it is not referred to under chapter 4 (para 4.1.1). Service availability represents a key tech risk and we believe that both Information security and system availability should be specifically referenced in the context of technology risk management. We acknowledge that this could potentially be inferred from "Data confidentiality and integrity, system security and reliability, as well as resilience in its IT operating environment." However, we believe that for the sake of consistency and clarity, stability of the production IT environment should also be captured in chapter 4.

		Comments on technology risk management framework: • 4.1.3 (d) - Risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, systems, environmental or operating conditions; and report key risks to the board of directors and senior management We suggest to add a qualifier where risk that customers exposed within the "scope of service provided" by FIs.
		Comments on technology risk management framework: • 4.2.1 The FI should identify the threats and vulnerabilities, as well as the risks posed to its IT environment, including information assets that are maintained or supported by third party service providers. The risks posed to information assets that are maintained or supported by third party service providers should be assessed in an appropriate way.
		Comments on technology risk management framework: • 4.4.1 For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of the information assets and the level of risk tolerance. We suggest that paragraph 4.4.1 be amended to include the criticality of service as follows: a. For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of information assets, level of risk tolerance and the criticality of service.

		Comments on technology risk management framework: • 4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, the FI should give priority to threats and vulnerabilities with a higher risk rating, such that those which could cause significant harm or impact to the FI's information assets and operations Suggestion to reword for clearer understanding: "The FI should identify the threats and vulnerabilities, as well as the risks posed to its IT environment".
		Comments on technology risk management framework: • 4.4.5 The FI should refrain from implementing a system or acquiring an IT service where threats to the safety and soundness of the FI cannot be adequately controlled and the risks out-weigh the benefits. The decision to refrain from implementing or acquiring a system is not only limited to threats to the safety and soundness of an FI. This should be a conscious decision derived through a risk assessment to determine if residual risks can be effectively mitigated to an acceptable level. Suggested edits below. "The FI should refrain from implementing a system or acquiring an IT service outside the FI's risk appetite or tolerance limit".
		Comments on technology risk management framework: • 4.4.6 To mitigate risks, the FI could consider taking insurance cover for various insurable technology risks, including recovery and restitution costs. As insurance cover does not mitigate the risk, but only transfers the financial impact of the risk event to the insurers, we suggest para 4.4.6 be mentioned as a risk transference approach and not as a risk mitigation.

9.	Aviva Ltd	Comments on technology risk governance and oversight: Regarding the consultation paper issued by the MAS on TRM Guidelines in Mar 2019, we like to seek clarification on Para 3.1.2 where both the board of directors and senior management should have members with the knowledge to understand and manage technology risk. In assessing whether Aviva's Board meet this new requirement, we need MAS' guidance as to what the criteria (i.e. IT related working experience or qualifications) that we can use to assess and ensure our board member(s) have the necessary skills and understanding of technology risks.
10.	Deloitte & Touche Enterprise Risk Services Pte Ltd	Comments on IT resilience: Sub-section (8.1.1) Implementation of system redundancy or fault-tolerant solutions We note that MAS expects "… The FI should implement system redundancy or fault-tolerant solutions to achieve the high system availability." We wish to suggest MAS provide further guidance on whether this clause is applicable only to critical systems or to all systems as it may seem to contradict Clause 5 of the Notice on Technology Risk Management which requires an FI to "make all reasonable effort to maintain high availability" only for critical systems.
		Comments on IT resilience: Sub-section (8.3.4) Definition of "extended period" We note that MAS expects FIs to operate from the recovery site for an "extended period" as part of disaster recovery testing to gain the assurance and confidence that the recovery site is able to support business needs. We wish to seek clarification what constitutes an "extended period" of time.
		Comments on IT resilience:

		Sub-section (8.2) Definition of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) We note that the definition of RTO as described in the footnote 16 indicates that "RTO is the duration of time, from the point of disruption, within which the system should be restored." In the Proposed Revisions to Guidelines on Business Continuity Management issued in March 2019, the definition of RTO is indicated as "RTO comprises: (1) The duration of time from the point of business disruption, to the point of declaring the activation of BCP(s) for business functions or units and interdependencies, and (2) The duration of time from the BCP activation to the point where the specific business function or unit is recovered to its Minimum Performance level." We wish to suggest to MAS for the definitions of RTO in the Technology Risk Management Guidelines to be in line with the Guidelines on Business Continuity Management.
		Comments on operational infrastructure security: Sub-section (11.5.1) Inventory of all its IoT devices We wish to suggest that MAS provide further guidance on how FI should "maintain an inventory of all its IoT devices, the networks which they are connected to and their physical locations" given the prevalence of smart phones and mobile devices connecting to FIs' network or internet via WIFI. Furthermore, with regard to sub-section (11.5.5), we note that MAS expects FI to log and monitor the system activities of IoT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours. We wish to seek clarification if this extends to users' smart phones and mobile devices regardless of risk.

		Comments on operational infrastructure security: Sub-section (11.5.1) Inventory of all its IoT devices We wish to suggest that MAS provide further guidance on how FI should "maintain an inventory of all its IoT devices, the networks which they are connected to and their physical locations" given the prevalence of smart phones and mobile devices connecting to FIs' network or internet via WIFI. Furthermore, with regard to sub-section (11.5.5), we note that MAS expects FI to log and monitor the system activities of IoT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours. We wish to seek clarification if this extends to users' smart phones and mobile devices regardless of risk.
		Comments on operational infrastructure security: Sub-section (12.2.1) Monitoring or surveillance systems With regard to sub-section (12.2.1), we noted that MAS expects that "FI should implement monitoring or surveillance systems to ensure it is alerted to any suspicious or malicious system activities" We wish to suggest that MAS may wish to consider allowing FIs to adopt a risk-based approach based on the criticality of business functions, specific only to systems that have access to sensitive information including customer information.
		Comments on operational infrastructure security: Similarly, with regard to sub-section (12.2.6), we noted that MAS expects that the "FI should establish a baseline profile of each system and user's routine activity" and that "the profiles should be regularly reviewed and updated". We wish to suggest that MAS may wish to consider allowing

		FIs to adopt a risk-based approach based on the criticality of business functions, specific only to systems that have access to sensitive information including customer information.
		Comments on cyber surveillance and security operations: Sub-section (12.2.1) Monitoring or surveillance systems With regard to sub-section (12.2.1), we noted that MAS expects that "FI should implement monitoring or surveillance systems to ensure it is alerted to any suspicious or malicious system activities" We wish to suggest that MAS may wish to consider allowing FIs to adopt a risk-based approach based on the criticality of business functions, specific only to systems that have access to sensitive information including customer information.
		Comments on technology risk governance and oversight: Sub-section (3.1.5) (c) and (d) Appointment of key positions We note that the board of directors or a committee delegated by it, is responsible for: • Sub-section (3.1.5) (c) "Appointing a Chief Information Officer, Chief Technology Officer or Head of Information Technology with the requisite expertise and experience" • Sub-section (3.1.5) (d) "Appointing a Chief Information Security Officer or Head of Information Security" We wish to seek MAS clarification if all FIs (regardless of size or operations) are expected to appoint a "Chief Information Officer" and a separate "Chief Information Security Officer or Head of Information Security". Specifically for FIs where there is only a local branch, we wish to seek clarification if the above appointment can be headed by a regional representation of a Group or a within a related entity.

		Comments on IT service management: Sub-section (7.4.1) Patch Management We note that MAS requires "a patch management process should be established to ensure functional and non-functional patches are implemented within a timeframe". We wish to suggest the patches should be reviewed before decision is made as very often, patches released by the vendors couldn't be implemented due to potential new conflict and impact it may introduce to the system.
		Comments on IT service management: Sub-section (7.7) MAS Notice on Incident Reporting We note that MAS had separately published Instructions on Incident Notification and Reporting to MAS, as additional guidance to the Notices on Technology Risk Management. MAS may wish to consider incorporating these instructions in the proposed Technology Risk Management Guidelines for consistency and ease of reference.
		Comments on technology risk management framework: Sub-section (4.1.1) Technology Risk Management Framework We note that MAS requires FIs to establish a Risk Management Framework to manage technology risk in a consistent and systematic manner. a) We wish to suggest that the technology risk management framework should also take into consideration the FI's business portfolio and functions; effective risk management practices and internal controls should commensurate with the criticality of the business functions they support. b) Further in sub-section (4.1.3) (b), risk assessments should

		also take into account the weakest link in the end-to-end process of a business line.
		Comments on technology risk management framework: Sub-section (4.2) Risk Identification to include legacy systems, single point of failure and data leakage a) We note that MAS expect FIs to "identify the threats and vulnerabilities, as well as the risks posed to its IT environment, including information assets that are maintained or supported by third party service providers". We wish to suggest that MAS include specific reference to the management of "legacy systems", including whether they continue to be maintained and/or supported. We further suggest that Risk identification include a process to identify IT assets that constitute a single point of failure or a multiple concentration risks should be separately treated as vulnerability. The same concern would apply to section 7.3.2.
11.	Depository Trust and Clearing Corporation	Comments on IT project management and security-by-design: 5.3.4 A source code escrow agreement should be in place, based on the criticality of the acquired software to the FIs business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. There is a question to the feasibility of having a company provide its intellectual property to its customers. I would need greater feedback from the Legal and Procurement to see if this is something that we are able to complete.
		Comments on technology risk governance and oversight: 3.1.2 Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. While the organization should have members with the knowledge to understand and manage technology risks, the Board should have access to the knowledge and expertise

		needed to manage this risk. It is not clear from this statement if the requirement is for Boards to change the composition of its members to include someone with this specific skill set. There should be clarity of the intent and a push to only require access and no changes to Board composition.
		Comments on technology risk governance and oversight: 3.1.5 The board of directors or a committee delegated by it, is responsible for: (C) Appointing a Chief Information Officer, Chief Technology Officer, or Head Of Information Technology with the requisite expertise and experience, to be responsible for Information technology and computer systems that support enterprise goals; (D) appointing a Chief Information Security Officer or Head Of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme Generally, the board of directors does not appoint these roles. This is the responsibility of the Senior Management of an organization to make this assignment. Secondly, there can be many titles afforded to the individuals that are accountable for Information Security and Information Technology so, instead of trying to list them all, it may be better to outlines the role attributes (e.g., expertise, experience, accountable, empowered) rather than include the titles.
		Comments on technology risk governance and oversight: 3.1.5 The board of directors or a committee delegated by it, is responsible for: (H) undertaking regular reviews of the technology risk management strategy for continued relevance The Supervisor may have required cyber expertise on the Board in part to have a credible review of this specific task with the MAS-defined Board responsibilities. The aforementioned proposal should be provided to MAS.

		Comments on technology risk governance and oversight: With regard to Para 3.4 on the Management of Third Party Services, with specific reference to the FMI entities that are a trade repository ("TR"), given that a TR is subjected to all relevant regulations, MAS notices and license conditions, including but not limited to the MAS' technology risk management requirements, we respectfully submit that the proposed requirements under Para 3.4.2 should not be made applicable to the TR. At most, the grant of a TR license by MAS should be summarily recognized by the industry and be sufficient in and of itself.
		General Comments: DTCC welcomes the opportunity to respond to the recent consultation document prepared by the Monetary Authority of Singapore ("MAS"), Proposed Revisions to the Technology Risk Management Guidelines Consultation. DTCC continues to strongly support efforts to create a safe and resilient financial industry through the consistent adoption of appropriate technology risk management measures. We believe these are indispensable to protect the financial services and the economies that depend on them. However, care should be taken to ensure that regulatory frameworks achieve their goals in a manner that is appropriate for each participant and the industry without introducing unnecessary complexity into an already complex regulatory regime. Accordingly, DTCC provides the following considerations leveraging our experience not only as an operator of trade repositories globally, but also as the offeror of a wider range of services to the financial industry globally. DTCC welcomes the opportunity to further discuss these comments and to provide additional views related to technology risk management.
		Comments on cyber security assessment: 13.2.3 To obtain a more accurate assessment of the robustness of the FIs security measures, penetration testing should be conducted on the production environment.

		Proper safeguards should be implemented when penetration testing is conducted on the production environment. Penetration testing carries an operational risk of creating outages or unpredictable outcomes in system performance. In a critical environment, conducting these tests could cause a marked increase in operational risk to systems that provide critical business functions and could lead to potential outages of this infrastructure. Organizations should evaluate the risks of conducting penetration tests in the production environment and, if determined to be outside of their risk appetite, should conduct these tests in an environment that mimics the operation of the production environment (e.g., UAT, QA).
		Comments on access control: 9.2.1 Users granted with privilege system access have the ability to inflict severe damage on the stability and security of the FIs IT environment. Access to provided accounts should only be granted on a need-to-know basis; activities of these accounts should logged and reviewed as part of the FIs ongoing monitoring Organizations have implemented multiple controls from onboarding background checks to strong access and authentication controls to the logging of activities conducted by users. These layered controls are in place to limit the exposure of the organization to employees and contractors conducting activities which requires privileged access. While it is agreed that accounts should be granted on a need-to-use basis, the additional activity of monitoring activities then conducted by the use of these accounts may not provide the additional security benefits when compared to the cost of implementation. The activity of reviewing log entries and tying these activities back to a change description may, in many cases, be inconclusive as log entries to application activities may not provide sufficient information to determine all activities conducted by a user

12.	Holland & Marie Pte. Ltd.	Comments on IT service management: We believe the proposed problem management framework should be qualified for materiality.
13.	HSK Resources Pte Ltd	Comments on cryptography: No comments
		Comments on IT resilience: No comments
		Comments on operational infrastructure security: No comments due to small operations in nature.
		Comments on IT project management and security-by-design: No comments
		Comments on software application development and management: No comments
		Comments on cyber surveillance and security operations: No comments due to small operations in nature.
		Comments on IT audit: no comments
		Comments on application security testing: no comments
		Comments on BYOD security: no comments

		Comments on mobile application security: no comments
		Comments on online financial services: no comments.
		Comments on technology risk governance and oversight: No Comments
		General Comments: No comments
		Comments on IT service management: No comments
		Comments on cyber security assessment: No comments due to small operations in nature.
		Comments on access control: No comments
		Comments on technology risk management framework: No comments
14.	IG Asia Pte Ltd	Comments on application security testing: A.2 Common testing methods for security vulnerabilities in software applications include: a) Static Application Security Testing - In general, Static Application Security Testing (SAST) Tools are not very cost-effective for the limited benefits they provide. We feel that the use of SAST are limited and therefore are shifting focus to earlier in the SDLC by

		implementing improved secure development training, threat modelling and periodic secure code reviews.
		Comments on mobile application security: Annex C: Mobile Application Security d) implement certificate or public key pinning to protect against MITMA; - We would like to share that certificate pinning is not always possible in a micro-service architecture which involves multiple services.
		Comments on technology risk governance and oversight: 3.1.5 The board of directors or a committee delegated by it, is responsible for: a) ensuring a sound and robust risk management framework is established and maintained to manage technology risks in a manner that is commensurate with the FI's risks; - Please can MAS help provide clarification for FIs that receive intra group technology services wherein the Group board ensures appropriate governance and oversight of Technology risk and has board and management committees dedicated to risk and technology risk. Can these committees act as the delegated authority for the local entity board? Would it be acceptable for decisions to be made at Group level with regular monitoring and exception reporting at the local entity level?
		Comments on technology risk governance and oversight: 3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes. It would not seem beneficial or realistic to maintain an inventory of all information assets. For assets that are deemed non critical (medium or low), it would not seem beneficial or realistic to maintain a register of this

		information due to the sheer amount and volume of information held within a company. This activity would surely dilute focus and efforts that should be spent on managing critical/high value data.
		Comments on technology risk governance and oversight: 3.4.2 Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognized by the industry, before entering into a contractual agreement or partnership with the service provider. - We would appreciate if more clarity, definition, and guidance could be provided the reference to "Proper due diligence". Is this required for all vendors, or can a FI decide to perform and complete due diligence for vendors deemed high risk only?
		General Comments: IGA is providing further feedback via this electronic submission. This is in addition to the consolidated responses submitted via the Securities Association of Singapore of which IGA is one of the respondents. As a general comment, we think it will be very helpful if a mapping document/audit trail can be provided to help FIs to map the old and new references, and identify if the guideline is new or amended. This will assist FIs in performance of a gap analysis against the proposed new requirements.
15.	Investment Management Association of Singapore (IMAS)	Comments on cyber security assessment: For small to mid-sized enterprises, implementation of "machine learning", "user behavioural analytics", "red team exercise" would be very resource-intensive and may face talent gap to assist in the design, testing and implementation.

		Comments on access control: Implementation of multi-factor authentication may not be feasible for all systems and may pose resource challenge for existing off-the-shelf systems which may not be MFA-ready to be re-suited to be MFA-compliant. Further, we would like to know the Authority's view about personal device hardening in cases where FIs have put in place the necessary protection such as encryption, strong multi-factor authentication and containment of connection as implied in paragraph 9.3.1 of the Consultation Paper, such that data leakage will be prevented, would there still be an expectation to enforce hardening of devices belonging to individual employee?
16.	KPMG Services Pte Ltd	Comments on cryptography: We have no comments on this section.
		Comments on IT resilience: 8.1 Availability (8.1.2) We suggest for MAS to consider extending the requirement for Single Pont of Failure ("SPOF") analysis to be done for external vendors providing critical services to FIs as well. (8.1.3) MAS should consider whether all FIs should have to abide by the same pre-defined thresholds. MAS may consider extending thresholds to customer serving systems along with real-time transaction systems. (8.1.4) As the application of the concept of "high-availability" may differ from each FI, we suggest for MAS to specify the definition of high availability systems (e.g. active-active setup). Based on our experience, we noted some FIs where an active-passive setup is also considered as a "highly-available" infrastructure, depending on the system. We would recommend for MAS to provide a more useful definition of "high-availability" as this also impacts the FIs ability to comply with the related TRM Notices - for critical systems.

		8.3 Testing of disaster recovery plan (8.3.4) MAS has requires that the FI should operate from recovery site for an extended period as part of disaster recovery testing. We recommend MAS to provide further clarity on the definition of “extended period”. (8.3.5) MAS has used the word “critical system” with regard to conducting disaster recovery tests with service providers. We suggest for MAS to provide greater clarity on the definition of critical systems, and whether the same definition in the MAS TRM Notices can be referred in this context. 8.5 Data Centre Resilience (General Comment) We noted MAS has used the word "data centre" ("DC"), which may be misunderstood by other FIs that this only pertains to purpose built data centres. As we noted that other FIs may host their systems in the same premise as their offices, we understand that the same level of protection should be applied as a "data centre" would . In this regard, we recommend MAS to provide clarity on the extent of the applicability of these controls, and strongly recommend the enforcement of these controls regardless of the location of hosting. (8.5.5) – MAS has required that the DC’s physical security and environment controls should be monitored on a 24x7 basis. We request for MAS to provide guidance on how this can be achieved (e.g. use of automated tools for monitoring such as CCTVs, building management systems). In addition, as some FIs may host there systems in a premise which is not a “purpose-built” data centre, this poses a challenge for FIs to comply and may require them to move their systems to a proper data centre. MAS should provide guidance on how this requirement can be complied with respect to other simpler hosting setup.
		Comments on operational infrastructure security: 11.1 – Data Security

		General Comment: Beyond the current measures adopted by most FIs for data loss protection, we would suggest MAS to provide guidelines for FIs to further adopt measures to maintain control of confidential information that are already held by non-FI parties (or external parties). We would also suggest MAS to provide additional guidelines in exchanging confidential information between FIs and its external parties, such as through encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length.
		Comments on operational infrastructure security: 11.2 – Network Security (11.2.8) We recommend MAS to provide further clarity by stating denial of service 'protection' solution rather than denial of service solution.
		Comments on operational infrastructure security: 11.3 – System Security (11.3.3) Based on our experience with the industry, we foresee that smaller FIs will experience challenges implementing behavior-based endpoint protection solutions. As such, we recommend the consideration of providing other practices, controls or solutions to achieve similar endpoint protection capabilities.
		Comments on IT project management and security-by-design: 5.1 Project Management Framework (5.1.2) The requirement of having project plans for all IT projects may not be feasible for some FIs. Additionally, having a steering committee for every project, regardless of size would be very challenging to meet specially for FIs with slim organisational structure. In this regard, we recommend MAS to consider the application of these requirements based on a "tiering" system, which classifies projects based

		on risk, as part of the security by design framework such that the aforementioned requirements should only be mandatory for more complex or higher risk projects. Separately, we noted that there is no defined requirement on establishing hard and soft gates for project management and SDLC. We would suggest MAS to adopt this concept to fortify decision making within and ensure involvement of key stakeholders on critical junctures within the SDLC.
		Comments on software application development and management: We have no comments on this section.
		Comments on cyber surveillance and security operations: 12.1 – Cyber Threat Intelligence and Information Sharing (12.1.1) While MAS has recommended the establishment of a process to collect, process and analyse cyber-related information, we further suggest MAS to make it clear that the information should also include those coming from external and internal cyber threats. In addition, MAS should require the industry and promote open sharing of this information through briefings and targeted forums on specific FIs. (12.1.2) While MAS has recommended the consideration of procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties, we would like to highlight that smaller FIs might not be able to obtain such service as this might not be cost effective for them. Alongside with our comment form 12.1.1, the success for smaller FIs may be dependent on other venues such as those industry-sharing exercises, or potentially those coming from circulars which MAS may issue from time to time.

		Comments on IT audit: We have no comments on this section.
		Comments on application security testing: We have no comments on this section.
		Comments on BYOD security: We have no comments on this section.
		Comments on mobile application security: We have no comments on this section.
		Comments on online financial services: We have no comments on this section.
		Comments on technology risk governance and oversight: 3.1 Role of the board of directors and Senior Management (3.1.5) In relation to the responsibilities of the board in managing technology risk, we noted that MAS has mandated the appointment of certain key positions within the FI's organisation, such as the CIO, CTO, or Head of IT, and a CISO or Head of Information Security. While these roles are mostly appointed and existing for larger FIs, this requirement will pose a significant challenge for FIs with slim organisational structure or those operating as a branch in Singapore. We recommend MAS to confirm whether it is essential for these roles to be designated and must be in the Singapore office, or whether support from overseas head office on this roles will be sufficient to meet the requirement.
		General Comments: With the release of the proposed revisions to TRM Guidelines, we noted that MAS has placed greater emphasis on technology risk domains which the FS sector needs to bolster its capabilities in preventing and

		responding to cyber-attacks. With this, we foresee greater investment in people, process and technology not only to meet the expected guideline requirements, but also to support MAS in its objectives in making Singapore a safe place to conduct business for the sector. On the other hand, we also foresee that the FS sector will definitely have challenges in meeting the new enhanced requirements, let alone the requirements in the MAS TRM released in 2013. Through our experience working with the FS sector, we have noted challenges predominantly on the lack of robust processes or capabilities on the following domains: 1. Privileged Access Management 2. Network Security (e.g. Establishing network perimeter defenses, baseline hardening and enforcement) 3. Security Incident Management (Manual means of identifying security events, or no capability at all). 4. Managing risk on outsourcing (Due diligence is not comprehensive, audits cannot be enforced on third-party service providers). Similar to how other regulations were rolled out (e.g. MAS Guidelines on Outsourcing), we recommend MAS to specify a period for the FS to adjust and cope up with the requirements through self-assessments within a defined timeframe. This will allow the sector to identify its preparedness in meeting the requirements and identify more pragmatic approach in meeting the requirements. We also noticed that the amount of data, complexity of technologies which the FS sector manages, and the higher likelihood of people to fail due to error and fatigue has become a challenge for the sector to manage technology risk effectively. To aid in the said challenge, we also recommend MAS to consider embedding automation through the use of certain tools to manage and facilitate control processes, coupled with sufficient due diligence to assess the tool's capability prior to using them.
		Comments on IT service management: 7.1 Configuration Management

		(7.1.1) We suggest MAS to define the systems (e.g. application, operating systems, middleware, databases, network devices, etc.) for which the FIs need to manage security configurations. Based on our experience with the industry, especially those FIs which have large number of assets that are subjected to configuration reviews, it will be difficult to review all the assets manually. In this regard, we recommend MAS to provide additional guidance on using automated tools when conducting regular enforcement checks. This will also help the FIs to monitor the baseline standards are consistently applied.
		Comments on IT service management: 7.3 Technology Refresh Management (7.3.2) Based on our experience with the industry, although there are exception forms, these exceptions (or dispensation) are not reassessed considering the changes on the IT control environment and the risk appetite of the FIs. We suggest MAS to mandate that the approved exceptions should have a validity period for the FIs to regularly assess these exceptions from policy requirements.
		Comments on IT service management: 7.4 Patch Management (7.4.1) We recommend MAS to provide additional guidance on how the FIs will manage and monitor the patches applied to the FI's systems, such as the use of automated tools. In addition, similar to how it was presented in the 2013 version of the MAS TRM Guidelines, we suggest MAS to expand on the process related to managing patches from identification, categorisation, prioritisation, deployment and dispensation process. This is in recognition that patching is a key control in securing systems from cyber attacks – hence we recommend MAS to specify the necessary baseline for key domains such as patch management. In addition, we recommend MAS to provide requirements on ensuring the completeness of patches applied into

		systems through linking patch management and IT asset management.
		Comments on IT service management: 7.5 Change Management (7.5.2) We suggest MAS to consider the assessment on existing infrastructure, network, upstream and downstream systems in performing the risk and impact analysis of the change request.
		Comments on IT service management: 7.5 Change Management (7.5.4) Based on our experience with the industry, FIs with slim organisational structure may face difficulties in forming a change advisory board. To provide alternatives, we recommend MAS to give emphasis the involvement of the business and IT management in approving and prioritising the changes to the production environment.
		Comments on IT service management: 7.7 Incident Management (7.7.2) We suggest MAS to provide alternatives (e.g. completed controls self-assessment addressing the minimum requirements) when FIs are unable to engage an external assistance to ensure sufficient resources are available to facilitate and support incident response and recovery.
		Comments on IT service management: (7.7.5) We recommend MAS to include the criteria used for assessing the severity levels of incidents in the incident management framework. Other comments: Based on our experience with the industry, FIs are starting to adopt automated tools to on-board their security devices and configure logs to be analysed to identify security events. In addition, it becomes impractical for FIs to rely on manual processes such as manually reviewing logs, as this

		will not be effective and as efficient compared to automated real-time analysis of logs. We suggest MAS to include one of its requirements to consider implementing these automated tools for the FIs to perform real-time monitoring of security events. We recommend MAS to explicitly include the requirements to inform MAS as soon as possible in the event a relevant incident occurs and to have documented procedures to notify MAS of these incidents.
		Comments on IT service management: 7.8 Problem Management (7.8.1) We recommend MAS to provide more guidance on the establishment of problem management rather than putting a generic requirement. It will be helpful for FIs to address the minimum content/coverage of the framework such as roles and responsibilities, key metrics to be identified and analysed, tools and techniques to be used.
		Comments on cyber security assessment: We have no comments on this section.
		Comments on access control: 9.1 User Access Management (9.1.2) MAS has required for FIs to establish user access management process, which includes provisioning and deprovisioning of user accounts and rights. To enhance requirements on user access management, we suggest for MAS to consider the following provisions for authorisation and approval of access rights: 1. The next closest role to the information asset owner as documented in the User Access Management matrix is able to assume the responsibilities of the asset owner, should the asset owner be unavailable. 2. MAS could also consider the possibility recommending automated user access reviews implemented within an organisation.

		Comments on technology risk management framework: We have no comments on this section.
17.	Life Insurance Association / AIA	Comments on operational infrastructure security: Para 11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet. Could we please clarify on the meaning of isolation, and whether this can be achieved logical or it has to be physical?
	Life Insurance Association / AIA	Comments on IT project management and security-by-design: Para 5.8.2 – Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI's policies, procedures and standards, and achieve the project objectives. Independent QA function - This may not necessarily go well with modern development methodology such as DevOps practices, where software testing is often integrated within the development processes and not necessarily done by an independent party.
	Life Insurance Association / AIA	Comments on IT project management and security-by-design: Para 6.3 – DevOps Management As a principle in DevOps, segregation of duties between Development and Operations is minimized by giving development team higher control using automation tools.

		Would MAS be able to share more details on MAS' expectation in terms of DevOps implementation?
	Life Insurance Association / AIA	Comments on mobile application security: Annex C.1 (a) – avoid storing or caching data in the mobile application to mitigate compromise of the data on the device; Could MAS clarify what is the caching data allowed in the mobile application? Would cookies be considered as caching data?
	Life Insurance Association / AIA	Comments on mobile application security: Annex C.1 (e) – implement a secure in-app keypad to mitigate against malware that captures keystrokes; What does the "in-app keypad" means? Does it mean that this clause is only applicable if the app has a build-in keypad?
	Life Insurance Association / AIA	Comments on online financial services: Para 14.2.7 – The performance of the biometrics solution, based on false acceptance rate38 and false rejection rate, should be calibrated to commensurate with the risk associated with the online activity. Are the FAR & FRR based on the new product during the UAT testing or the statistical performance of the solution provided by the vendor?
	Life Insurance Association / AIA	Comments on technology risk governance and oversight: Para 3.1.5(e) – giving senior executives, who are responsible for executing the FI's technology risk management strategy, sufficient authority, resources and access to the board of directors; Could we clarify with MAS on the senior executives mentioned? We would also like to seek clarification for the term "sufficient authority" & "access to the board of

		directors"? Does it mean a required reporting line to the board of directors?
	Life Insurance Association / AIA	Comments on technology risk governance and oversight: Para 3.5 – Competency and Background Review What is the requirement from FI to demonstrate it in terms of the extent of competency and background review of contractors' and service providers's staff. Would this require annual attestation from the contractor or service provider of their staff's background and competency? Some of the contractors or service providers may not be willing to provide this.
	Life Insurance Association / AIA	Comments on cyber security assessment: Para 13.2.3 – To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment. Would FI be required to conduct PT in the production environment if FI is able to maintain similar setup between UAT environment and production environment, and able to meet the objective of accurate assessment of penetration testing? PT on production is less intrusive and cannot find certain vulnerabilities. Testing should be conducted on both production and UAT with appropriate controls. Para 13.4 – Adversarial Attack Simulation Exercise Is FI required to demonstrate conduct the adversarial attack Simulation exercise on an annual or progressive basis?
	Life Insurance Association / Aviva	Comments on IT project management and security-by-design:

		We would like to seek clarification on the following sections: 6.1 What is the difference between application security testing (6.1) and penetration testing (13.2)? 6.5 Emphasis should be placed on the business to engage IT frequently so that IT may offer the appropriate support described within the section.
	Life Insurance Association / Aviva	Comments on online financial services: 14.1.6 Is the need to inform law enforcement agencies limited to phishing attempts by source impersonating to be the FI targeting at the FI's customers? 14.3 Clarification needed for the extent of "actively monitor".
	Life Insurance Association / Aviva	Comments on technology risk governance and oversight: We would like to seek clarification on the following sections: 3.1.5 Is it mandatory to have a CISO or Head of Information Security? Can the responsibilities be assumed by the CIO? 3.1.5 Where it is a shared services model at regional or group level, how will items (c), (d), and (e) be applied?
	Life Insurance Association / Aviva	Comments on technology risk governance and oversight: 3.2.2 What is the definition for attendant risks?
	Life Insurance Association / Aviva	Comments on technology risk governance and oversight: 3.5.2 What is the scope of background/ screening check?

		And what are the disqualifying criteria?
	Life Insurance Association / Aviva	Comments on cyber security assessment: 13.2 Penetration testing conducted on the production environment may be disruptive. Suggest to do conduct penetration testing in an UAT environment instead.
	Life Insurance Association / Etiqa	Comments on IT resilience: 8.2.3. During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management Clarity should be provided on the member compositions of "management". As stated in the TRM Guidelines, the role of senior management has been defined. Thus, member compositions of both management and senior management may possibly differ. MAS may wish to consider that the Board or its delegated committee shall also provide oversight of Disaster Recovery planning within the financial institution. This include the review and endorsing of defined recovery objectives of critical systems. Otherwise, further guidance could be provided in setting of RTO for critical systems. This recommendation should also be aligned with the changes that will be applied in the MAS BCM Guidelines as follows: "4.3 the Board should (b) review and endorse, at least annually, the FI's critical business functions, business continuity objectives4 and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place; and "
	Life Insurance Association / Etiqa	Comments on operational infrastructure security: 11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and

		prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following: MAS may wish to include “data in use” as well for completeness.
	Life Insurance Association / Etiqa	Comments on IT project management and security-by-design: 5.1.2 Detailed IT project plans should be established for all IT projects. The existing wordings may create the impression that plans should be very detailed, rather than sufficiently detailed to contain the appropriate information. Other than the suggested components, MAS may wish to include the key risks and mitigation plans as a consideration in IT project plans. 5.3.2 The FI should ensure the vendor puts in place robust software development and quality assurance practices, as well as stringent security practices to safeguard and protect any sensitive data the vendor has access to over the course of the project. An FI can request the vendor to declare its software development and quality assurance practices, as well as security practices. However, an FI may not have the capacity or capability to verify the information or conduct audits without incurring additional efforts and costs. Nonetheless, an FI may rely on an independent third party audit report on vendor development or security practices, if the vendor is able to provide. However, it is to note that not every vendor would conduct such independent audits. To this end, it is recommended to amend the use of “ensure” to “assess”. An FI should assess the software development and security practices, however, it can’t “ensure” such practices. 5.3.4 A source code escrow agreement should be in place,

		based on the criticality of the acquired software to the FI's business For commercial off-the-shelf solutions which are commonly deployed around the world, such as MS Windows, MS Office, Oracle database etc., a source code escrow agreement may not be practical. In this regard, MAS may wish to state instead, that financial institutions assess the risk of access to the source code before deciding if such an escrow agreement is required. 5.6.2 The FI should use track and verify that system requirements are met by the current system design and implementation. There could be a typographic error here.
	Life Insurance Association / Etiqa	Comments on software application development and management: 6.1.3 The FI should ensure its software developers are trained to apply the standards when developing software. If software developers are a contracted service, the responsibility for training and adherence to training standards may not lie with the FI. To this end, MAS may wish to require instead, that software developers are adequately skilled and competent to apply the standards when developing software.
	Life Insurance Association / Etiqa	Comments on software application development and management: 6.1.4 The FI should use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. Static, dynamic and interactive application security testing methods typically require tools or services. Financial institutions should be permitted to choose any methods applicable such as manual source code review in line with

		the assessed risks as long as they can achieve the intended outcomes. 6.1.6 The FI should ensure issues and software defects discovered from the source code review and application security testing, which affect the confidentiality, integrity and availability of information and the IT system, are tracked and remediated before production deployment With adequate risk assessment, mitigating measures as well as controls measures emplaced, an FI may proceed with production deployment before issues are resolved. To this end, the production deployment should be permissible.
	Life Insurance Association / Etiqa	Comments on technology risk governance and oversight: 3.1.5 The board of directors or a committee delegated by it, is responsible for: (e) appointing a Chief Information Officer, Chief Technology Officer or Head of Information Technology (d) appointing a Chief Information Security Officer or Head of Information Security We would like to clarify if the above-mentioned roles should be independent of each another. For smaller-scaled financial institutions, this may not be practical as the information and cyber security responsibilities may in some organisations, be undertaken by the Head of Information Technology who oversees IT infrastructure and services in line with the company's appetite for information / cyber risks.
	Life Insurance Association / Etiqa	Comments on technology risk governance and oversight: 3.1.6 Senior management is responsible for: (f) ensuring there is an independent audit function to assess the effectiveness of controls, risk management and governance within the FI. To maintain the independence of the third line of defence, the board of directors should be responsible for the appointment of independent audit for technology risk and

		governance. In respect of a larger scale of insurer, the appointment can be delegated to the sub-Board.
	Life Insurance Association / Etiqa	Comments on technology risk governance and oversight: 3.4.2 Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognised by the industry, before entering into a contractual agreement or partnership with the service provider. Due diligence should be performed in tandem with the risk associated with service provider. It may not be possible to obtain the specific industry accreditation. The indicative considerations should be included as examples.
	Life Insurance Association / Etiqa	Comments on technology risk governance and oversight: Footnote #4 (page 12): Third party is understood as a broad sense, including: (i) all forms of outsourcing (including cloud computing services) The sentence can be easily misinterpreted by financial institutions that all cloud computing services constitute outsourcing arrangements. The definition of an outsourced function must be satisfied before considering Para 6 – Cloud Computing with reference to MAS Outsourcing Guidelines
	Life Insurance Association / Etiqa	General Comments: Sufficient time should be granted for financial institutions to implement the revised regulations, particular the changes that may involve investments in IT assets and complex solutions.
	Life Insurance Association / Etiqa	Comments on cyber security assessment: 13.2.1 A combination of blackbox and greybox testing should be conducted for online financial services. The limitations of greybox testing such as limited scope /

		effectiveness, should be noted. MAS may wish to consider permitting financial institutions to consider blackbox and greybox testing in accordance with the assessed risks.
	Life Insurance Association / Etiqa	Comments on technology risk management framework: 4.4.6 To mitigate risks, the FI could consider taking insurance cover for various insurable technology risks, including recovery and restitution costs. We presume that the recommendation refers to an insurance coverage that should indemnify own damage losses for financial institutions only.
	Life Insurance Association / Friends Provident	Comments on IT project management and security-by-design: Re: Section 5.3, would like to suggest that ESCROW be positioned as 'may be put in place' rather than 'should be put in place'. Usefulness of access to source code varies greatly on many factors.
	Life Insurance Association / Friends Provident	Comments on online financial services: Re: Section 14.1.6 on "The FI should actively monitor the Internet, mobile application stores, social media websites, emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers. ", we would appreciate if MAS can provide more explanation on the extent of "actively monitor". We are of the view that FIs may be more reactive in general. Re: Section 14.3 on Fraud Monitoring, is it really an achievable expectation or applicable to all business models? We would appreciate if further explanation on the "extent of the monitoring" can be provided. We are of the view that FIs may be more reactive in general. Re: Section 14.4.3, we would appreciate if MAS can provide greater clarity on the extent to which MAS would expect an FI to be active in alerting their customers to cyber threats and incidents.

	Life Insurance Association / Friends Provident	Comments on access control: Re: Section 9.3.2 on "The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards." would like to suggest a 'may' and not a 'should'.
	Life Insurance Association / Friends Provident	Comments on technology risk management framework: Re: Section 3.5.2 – We would appreciate further guidance on what is expected as a suitable background check. For instance, would normal pre-employment references be sufficient or are financial and/or criminal checks expected?
	Life Insurance Association / FWD	Comments on IT resilience: 8.3.5 Do we do this disaster recovery with other FIs?
	Life Insurance Association / FWD	Comments on software application development and management: 6.5.3 How would you define shadow IT in the FSI
	Life Insurance Association / FWD	Comments on technology risk governance and oversight: 3.1.5 Must this be a local entity CISO or can it be leverage on a regional role?
	Life Insurance Association / FWD	Comments on technology risk governance and oversight: 3.1.5(h) Must this review be signed off?
	Life Insurance Association / FWD	Comments on technology risk governance and oversight: 3.2.1 Must this review be signed off?
	Life Insurance Association / FWD	Comments on technology risk governance and oversight: 3.4 Ajax claim repair or marketing partners Expatriates partner are they deem as Third Party Services?

	Life Insurance Association / FWD	Comments on IT service management: 7.5.5 Is roll back plan be tested for each and every change prior to production implementation?
	Life Insurance Association / Manulife	Comments on software application development and management: Under section 6.1.3 The FI should ensure its software developers are trained to apply the standards when developing software. What is the expectation of MAS in terms of security training for developers? Are software developers expected to undergo any training on any specific standards (such as OWASP, NIST etc)? Under section 6.4.3 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. The vetting criteria should take into account the third party's nature of business, security policy, industry reputation and track record amongst others. What is the expectation of MAS in terms of vetting the third parties connecting via APIs? Should they undergo vetting similar to a third party technology risk assessment (such as Standard Information Gathering, Pentesting and other controls)?
	Life Insurance Association / Manulife	Comments on application security testing: Annex A - Application Security Testing- A.2 - Is it mandatory to conduct all three tests mentioned - Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST) for all applications. Does an application which undergoes pen-test still need to undergo DAST & IAST?

	Life Insurance Association / Manulife	Comments on online financial services: Under section 14.2.5 when implementing time-based one-time-passwords (OTPs), the FI should establish a validity period that is as short as practicable to lower the risk of a stolen OTP being used for fraudulent transactions. What is MAS suggestion on validity period for OTP's? Incase there is no suggestion, are FIs expected to perform a risk assessment on the duration of the time window and select the duration that is most appropriate for their services?
	Life Insurance Association / Manulife	Comments on technology risk governance and oversight: Under section 3.1.5(d) the guideline says to appoint a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme. For companies which are international and have global headquarters in other part of the world where this role is already present, should there be an additional role that needs to be specifically Singapore based or the global or regional (Asia) role would suffice the requirement?
	Life Insurance Association / Manulife	Comments on technology risk governance and oversight: Under section 3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes. Is there a timeline for "periodically" i.e. monthly or Quarterly? Or is it up to the entity to define the timelines?
	Life Insurance Association / Manulife	Comments on technology risk governance and oversight: Specific guidelines on cloud computing and IT outsourcing which are available in the MAS TRM 2013 guidelines seems to have been removed and merged into a much broader topic – 3.4 Management of Third Party Services.

		What are MAS expectations on cloud computing with regards to the revised guidelines?
	Life Insurance Association / Manulife	Comments on IT service management: Under section 7.2.2 The FI should review and verify the configuration information of its information assets on a regular basis to ensure they are accurate and kept up to date. Is there a timeline for "regular" i.e. monthly or Quarterly? Or is it up to the entity to define the timelines? Is section 7.2.2 reiterating the same that has been said in section 3.3.2?
	Life Insurance Association / Manulife	Comments on cyber security assessment: Under section 13.3 The FI should carry out regular scenario-based cyber exercises to validate and review its response and recovery, as well as communication plans against cyber threats. These exercises could include social engineering, table-top, or cyber range exercises. a) Are cyber exercises mandatory for all FIs including Insurance companies? b) What is the expectation in terms of the frequency of conducting cyber exercises – is there a frequency recommended by MAS? c) Would the participation in Raffles exercise comply with this requirement? Under section 13.4 Adversarial Attack Simulation Exercise – What is the expectation in terms of conducting red teaming exercises for global organisations? Does specific exercise need to be conducted for Singapore offices or activities conducted at global level involving SOC teams monitoring Singapore are sufficient?

	Life Insurance Association / Manulife	Comments on access control: Under section 9.1.5 Multi-factor authentication should be implemented for users with access to critical system functions to safeguard the systems and information from unauthorised access. Is this guideline only for critical system facing internet or is also applicable to internal critical systems not connected to internet? If there are no critical systems within an entity does it mean this requirement or guideline is not applicable?
	Life Insurance Association / Prudential	Comments on software application development and management: Section 6.1.4: There is a mention that "FI should use mixture of static, dynamic and interactive application security testing methods". Is the expectation either Static +Interactive, Dynamic+ Interactive testing?
	Life Insurance Association / Prudential	Comments on online financial services: Section 14: Should this section be named more obviously as Online Financial and Insurance Services if this entire section is applicable to Insurance Online Services as well Section 14.2.3 Would like to clarify that "Sensitive customer data includes customer office and home address, email and telephone contact details", is that MAS interpretation of sensitive data? We may not necessary identify them as sensitive individually if that does not attribute to uniquely identify an individual. Section 14.4.1: " whenever changes are made to the security features of the services." – Can this be at the FI discretion to determine whether to inform or not?
	Life Insurance Association / Prudential	Comments on cyber security assessment:

		Section 13.2.3: We have concerns on Penetration testing on Production system as that affects the integrity of Production data and even possibly availability of the system
	Life Insurance Association / Tokio Marine Life	Comments on operational infrastructure security: 11.1.7 – What is the minimum guideline that FIs should adopt for "irrevocably removed"? E.g. Level of wipe on the media before disposal
	Life Insurance Association / Tokio Marine Life	Comments on IT project management and security-by-design: 5.3.2 – We would like to understand better MAS' expectation of FIs monitoring the access of the vendor to its systems, and the extent an FI should go to ensure that the vendor has various practices in place. Is the monitoring supposed to be in real-time and can reliance on certifications (e.g. ISO 27001) suffice? 5.3.4 – A clearer definition is needed on when the escrow should come into effect and the minimum requirements that should be in place in the agreement to comply with this section.
	Life Insurance Association / Tokio Marine Life	Comments on technology risk governance and oversight: 3.1.6(c) – We would like to understand better how the delineation of duties in managing technology, especially on the security side, can be achieved using RACI. This is because in small organizations, it may not be always possible to ensure a clear segregation of some roles. In addition, we would like to clarify if there is an expectation on covering all the typical 3 Lines of Defence in this requirement.
	Life Insurance Association / Tokio Marine Life	Comments on technology risk governance and oversight: 3.2.3 – Would like to clarify the responsible party in the organization to ensure that the compliance processes, verification and follow-ups are carried out. Is MAS expecting the Second Line (e.g. Compliance, Risk

		Management) to do so, or would some staff in the IT department suffice?
	Life Insurance Association / Tokio Marine Life	Comments on technology risk governance and oversight: 3.4 - In the context of using third party services, more detailed guidance (i.e. in addition to paragraphs 3.4.1, 3.4.2 and the footnote 4) should be provided This is because financial institutions have used MAS' outsourcing definition to date, and with the removal of the "Management of IT Outsourcing Risks" section of the TRM Guidelines, it is unclear what third party providers will be in scope. In addition, if the requirement is retrospective, then sufficient time (e.g. 2 years) should be given to ensure that existing vendors all comply with this section.
	Life Insurance Association / Tokio Marine Life	Comments on technology risk governance and oversight: 3.5.2 - Background checks on contractors and service providers by financial institutions might not be practical due to the number of turnovers and it is primarily the responsibility of the contractor and service provider to ensure that their staff are fit and proper.
	Life Insurance Association / Tokio Marine Life	Comments on technology risk governance and oversight: 3.6.3 – The level of security awareness and training for Board will be quite different from general staff. Instead of extending the training programme, a separate one should be tailor-made for the Board of Directors.
	Life Insurance Association / Tokio Marine Life	General Comments: The "Revision to Technology Risk Management Guidelines" consultation paper as a whole sets a very high standard for organizations to meet and it may only be realistically complied by very mature and adequately resourced financial institutions. Although TMLS agrees that the technology landscape warrants better TRM practices and the document is a guideline, we hope that MAS exercises greater discretion and allow financial institutions more flexibility in implementing the guidelines that are relevant to its size, complexity and level of maturity. It may thus be

		useful to have in each section, a distinction between what are highly expected and what are merely good practices. This will provide clarity to the industry and better alignment of expectations.
	Life Insurance Association / Tokio Marine Life	Comments on access control: 9.1.5 – Would like to seek clarification at which point minimally should the need to implement 2FA for user access. If the organization does not have a defined critical system, does this mean that 2FA is not required? 9.3.2 - We would like to enquire if insurance agents' devices are in scope for this section.
	Life Insurance Association / Transamerica Life	Comments on operational infrastructure security: For 11.3.6, we would like to clarify "application white-listing" is just one of the examples to ensure FI has security measures in place to restrict the installation of authorised software. We may implement similar security measures to achieve the same objective based on our system security framework.
	Life Insurance Association / Transamerica Life	Comments on technology risk governance and oversight: For 3.1, with respect to the point on both BOD and senior management need to have members with necessary skills and understanding of technology risks, further guidance on the extent of expected skills and knowledge of technology risks would be helpful.
18.	Life Insurance Association ISCCS	Comments on software application development and management: - What is the aceptable encryption standards and key management?
	Life Insurance Association ISCCS / AIA	Comments on IT project management and security-by-design: Independent QA function - This may not necessarily go well with modern development methodology such as DevOps

		practices, where software testing is often integrated within the development processes and not necessarily done by an independent party.
	Life Insurance Association ISCCS / AIA	Comments on software application development and management: As a principle in DevOps, segregation of duties between Development and Operations is minimized by giving development team higher control using automation tools. Would MAS be able to share more details on MAS' expectation in terms of DevOps implementation?
	Life Insurance Association ISCCS / AIA	Comments on mobile application security: Could MAS clarify what is the caching data allowed in the mobile application? Would cookies be considered as caching data?
	Life Insurance Association ISCCS / AIA	Comments on mobile application security: What does the "in-app keypad" means? Does it mean that this clause is only applicable if the app has a build-in keypad?
	Life Insurance Association ISCCS / AIA	Comments on online financial services: Are the FAR & FRR based on the new product during the UAT testing or the statistical performance of the solution provided by the vendor?
	Life Insurance Association ISCCS / AIA	Comments on online financial services: Are the FAR & FRR based on the new product during the UAT testing or the statistical performance of the solution provided by the vendor?
	Life Insurance Association ISCCS / AIA	Comments on technology risk governance and oversight: Could we clarify with MAS on the senior executives mentioned? We would also like to seek clarification for the term "sufficient authority" & "access to the board of

		directors"? Does it mean a required reporting line to the board of directors?
	Life Insurance Association ISCCS / AIA	Comments on cyber security assessment: Would FI be required to conduct PT in the production environment if FI is able to maintain similar setup between UAT environment and production environment, and able to meet the objective of accurate assessment of penetration testing.
	Life Insurance Association ISCCS / AIA	Comments on cyber security assessment: Is FI required to demonstrate conduct the adversarial attack Simulation exercise on an annual or progressive basis?
	Life Insurance Association ISCCS / AIA / MSIG	Comments on technology risk governance and oversight: AIA: What is the requirement from FI to demonstrate it in terms of the extent of competency and background review of contractors' and service providers's staff. Would this require annual attestation from the contractor or service provider of their staff's background and competency? Some of the contractors or service providers may not be willing to provide this. MSIG: In a intra-group scenario, is reliance on group background check sufficient?
	Life Insurance Association ISCCS / AXA	Comments on cryptography: - What is MAS stand on using key management from cloud provider even if it fulfill the requirements stipulated in TRM?
	Life Insurance Association ISCCS / AXA	Comments on IT audit: Any recmmendation or suggestion to who would be the correct party to determine or assess the competency and skills of the IT auditors?

	Life Insurance Association ISCCS / AXA	Comments on technology risk governance and oversight: Does it includes devices not own or managed by FI such as Telecommunciation equipment which technically is owned by telco?
	Life Insurance Association ISCCS / AXA	Comments on technology risk governance and oversight: 3rd party seems to be relating to:- - outsourcing - services rendered to insurer, - interconnected counterparties what about business partner with no interconnection? (e.g users using your services like portals?) - Include insurer's tight agents? - How detail is expected of the due diligence? - Financial - how far back? - How or any means to assess or determine the reliability? - How or any means to assees or determine the capability?
	Life Insurance Association ISCCS / GE	Comments on cryptography: Feedback The appliance maybe embedded with cryptographic algorithm for the purposes of HTTPS or SSH or etc, and the product owner is unwilling to share the CPRNG and CSPRNG details. The same applies to 3rd party hosting such as Cloud platform. Will there be any exemption?
	Life Insurance Association ISCCS / GE	Comments on cryptography: Clarifications Rigorous testing or vetting is to be performed by FI or using reference from well-established international standards
	Life Insurance Association ISCCS / GE	Comments on cryptography: Feedback The appliance maybe embedded with cryptographic

		algorithm for the purposes of HTTPS or SSH or etc, and the product owner is unwilling to share the CPRNG and CSPRNG details. The same applies to 3rd party hosting such as Cloud platform. Will there be any exemption?
	Life Insurance Association ISCCS / GE	Comments on cryptography: Clarifications Rigorous testing or vetting is to be performed by FI or using reference from well-established international standards?
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Feedback Prevent and detect Data Theft will be challenging and it could also imply Digital Right Management solution to track digital record.
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Feedback Real-time scanning of IOCs of significant impacts which the organization deemed essential. As this is scanning of all potential IOC can be intensive to end users and infrastructure supporting businesses, as well as 3rd party hosting implications
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Feedback Real-time scanning of IOCs of significant impacts which the organization deemed essential. As this is scanning of all potential IOC can be intensive to end users and infrastructure supporting businesses, as well as 3rd party hosting implications
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Feedback Application whitelisting could be operational intensive for FI, 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 and hamper agility of the organisation. Alternative measures such as advanced malware detection software should also be considered.
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Feedback Application whitelisting could be operational intensive for FI, 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 and hamper agility of the organisation. Alternative measures such as advanced malware detection software should also be considered.
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Clarification / Feedback Hypervisor (e.g. Esxi) does not has the OS interface, feature and OS controller (except BIOS) like Windows/ Unix servers. The configuration is merely accessible via vsphere web interface via remote client to configure the VMs. Hence, may not be possible to restrict administrative access.
	Life Insurance Association ISCCS / GE	Comments on operational infrastructure security: Clarification / Feedback Hypervisor (e.g. Esxi) does not has the OS interface, feature and OS controller (except BIOS) like Windows/ Unix servers. The configuration is merely accessible via vsphere web interface via remote client to configure the VMs. Hence, may not be possible to restrict administrative access.
	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification On application security testing in Agile software development, does it imply Annex A requirements must be

		fulfilled (dynamic and interactive) for every releases, as it will slow down releases.
	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification The end user computing and application are usually created by the business units to enhance their business processes. Is MAS expecting this type of application to follow the IT SDLC process from review to testing?
	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification Should the Software developers be industry body certified or internal training certified with specific programming language?
	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification The definition of "mixture of static, dynamic, and interactive" appears to be contradicted with the definition of "interractive" in Annex A "involves a combination of SAST and DAST techniques". For example mixture of static with interactive, does it means combination of SAST with IAST (SAST+DAST), thus SAST appears to be redundant. Could the mixture means combine the various results from different vendor, for example vendor A tested SAST and Vendor B tested IAST?
	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification On application security testing in Agile software development, does it imply Annex A requirements must be fulfilled (dynamic and interactive) for every releases, as it will slow down releases?

	Life Insurance Association ISCCS / GE	Comments on software application development and management: Clarification The end user computing and application are usually created by the business units to enhance their business processes. Is MAS expecting this type of application to follow the IT SDLC process from review to testing?
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations:Clarification What is MAS definition of real-time? Can it based on organization definition or is there a best practices that organization should follow? The same principles and enquiries applies to definition of critical systems.
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations: Clarification Is MAS expecting organization to implement solution or tool to fulfil user profile baselining?
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations: As above
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations: Clarification What is MAS definition of real-time? Can it based on organization definition or is there a best practices that organization should follow? The same principles and enquiries applies to definition of critical systems.
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations: Clarification Is MAS expecting organization to implement solution or tool to fulfil user profile baselining?
	Life Insurance Association ISCCS / GE	Comments on cyber surveillance and security operations:

		As above
	Life Insurance Association ISCCS / GE	Comments on online financial services: Clarification Does MAS has any guidelines on the expected validity period for the OTP?
	Life Insurance Association ISCCS / GE	Comments on online financial services: Clarification Is MAS expecting FIs to inform customers of all changes made to the security features or only the major ones? Can MAS quote some examples on the changes made to the security features that require to notify customers?
	Life Insurance Association ISCCS / GE	Comments on online financial services: Clarification Does MAS has any guidelines on the expected validity period for the OTP?
	Life Insurance Association ISCCS / GE	Comments on online financial services: Clarification Is MAS expecting FIs to inform customers of all changes made to the security features or only the major ones? Can MAS quote some examples on the changes made to the security features that require to notify customers?
	Life Insurance Association ISCCS / GE	Comments on IT service management: Feedback As most of the changes to production environment are technology-centric and mainly about technical implementation details, it may not be meaningful for business management to participate in change advisory board.
	Life Insurance Association ISCCS / GE	Comments on IT service management: Clarification

		Can be subjective for application software to have audit and security logs and require exemption based on criticality and legacy system.
	Life Insurance Association ISCCS / GE	Comments on IT service management: Feedback As most of the changes to production environment are technology-centric and mainly about technical implementation details, it may not be meaningful for business management to participate in change advisory board.
	Life Insurance Association ISCCS / GE	Comments on IT service management: Clarification Can be subjective for application software to have audit and security logs and require exemption based on criticality and legacy system?
	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: VA should be conducted in production only for more accurate assessment since it is non-intrusive?
	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: Feedback Pen-test on production is potentially disruptive. We suggest flexibility should be given to FI to use UAT or virtualized environment for pen-test, as long as the source code & configuration closely mirror the Production system.
	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: Clarification Does MAS has any guidelines on the definition of major changes or updates?
	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: VA should be conducted in production only for more accurate assessment since it is non-intrusive?

	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: Feedback Pen-test on production is potentially disruptive. We suggest flexibility should be given to FI to use UAT or virtualized environment for pen-test, as long as the source code & configuration closely mirror the Production system.
	Life Insurance Association ISCCS / GE	Comments on cyber security assessment: Clarification Does MAS has any guidelines on the definition of major changes or updates? Does MAS expects PenTest to be done for internal systems?
	Life Insurance Association ISCCS / GE	Comments on access control: Clarification Definition of user management activities for e.g configuration of mail server, performing software upgrade, enabling and disabling of debug mode and etc
	Life Insurance Association ISCCS / GE	Comments on access control: Feedback Alternative measures that are as effective as MFA in protecting the authentication credentials of critical systems should also be considered, such as privilege access management solution that lodge system passwords and only release them for temporary use, and immediately reset the password after use. Clarification Can legacy system such as AS400 be exempted?
	Life Insurance Association ISCCS / GE	Comments on access control: Clarification Can there be an exemption for legacy systems or implementation based on system criticality?

	Life Insurance Association ISCCS / GE	Comments on access control: Clarification Does the Definition of user management activities includes for e.g configuration of mail server, performing software upgrade, enabling and disabling of debug mode and etc?
	Life Insurance Association ISCCS / GE	Comments on access control: Feedback Alternative measures that are as effective as MFA in protecting the authentication credentials of critical systems should also be considered, such as privilege access management solution that lodge system passwords and only release them for temporary use, and immediately reset the password after use. Clarification Can legacy system such as AS400 be exempted?
	Life Insurance Association ISCCS / GE	Comments on access control: Clarification Can there be an exemption for legacy systems or implementation based on system criticality?
	Life Insurance Association ISCCS / GE / AXA	Comments on operational infrastructure security: GE: Feedback Prevent and detect Data Theft will be challenging and it could also imply Digital Right Management solution to track digital record. AXA: Data theft focusing on electronic theft only or include photo-taking, screen shots or photocopying or hard-copies?
	Life Insurance Association ISCCS / GE / MSIG	Comments on software application development and management: GE: Clarification Software developers have to be industry body certified or internal training certified with

		specific programming language. MSIG: Is developers is outsourced or turnkey projects, is it included/applied?
	Life Insurance Association ISCCS / GE / MSIG	Comments on software application development and management: GE: Clarification The definition of "mixture of static, dynamic, and interactive" appears to be contradicted with the definition of "interractive" in Annex A "involves a combination of SAST and DAST techniques". For example mixture of static with interactive, does it means combination of SAST with IAST (SAST+DAST), thus SAST appears to be redundant. Could the mixture means combine the various results from different vendor, for example vendor A tested SAST and Vendor B tested IAST? MSIG: If it is total outsourced development, can we rely on the process and practice from the outsourced vendors? Do we have to enforced this process on the vendors?
	Life Insurance Association ISCCS / Income	Comments on IT resilience: Is virtual data centre also in scope of this section? As virtualization technique expands it capabilities, a clusters of hypervisor machines on a server rack can easily be virtualized into a data centre through sophiscated operating system with data centre functions. Hence, the definition of data centre should be precise to ensure that FIs protect their virtual data centre which is housed in a server rack or computer room.
	Life Insurance Association ISCCS / Income	Comments on operational infrastructure security: While the virtualisation at platform (Infrastructure and network) was addressed, nothing was catered for application virtualisation, such as "portable applications". Would MAS consider expanding virtualisation security to also include the expectations on app-V containers?

	Life Insurance Association ISCCS / Income	Comments on IT project management and security-by-design: Is there a direction/guideline over project steering committee setup? This is because, while it is good to have an oversight over the projects, the project needs to be at at particular value prior such oversight function is required. For smaller FIs, this can be challenging.
	Life Insurance Association ISCCS / Income	Comments on IT project management and security-by-design: Will there be guideline over source code escrow agreement? E.g. new codes should be deposited after each major release or when a change of code took place, types of object deposited with the escrow agent include source code objects in readable format, compiler used, system platform type for the code to be compiled, etc.
	Life Insurance Association ISCCS / Income	Comments on cyber surveillance and security operations: Should real-time monitoring of cyber events be limited to only critical systems or internet facing systems? This is because malicious actor would often identify the weaker links and focus on the easier target instead of an asset with all monitoring efforts.
	Life Insurance Association ISCCS / Income	Comments on cyber surveillance and security operations: Is there an expectation over the retention of system logs by the regulator?
	Life Insurance Association ISCCS / Income	Comments on technology risk governance and oversight: Definition of data, hardware or software would need to expand to include new entities such as smart contracts which could be blockchain based, API, IoT within gadgets/facility managed device such as light bulbs or aircon.
	Life Insurance Association ISCCS / Income	Comments on technology risk governance and oversight: As BYOD is also in focus, could regulator also share the

		expectations of BYOD from a risk governance and oversight in this section?
	Life Insurance Association ISCCS / Income	Comments on technology risk governance and oversight: Could Training programme commensurate with the level of data classifications. In other words, the higher the corporate rank, more awareness training should be provided as the impact from a data leakage from the higher rank official is much more damaging. E.g. the recent HIV data leak. Hence, security training programs for higher rank officials should be frequent, more in depth and thorough. More often, technical competencies of key roles could have been obsoleted given that technology advances at a rapid rate. Hence, could MAS provide guidance over the minimum standard of training each key roles should have to ensure that existing competency of the key holders remain valid? A similar guidance from HKMA's enhanced competency framework on cybersecurity could be considered as a guiding document.
	Life Insurance Association ISCCS / Income	General Comments: Does this paragraph also apply to non-banking institutions using API to offer innovative services? Definition of open banking had not include non-banking institutions such as brokerages, insurance, fund houses
	Life Insurance Association ISCCS / Income	General Comments: Please lay the fundamentals of "weak links", where possible, provide examples, if not define the perspective. For e.g. weak link should be defined as the weaker connections which could exist in the form of data interface, people, processes or APIs.
	Life Insurance Association ISCCS / Income	Comments on IT service management:

		In the event of obsolete technology, is there a limit to how long a dispensation from its management can FI seek?
	Life Insurance Association ISCCS / Manulife	Comments on operational infrastructure security: "data at rest - data in computing endpoints such as notebooks, personal computers, portable storage devices and mobile devices, as well as files stored on servers, databases, backup media and storage platforms (e.g. cloud)." Does this statement mean a need to encrypt at the file level?
	Life Insurance Association ISCCS / Manulife	Comments on technology risk governance and oversight: "appointing a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme;" For MNCs, due to the inter-connected nature of a large part of the infrastructure and systems, the IT security programme may be executed on a global level. Hence the CISO appointed may not be based within the local subsidiary but has responsbility for multiple localities of which the Singapore subsidiary is part of. Would this suffice i.e. Does the CISO appointment need to be local or can be at the regional level.
	Life Insurance Association ISCCS / Manulife	Comments on technology risk governance and oversight: Is there any expected format or level of detail for a asset inventory of information asset?
	Life Insurance Association ISCCS / MSIG	Comments on operational infrastructure security: System that are not designed for database encryption such as legacy database or applications
	Life Insurance Association ISCCS / MSIG	General Comments: Does MAS mean we need to have a roadmap to implement

		it when we not able to do it now due to some reasons or limitations or business/management decisions or risk appetite?
19.	Microsoft Operations Pte Ltd.	Comments on IT resilience: 8.3.5 Where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and verified to meet its business needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems. While Microsoft agrees with the proposal by the MAS for FIs to ensure that disaster recovery arrangements are properly tested and verified to meet business needs, the proposal for FIs to participate in disaster recovery testing that is conducted by service providers is neither universally necessary nor feasible. A hyperscale cloud provider should design its service such that either disaster recovery is entirely the responsibility of the cloud provider or that clear instructions are provided to the FI on how to configure and use the cloud services such that disaster recovery is entirely under the FI's control. Thus with a well-designed hyper-scale cloud service no part of the disaster recovery plan is conducted together with customers, and there is no purpose served by joint testing. CSPs can provide FIs with information about their business continuity management programs and testing reports, as well as independent 3rd party certifications covering disaster recovery processes and evidence of compliance, e.g., ISO 22301, and SOC 2 Type II. Instead of requiring joint testing, it should be required that the FI ensure that the service providers' disaster recovery arrangements are "properly tested and verified," as set forth in the first sentence of 8.3.5. As such, we recommend the second sentence regarding FI participation in service providers' testing be modified to read: "The FI should assess the service provider's disaster recovery processes and, if there are any recovery steps requiring coordinated action between the service provider and the FI, participate

		in the disaster recovery testing that is conducted by service providers managing the FI's critical systems."
		Comments on IT project management and security-by-design: 5.3.3 If the project involves commercial off-the-shelf solution that does not meet the FI's requirements, the FI should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed. 5.3.4 A source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. It is not feasible for Microsoft and other hyperscale cloud service providers and software vendors to provide access to their proprietary source code (including through an escrow arrangement), given the rapid pace of change for code, the immense complexity in recreating the entire hyperscale cloud, and the importance of such intellectual property to their business. It is not clear whether that is the intent of this section. If 5.3.4 was intended to apply only in a situation as in Section 5.3.3, where the vendor writes customized source code for the FI such that there may not be adequate substitutes for such software, the provision makes more sense and we would recommend that Section 5.3.4 be revised to read: "Where customized source code is being written by the vendor for the FI, the FI may want to consider entering into a source code escrow agreement, according to the criticality of the acquired software to the FI's business, or taking other measures to ensure that the FI can have access to the source code in the event that the vendor is unable to support the FI." Otherwise, if that was not MAS's intent, we recommend deleting Section 5.3.4 in its entirety. FIs can rely on Section 5.3.1 - 5.3.3, which set forth the principles that should be considered in system acquisition without requiring access to proprietary source code.

		(Similarly, we note that MAS may want to clarify in Section 6 on Software Application Development and Management, that the "source code review" referenced in 6.1.1 and 6.1.2 is only applicable to software applications developed by the FI and not to third-party, non-customized software.)
		Comments on technology risk governance and oversight: 3.4 Management of Third Party Services Microsoft supports the revisions reflected in Section 3, which appears to replace the former Section 5 on "Management of IT Outsourcing Risks." Section 3.4.1-3.4.2 are good examples of principles-based guidelines which complement the more specific guidance in the Outsourcing Guidelines.
		General Comments: Microsoft would like to thank the Monetary Authority of Singapore ("MAS") for the opportunity to provide comments on the proposed revisions to the Guidelines on Technology Risk Management ("TRM Guidelines"). Microsoft supports MAS's initiative to continue to evolve the TRM Guidelines in light of the transforming technological landscape of the financial sector, and increasing experience of both MAS and financial institutions ("FIs") in technology risk management. We commend MAS for continuing to take a principles- and risk-based approach to the TRM Guidelines. Imposing overly prescriptive requirements could cause any guidance to fall out of step with developing technologies and may also have the undesired effect of stifling innovation in the financial sector. Microsoft particularly commends MAS for making this concept explicit in the "Application of the MAS Technology Risk Management Guidelines" section, where it states: "The extent and degree to which an FI implements the Guidelines should be commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services." The inclusion of these new paragraphs 2.2 and 2.3 is helpful. Other examples of improved provisions reflecting this approach are 3.4.2 (Management of Third Party Services);

		6.4 (API development); 7.3 (Technology Refresh Management); 7.7 (Incident management), and 8.1 (Availability). Overall, Microsoft views these proposed changes to the TRM Guidelines as positive and an appropriate reflection of technological and industry developments since the 2013 version.
		Comments on access control: 9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. This provision should not be directly transposed on cloud service providers. Cloud service providers will be unable to adhere to each customer's own security standards. Instead, the FI should assess the service provider's security standards, controls and policies and to determine whether these are sufficient to properly secure access by the service provider to the service provider's information assets. We suggest Section 9.3.2 be revised to clearly exclude cloud service providers, or in the alternative to clarify that the FI should assess the cloud service provider's security standards, controls and policies.
20.	MRS	Comments on technology risk governance and oversight: 3.1.5 c) and d) Within a Global organisation, there are Global Roles appointed as CIO, CTO, CISO or Head of IT/Security in the Global IT Structure. Regarding to the Branch level in Singapore, does the branch need to appoint a local representation?
21.	MSIG Insurance (Singapore) Pte. Ltd.	Comments on cryptography: No comments
		Comments on IT resilience: No comments

		Comments on operational infrastructure security: No comments
		Comments on IT project management and security-by-design: No comments
		Comments on software application development and management: It is not always possible to ask for a source code review from the application developers, especially in Software-As-A-Service situations. Can this be managed on a risk-based basis? Similarly, it is not always possible to ask for a source code escrow agreement as proposed in paragraph 5.3.4. There could be legal technicalities involved.
		Comments on cyber surveillance and security operations: Paragraph 12.2.1 refers to monitoring or surveillance systems of cyber events for critical systems. Does "critical systems" herein bear the same meaning as in MAS Notice 127? Does MAS have any expectation on the duration for keeping the logs? Would MAS like to consider the need to have Network Time Protocol to ensure all clocks are in sync for logs synchronization?
		Comments on IT audit: No comments
		Comments on application security testing: No comments

		Comments on BYOD security: No comments
		Comments on mobile application security: No comments
		Comments on online financial services: No comments
		Comments on technology risk governance and oversight: Board and Senior Management Role & Responsibility The proposed revised Guidelines stipulates that both the Board and senior management of a FI should have members who have the knowledge to understand and manage technology risks, which will include risks posed by cyber threats (paragraph 3.1.2). There is a limited pool of qualified technology personnel available in Singapore for appointment to the Board level. In any event, the role of a (non-executive) Board member should not extend to "managing technology risks" which is an operational responsibility. This requirement also seems contrary to paragraph 3.6.3 which stipulates the need for the Board to be subject to training on technology risks. Can a technology director ask to be exempted from such Board training? Similarly, the proposed responsibilities of the Board or a committee delegated by the Board appear to be too onerous on the Board (paragraph 3.1.5): if implemented, they extend the role of the Board to micro-managing technology risks and placing a management responsibility on the entire Board. Even if one Board member has the technical expertise to understand the technicalities involved, other Board members may not be able to understand the details. Does this mean that the other Board members will need to rely on the technology director?

		Even at operational level, it may not be easy for a FI to find a suitable senior management staff who is well-versed in technology. Can such a responsibility be undertaken by an organization at regional level? Can such a responsibility be outsourced to a professional consultant?
		Comments on technology risk governance and oversight: Management of Information Assets The proposed definition of "information assets" in paragraph 3.3.1 is rather wide and vague. Does it extend to applications, licenses? Will MAS be prescribing the information asset inventory? Or can FIs use their current or own-developed format?
		Comments on technology risk governance and oversight: Management of Third Party Services Most if not all services rendered by third party service providers (regardless of outsourcing or not) will involve using IT in one way or another. Many will involve holding onto customers information, e.g. workshops, adjusters, law firms. While the financial industry may be moving in a certain direction, the reality is that some industries (particularly, for general insurers, the workshop or body parts industry) lack the capability and ability to move in tandem and at the same pace. On the proposed assessment to be performed by FIs, would MAS be able to provide a security checklist for FIs to follow?
		Comments on technology risk governance and oversight: Competency and Background review It does not seem practical to ask for or have background checks performed on personnel of contractors and service providers. What kind of background check is acceptable to MAS? A Certificate of Clearance from the Police? Bankruptcy checks? Technical qualifications? If a FI were to

		engage a contractor or third party to do a job, it is because the FI may not have the relevant expertise. How would the FI then, have the ability to check on the competency of the contractor/third party? Further, this seems to be contrary to the Yellow Ribbon project to integrate reformed criminals to society. Would this also disadvantage experienced older workers who may not have the paper technical qualifications? Would such a background check be required when the service provider is a related company?
		Comments on technology risk governance and oversight: Security Awareness & Training On security awareness and training at paragraph 3.6.1, is MAS's expectation that all staff must be trained on the details of applicable laws, regulations and guidelines on information assets? There are different levels of staff in an organization: some of these staff in backend operations may not be able to grasp nor appreciate such details. Can organizations decide the scope and depth of the awareness and training programmes?
		General Comments: While the proposed revised Guidelines will enhance IT security for the financial industry, complying with the same may be challenging for the smaller Financial Institutions (FIs). Some of the FIs may still be operating legacy systems which are being phased out in stages. Will MAS allow exceptions for such legacy systems, with insurers managing the same on a risk-based basis? Similarly, smaller-scale service providers and contractors of FIs may not be able to support the requirements of the proposed revisions.
		Comments on IT service management: In paragraph 7.7.2, a 24/7 incident response capability is

		mentioned. This may not always be available in the market.
		Comments on cyber security assessment: Paragraph 13.2.3 states that Penetration Testing should be conducted on the production environment for a more accurate assessment. However, this may disrupt or interfere with operations and corrupt the data. Can MAS leave it to FIs to decide on this issue?
		Comments on access control: Paragraph 9.1.5 states that multi-factor authentication should be implemented for users with access to critical system functions to safeguard the systems and information from unauthorised access. "critical system functions" is further annotated as "[T]he criticality of a system function may be assessed based on the sensitivity of the data and criticality of the system". Can MAS clarify that the use of the words "critical system" herein does not bear the same meaning in MAS Notice 127? Does MAS want to clarify that revocation of access apply as well to paragraph 9.2 on Privileged Access Management?
		Comments on technology risk management framework: No Comments
22.	Oliver Wyman	Comments on IT resilience: Para 8.5) In addition to considering the political and economic climate of Data Centres (DCs) in designing Threat and Vulnerability Risk Assessment (TVRA), we recommend also considering segregation between in-house and outsourced data centres due to different risk characteristics associated with the two types of data centres.

		Comments on operational infrastructure security: Para 11.1) In addition to defining comprehensive data loss prevention policies for “data in motion” and “data at rest”, we recommend including “data in use” as the 3rd classification of data that requires data security. “Data in use” refers to data that is being used, processed or updated within a system.
		Comments on operational infrastructure security: Para 11.2.8) We recommend including, if not replacing DoS with, Distributed Denial of Services (DDoS), to guide FIs to develop leading capabilities for technology risk management.
		Comments on operational infrastructure security: Para 11.3.6) We suggest expanding the examples of security measures to include blocking of portable extension files as they are often source of malicious codes.
		Comments on operational infrastructure security: Para 11.5.2) We suggest also emphasising about the need for ongoing monitoring of controls that mitigate risks from the Internet of Things to ensure effectiveness.
		Comments on IT project management and security-by-design: Para 5.1) The reader, presumably a Chief Technology Officer, Chief Risk Officer or someone playing a similar role, should be made aware of the challenges associated about working with various stakeholders across the FI. We propose adding this challenge to help manage the expectations of senior management and set context for the project team from the FI. Para 5.2.2) While the roles of steering committee have been defined clearly, there is no guideline around the frequency of meeting of the steering committee. We recommend such project steering committees to meet at

		least quarterly, during the period when active projects are being carried out. Para 5.4) We recommend including a point about developing a tracking or monitoring mechanism for the FI to know if the security-by-design principles are being used effectively during every phase of SDLC and they are efficient in preventing cyber events. Para 5.5) We recommend the FIs to periodically assess the performance of the systems against the security requirements that are set at the time of acquiring / developing a system, to ensure that the system continues to perform as per the expected security levels. Para 5.7) We recommend clarifying that system testing should not just be limited to a single testing phase but should be conducted across the entire SDLC. One of the models that could be referenced for system testing across the SDLC is the V model for software testing. We also recommend including the test of resilience as an aspect of system testing to align this with the types of system requirements as described in 5.5.1
		Comments on software application development and management: Para 6.1.3) We recommend encouraging FIs to get external certifications for their software developers to ensure compliance to international standards such as the ISO12207. Para 6.2) We suggest further detailing the guidelines to incorporate security practices such as test drive development and periodic refactoring of the code, throughout the Agile process. We also suggest broadening the definition of “application security testing” to both infrastructure and application security testing to ensure full clarity. Para 6.3) We suggest adding further details on DevOps phases that are relevant to enhancing security:

		Regular operations phase: utilise continuous monitoring and automate enforcement Integration phase: carry out checks on both internal and external endpoints and analyse the impact of new workloads on security policies Infrastructure creation phase: leverage on test utilising tools Image creation and hardening phase: automate where possible Build phase: leverage on code analysis technologies Para 6.4) We recommend incorporating the option of automated API testing to reduce the possibility of human error and enhance the security of API integration.
		Comments on cyber surveillance and security operations: Para 12.1.4) The guideline asks for a process to establish timely dissemination of cyber related information with internal stakeholders. We recommend expanding this to ensure establishing process to ensure timely response and action from the internal stakeholders also. Para 12.3) We recommend establishing a framework to categorise cyber events into different criticality levels, based on expected severity and impact. This framework should be used as the basis to define incident response plans. We also recommend including that the cyber response should include details on collaboration and coordination required among various departments. Lastly, we encourage FIs to measure and monitor the efficacy of their cyber incident response plans and learning from actual cyber incidents to improve on these.
		Comments on online financial services: Para 14.3) We suggest including techniques such as artificial intelligence and machine learning to identify fraudulent activities. Para 14.4) We recommend providing more details on

		specific security measures, such as those mentioned in paragraphs 14.1.6 and 14.2.4, that customers should be informed about.
		Comments on technology risk governance and oversight: Para 3.6) We recommend FIs to develop specific training for IT operators and developers as they are key personnel managing technology risk. In addition, similar to the separate training programme for board of directors, there should be a customised training for senior management to ensure they have the adequate skill-set for guiding the organisation in case of actual cyber-attacks. Also, it is important to measure the effectiveness of training programmes in establishing security awareness. For this purpose, completion rates of trainings should be tracked, and relevant tests should be conducted to test employees' awareness levels. The results of these tests should be reported to management to ensure the training programmes achieve the desired outcomes.
		Comments on technology risk governance and oversight: Para 3.1.5) In the first statement, where it lays down responsibilities of board of directors or a committee delegated by it, we suggest replacing "committee" with "board committee" for greater clarity. We suggest to also include the ongoing monitoring of effectiveness of risk management practices and key issues of significance faced by the FI in role of the board of directors.
		Comments on technology risk governance and oversight: Para 3.1.6 (f). Ensuring that there is an independent audit function to assess the effectiveness of controls, has been mentioned as a responsibility or senior management. In our experience, this should be responsibility of board of directors to ensure independence of the audit function.
		Comments on technology risk governance and oversight: Para 3.4) The guidelines describe that FIs should assess

		third party service providers, we suggest for FIs to assess all third-party service providers on a periodic basis to ensure an ongoing view on their capabilities to manage associated technology risks. In our opinion, a one-off assessment at time of onboarding is not sufficient.
		Comments on technology risk governance and oversight: Para 3.5.2) In addition to background checks, MAS should encourage FIs to establish internal controls to ensure that no one individual has been given too much access that can potentially compromise the overall security of the organization. Depending on background checks to minimize risk from insider threat is not sufficient.
		General Comments: While emphasising the importance of managing technology risk efficiently, there could be mention of added complexity due to increasing use of third- party technology vendors by FIs. The draft paper provides details on setting risk management policies but does not mention guidelines relating to tracking and ongoing monitoring of effectiveness and efficiency of these risk management practices. There could be greater emphasis on that. We provide specific instances where focus on ongoing monitoring could be included in subsequent sections Comment on proposed definitions: • "Financial Institutions (FI)". We suggest, for clarity to the reader, to either include examples that illustrate what qualifies as a FI or define it as an entity that receives an MAS licence. The latter approach has the advantage of a more consistent definition of FI to the reader. • The paper currently uses the terminology "technology risk" while it also touches on aspects of "cyber risk". We suggest to better define the difference and/or relatedness of these two concepts as per below: "Technology risk" broadly speaking includes cyber risks (e.g. attacks on cyber space) and IT risks (e.g. software glitches)

		"Cyber risk" focuses on the risks from malicious attackers to intentionally cause harm to syste\ms. Examples include malware, ransomware, and distributed denial of service (DDoS).
		Comments on IT service management: Para 7.2) In our experience, large cyber events can be caused due to errors in configuration management, and hence, we recommend FIs to put in place adequate controls around configuration management.
		Comments on IT service management: Para 7.6) To provide that traceability and accountability of the all software code, we recommend FIs to have an internal policy to govern software release. Given the different nature of software release (e.g. minor release, major release and emergency releases), an internal policy creates traces, clarity and consistency in the frequency and circumstances which a software feature can be released.
		Comments on IT service management: Para 7.7.3) We recommend adding two points: • Highlighting the need for collaboration across teams to handle IT incidents as often, these incidents require collaboration across several business, operations and IT teams • Defining and monitoring performance against service level agreement for staff and external parties along every step of the incident response plan
		Comments on IT service management: Para 7.7.7) We recommend clarifying that regulators also need to be informed, wherever appropriate, in case of IT incidents.
		Comments on IT service management: Para 7.8) We suggest clarifying that a feedback loop should be created to ensure learnings from the incidents can be

		used to improve the risk management practices within the FI
		Comments on cyber security assessment: Para 13.2.3) We recommend adding details on red / blue teaming and threat hunting to encourage FIs to use leading penetration testing practices. In red / blue teaming, the red team tries to penetrate different systems to find vulnerabilities. On the other hand, the blue team is tasked to find ways to defend and strengthen the response to the attack. We recommend mentioning red / blue teaming because it takes penetration testing to a greater level by simulating the roles of the attacker and the defender. Threat hunting proactively looks for attackers that have not been active, or detected in the network, allowing greater insight into potential vulnerabilities.
		Comments on access control: Para 9.3) While MAS has defined guidelines for allowing staff remote access, we recommend also providing guidelines for third-party vendor remote access. In the event which the FI would like to provide remote access to a third-party vendor, it should include security measures such as granting access on a FI-issued IT equipment and to selected individuals with high clearance from the vendor. In addition, we suggest blocking off remote access to critical and / or sensitive assets to minimise the possibility of a data leakage and any other security breaches.
		Comments on technology risk management framework: Para 4.1.3) In reporting the key risks to the board of directors and senior management, we suggest encouraging FIs to develop a cyber risk appetite statement to identify areas of key risk exposures and using that for reporting. A cyber risk appetite should cover key components of the NIST framework and provide visibility to senior

		management along key exposure areas. This will allow senior management to identify areas of high exposure within the FI, and then suggest actions to mitigate the risk. Para 4.3) We suggest MAS to highlight the benefits from the risk assessment exercise to encourage adoption. One benefit from that could be mentioned is that knowing risk exposure helps senior management make informed decisions around technology investment and risk hedging measures.
23.	Prudential Assurance Company Singapore	Comments on operational infrastructure security: 11.2.5: Can the insecure network protocols be used granted that there is adequate compensating controls in place ? E.g. the use of FTP in a point to point connectivity (leased line) or if the underlying file is encrypted with file-level encryption.
		Comments on operational infrastructure security: 11.5.3: The first sentence here implies that access to all IoT devices (e.g. CCTV, IP TV, IP Phone, etc) must be secured with strong authentication. Is that understanding correct or the expectation is limited to only administrator access to IoT devices that need to be secured with strong authentication ? Further guidance / clarity here would be appreciated.
		Comments on IT project management and security-by-design: 5.8.1: What is expected quality attribute and assessment metrics? 5.8.2: Is the expectation a separate independent QA team be set up to perform this function?
		Comments on software application development and management: 6.1.4: There is a mention that “FI should use mixture of static, dynamic and interactive application security testing

		methods". Is the expectation either Static +Interactive, Dynamic+ Interactive testing? 6.3.2: Can we have further guidance / clarification whether this means we need to have different staffs assigned to each different DevOps functions ? Given the efficient and automated nature of DevOps, is such staffs level segregation really required ?
		Comments on cyber surveillance and security operations: 12.2.3: Is this limited to logs from Production systems only ? Further clarification / guidance here would be appreciated. 12.2.9: What would be the expected retention periods of system logs ? Appreciate further clarity on this.
		Comments on BYOD security: B.1(a) Can Mobile Application Management (MAM) be considered as an equivalent substitute for Mobile Device Management (MDM) solution ? Further clarification / guidance here would be appreciated.
		Comments on online financial services: 14. Can this section be named more obviously as Online Financial and Insurance Services if this entire section is applicable to Insurance Online Services as well? 14.2.3 : Would like to clarify that "Sensitive customer data includes customer office and home address, email and telephone contact details", is that MAS interpretation of sensitive data? We may not necessary identify them as sensitive individually if that does not attribute to uniquely identify an individual. 14.4.1: With regards to " whenever changes are made to the security features of the services."

		– Can this be at the FI discretion to determine whether to inform customers or not?
		Comments on cyber security assessment: 13.2.1: Is this applicable to all system regardless whether they are internet facing or not and whether they are considered critical systems or not ? Further clarification / guidance here would be appreciated. 13.2.3: We have concerns on Penetration testing on Production system as that affects the integrity of Production data and even possibly availability of the system. If our systems in UAT are close replica to Production, is that acceptable as well? 13.4.1: Can this adversarial attack simulation exercise by a red team be substituted by an automated & agent-based attack simulation software like SafeBreach ?
		Comments on access control: 9.1.3: The "logging" requirement in this statement, does it refer to all systems regardless of its criticality and functionalities (e.g. Prod, Dev, Test)? Further guidance and clarify on this would be appreciated.
		Comments on technology risk management framework: 4.4.6: Can we have further guidance like example of technology risks that can / should be considered to be insured ?
24.	Prusik Investment Management Singapore Pte Ltd	Comments on cryptography: No comments.
		Comments on IT resilience: No comments.

		Comments on operational infrastructure security: No comments.
		Comments on IT project management and security-by-design: No comments.
		Comments on software application development and management: No comments.
		Comments on cyber surveillance and security operations: No comments.
		Comments on IT audit: No comments.
		Comments on application security testing: No comments.
		Comments on BYOD security: No comments.
		Comments on mobile application security: No comments.
		Comments on online financial services: No comments.
		Comments on technology risk governance and oversight: No comments.

		General Comments: No comments.
		Comments on IT service management: No comments.
		Comments on cyber security assessment: No comments.
		Comments on access control: No comments.
		Comments on technology risk management framework: No comments.
25.	RBC Investor Services Trust Singapore Limited	Comments on IT resilience: Is this referring to the "Switch and Hold" test case? If so, how long is the minimal expectation to fulfill this requirement? Is this only applicable to MAS Critical systems? Does TVRA also apply to FI's Global Data Centre and DR Centre (Internal, Non colocation DCs) outside Singapore?
		Comments on operational infrastructure security: Is this applicable to end user computers and devices (with Internet surfing capabilities) which have a direct access to MAS Critical systems? Similar to network segregation/isolation for SWIFT CSP 1.1 Mandatory Control Requirement "SWIFT Environment Protection"?
		Comments on technology risk governance and oversight: MAS expectations in terms of the appointment of a local CISO/CIO. Could this be a regional or global role, who sits

		outside Singapore but a member of the local board or senior management team in RBC SG entity?
		Comments on cyber security assessment: Unclear in terms of what is requirement to meet MAS expectations in terms of scope and "regular" frequency of local Cyber exercises. Is once every 2 years acceptable?
		Comments on access control: Does this imply and prohibit the use of personal/non corporate managed device and Virtual Desktop Infrastructure (VDI) solution? If so, this may potentially impact BCM plan if FI rely on remote access via home desktops or personal smart devices.
26.	REIT Association of Singapore	General Comments: We submit that the TRM Guidelines are more relevant for the Fis that provide time-sensitive and critical financial services to the public and hold sensitive financial data of their customers (such as banks and insurance companies). A REIT Manager's primary role / business function is to set the strategic direction of the REIT and give recommendations to the Trustee on acquisition, divestment or enhancement of the assets in accordance with its stated investment startegy. The operations of REIT managers are such that we do not possess or store sensitive financial data of the REIT's unitholders and provide the Unitholders with critical financial services. It is submitted that the TRM Guidelines should provide flexibility for Fis such as REIT Managers to determine for themselves the best approach to technology risk management given the nature, size and complexity of their business operations, rather than imposing a one-size-fits all approach that does not take into account the business characteristics of REIT Managers.
27.	RHT Compliance Solutions	Comments on IT resilience: 1. Some participants felt that the topic on IT resilience does not connect the TRM guidelines with the BCM

		guidelines which gives the impression of a very narrow view of achieving recovery. IT recovery should be from a broader perspective on how it impacts the overall recovery of the business function, and not just the IT aspect alone. Participants feel that it would be beneficial if there were to be some form of reference. 2. The current TRM guidelines recognises that in some cases, FIs may use data centres ("DC") provided by a third party and states explicitly that FIs must obtain a TVRA report before using a DC facility provided by the provider. However, there is no mention on the specifics about the requirements in the revised guidelines and participants sought clarification on this. 3. We noted that both the TRM Guidelines and BCM Guidelines were published on the same day. However, we found inconsistencies in the definitions of RTO and RPO in the TRM and BCM guidelines. To avoid confusion, we propose that MAS make the definitions consistent: a. In the TRM Guidelines, RTO is the duration of time from the point of disruption within which a system should be restored. However, this definition does not say the end point from the point of disruption – there is no definite timeline. In the BCM guidelines, the definition is more specific in that it comprises: (1) the duration of time from the point of business disruption, to the point of declaring the activation of BCP(s) for business functions or units and interdependencies, and (2) the duration of time from the BCP activation to the point when the specific business function or unit is recovered to its Minimum Performance Level. b. In the TRM Guidelines, RPO refers to the acceptable amount of data loss for a system should a disaster occur. It is unclear what situations would be considered a disaster. In the BCM Guidelines however, it defines RPO as the maximum tolerable data loss and this is measured from the point of the last backup.

		Comments on online financial services: 1. Real-time fraud monitoring is not possible for all products and where possible, it is onerous for FIs to be able to detect real time fraud and block those transactions from happening at the same time. One participant suggested to leverage off the end user protection guidelines in that whenever an online transaction has been performed, a real time notification be sent to those customers for them to verify that the transaction is valid. In the event they detect anything suspicious or a transaction that is not authorised by them, they can flag it out immediately.
		Comments on technology risk governance and oversight: 1. The revised guidelines place greater focus on technology risk governance and oversight, with additional requirements that both the Board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. Participants felt that this is onerous and difficult to achieve as it is not realistic to find Board members who can understand and manage technology risk and cyber threats. 2. As financial institutions reliance on technology to carry out their financial services, technology risk and knowledge are no longer solely an IT issue but more of an organisational issue now. Hence the proposed guidelines place greater onus on the Board and senior management, and requirements being more prescriptive. a. Participants sought clarification on how FIs level of knowledge of technology risk is expected of Board members and how they can ensure that the Board has such knowledge when they are situation overseas in the headquarters for example. b. We would also like to seek clarification on whether the committee delegated to perform the role of Board of Directors in technology risk management has to be a Board-level committee, or whether it can be a Management-level committee. c. Participants found the requirement for Board to have at

		least one Director to understand and manage technology risks is overly onerous for many of the smaller FIs. d. As this set of TRM Guidelines is not legally binding, and the requirements are very onerous or not possible to meet, especially where the financial institutions run a lean operation, we request clarification on how MAS would gauge FIs' compliance to guidelines. It would be helpful if MAS could share what factors would be considered in deciding how much FIs should scale down on these onerous requirements. 3. One of the responsibilities of the Board as set out in the guidelines is the appointment of a CIO and CISO. However, this would pose as a practical constraint for the smaller FIs. Participants sought clarification on whether it would be allowed for FIs to have CISO as a hired service. Basically, to have CISO as an outsourcing arrangement. 4. One of the requirements of the revised guidelines is for FIs to conduct assessment on third party exposure – third party arrangements that are not ordinarily included as outsourcing in the revised guidelines. However, definition of what constitutes a third party is too broad and impractical as it encompasses standardised and non-standardised services such as telecommunications and power, interconnected counterparties and FMIs. These were specifically carved out from the outsourcing guidelines, and participants would like to seek clarification on why there is a change in stance. In the event that MAS considers it necessary to have this requirement, it would be neither efficient nor realistic for each FI to do this assessment on the same service provider that is being used by most players in the industry. Participants suggested that these third party due diligence be done in conjunction with ABS' list of OSPAR Audited Outsourced Service Providers since this report is an industry effort. This would be more a more practical and efficient approach. 5. In addition to the above, participants sought clarification on the extent to which they have to apply the third party management requirement retrospectively they would not

		have fulfilled the requirements in respect of third party service not considered outsourcing. For example, banks would have their own set of outsourcing guidelines which complies to the MAS Outsourcing Guidelines, and so most banks would probably not have fulfilled the requirements of conducting the risk assessment and due diligence e.g. Power provider. Participants wanted to clarify whether this requirement meant that banks will need to retrospectively do the due diligence on those parties which they have not done so. 6. Further, participants felt that MAS should take into consideration the practical constraints the industry would face in regard to the requirement to conduct due diligence on third party service provider. For example, there had been breaches where mail with customer information ended up in the trash bin, but SingPost remain the only main mail delivery service provider. Participants would like to seek clarification on what they should o in such situations where service provider did not meet their standards of due diligence but there were no alternatives.
		General Comments: RHT Compliance Solutions Pte. Ltd. conducted a roundtable discussion with industry members/financial institutions around the substantive proposed measures raised in the Consultation Paper on Proposed Revised TRM Guidelines issued on 7 March 2019 (the "Consultation Paper"). The roundtable was attended by 125 attendees from 89 companies on 1 April 2019. Participants included representatives from banking and financial institutions across a broad spectrum. Whilst we are broadly supportive of the proposals, we urge MAS to further consider the implications of some suggestions raised in the Consultation Paper. Our comments on the measures posed in the Consultation Paper are set out below and incorporate, where appropriate, inputs received from the roundtable participants.

		1. With regards to the entire guidelines, what is a realistic duration given to FIs to implement these changes / requirements?
		Comments on access control: 1. In the cyber hygiene consultation paper, it is a legal requirement that all systems with confidential data that can be assessed remotely be secured with a multi-factor authentication. However, the revised guidelines made no reference to this. Participants feel that it would be useful if MAS could clarify and elaborate on this in the revised guidelines.
		Comments on technology risk management framework: 1. Participants felt that the identification of a risk owner was a useful addition to the revised guidelines. However, they sought clarification on what MAS considers as a risk owner. Is the risk owner a technology person, or is the business who uses the service of the technology the risk owner?
28.	Schroder Investment Management (Singapore) Ltd	Comments on cryptography: 10.1.3. Can you please clarify what constitutes 'rigorous testing'? We would like to suggest that cryptographic algorithms that satisfy industry accepted standards from the NIST and/or GCHQ (CESD) would be sufficient.
		Comments on IT resilience: 8.3.4 Can the statement for operating from a recovery site for an 'extended period' be clarified?
		Comments on operational infrastructure security: The requirements listed are comprehensive and sensible. Many of the suggested improvements to security would likely be major initiatives for many FIs, and would require time to implement.

		Comments on IT project management and security-by-design: 5.1 This section seems to emphasise a waterfall like delivery model, however projects can also be delivered using alternate methodologies such as Agile frameworks. Whilst there is a section on Agile software delivery (6.2) we would like to suggest the project management section also include references to agile project delivery framework. We would like to propose that project governance should be proportionate to the criticality, cost, complexity and scale of the project. For example, sections 5.5 and 5.6 should be driven by the criticality of the system. 5.7 The system testing and acceptance section also seems to emphasis a waterfall model. For those FIs that have adopted Agile delivery methods, these requirements are encompassed in shorter iterations through for example continuous integration and delivery, and we would suggest that this be reflected in the guidelines as acceptable practice.
		Comments on software application development and management: We understand that the requirements of section 6, including the purpose of secure coding, source code review and application security testing, to be applied across the SDLC. We would like to propose that FIs should adopt a framework of these controls that can be applied in a manner that is commensurate with the criticality of the application. This would enable FIs to emphasize the application of stronger controls to critical applications. 6.3.2 We would like to suggest enforcing the segregation of duties for the development, testing and operations functions in its DevOps processes can be achieved through technical means, well as through process or people segregation. 6.5.3 Can you please clarify the guidance on Shadow IT?

		The draft states that “End User should not be allowed to use Shadow IT until... approved for use”. The term Shadow IT suggests it is unapproved IT already in use; is it instead suggested that policy be established so that users understand that Shadow IT is not allowed?
		Comments on cyber surveillance and security operations: 12.2.9 It is the industry norm to retain logs online for 1-3 months, and offline for at least one year. We would like to seek guidance on what is the recommended retention period for system logs should there be a need to support an investigation.
		Comments on IT audit: No comment
		Comments on application security testing: No comment
		Comments on BYOD security: No comment
		Comments on mobile application security: No comment
		Comments on online financial services: No comment
		Comments on technology risk governance and oversight: 3.1.2 We would like to propose differentiating the requirement to ‘understand’, from the requirement to ‘manage’ technology risks. We would like to suggest the Board should understand the impact of technology risks including cyber threats, whilst both the understanding and management of technology risks including cyber threats

		should sit with senior management who would typically have more expertise to address this concern.
		Comments on technology risk governance and oversight: 3.1.5 (e) & 3.1.5 (i), both clauses are similar in the requirement to ensure the provision of adequate resources. We would like to propose both clauses be combined into one clause.
		Comments on technology risk governance and oversight: 3.4.1. Third parties can include entities that are considered market utilities such FMIs (e.g. payment and settlement systems, stock exchanges, central securities depositories and central counterparties). Is the intention for FIs to also conduct due diligence on these FMIs which are typically highly regulated?
		General Comments: No comment
		Comments on IT service management: 7.5.2 Whilst we understand the need to conduct a risk and impact analysis of the change to an information asset so that the operation of the systems is not severely impacted due to the change. However, the criticality of the FI's systems would have different business impact to the operations of the FIs, therefore we would like to include such analysis should be commensurate with the scale of change and criticality of the information asset. This would enable FIs to emphasize on conducting a detailed risk and impact analysis on critical information assets. 7.5.3 It is noted that test plans for changes should be developed and approved by the relevant business and IT management who would be accountable for the test plans. We would like to propose to append the clause 'or by a sufficiently empowered and responsible person within the FI's established risk management framework'.

		7.5.7 FIs can use audit and security logs for investigations and trouble-shooting, however this can include many different types of log and activity recording facilities and is a very broad requirement. Can you please clarify categories of logging facilities expected here?
		Comments on cyber security assessment: 13.2.2 We understand that a bug bounty programme, though useful for identifying vulnerabilities in the systems, may not be appropriate for all types of FIs. As such we are supportive of the proposed language that makes clear this is optional, for consideration, and is not mandatory. 13.3 The need for cyber exercises is to better prepare the FIs in the event of a cyberattack; we would like to propose to add a clause to include a cyber-framework requiring FIs to take a holistic view of threats and establish a programme that is commensurate with the Fl's size, complexity and scale.
		Comments on technology risk management framework: No comment
		Comments on access control: 9.1.3. We would like to propose the FI should ensure records of user access and user management activities are uniquely identified and logged that is commensurate with the criticality of the information asset. 9.1.4 Strong password controls requiring maximum validity and complexity differ to guidance issued from NIST and GCHQ. The NIST Special Publication 800-63B - Digital Identity Guidelines and GCHQ (CESD) - Password Guidance Simplifying Your Approach, specifies password controls such as not imposing password complexity and maximum validity period while there are additional controls. Both publications have provided the rationale that due to the limited ability of humans to memorize complex, arbitrary secrets, they often choose passwords that can be easily

		guessed. Analysis of breached password databases reveal that the benefit of complexity and maximum validity period is not nearly as significant as initially thought, although the impact on usability and memorability is severe. Therefore, we would like to suggest the adoption of guidance similar to NIST or GCHQ (CESD) password controls. 9.3.1. We would like to clarify if the use of multi-factor authentication for remote access is applicable to externally hosted platforms (e.g. SAAS) as well as internal platforms? We would suggest this be commensurate with the criticality of the external service. 9.3.2 We would like propose that this requirement, where remote access to the FI's information assets is only allowed from approved hardened devices, is commensurate with the criticality of the information asset.
29.	SingCash Pte Ltd and Telecom Equipment Pte Ltd	General Comments: 1. We support the MAS circulation and requirements for Financial Institutions to put in place guidelines for technology risk management and business continuity (Guidelines). Our views here cover both sets of Guidelines. 2. There are areas that we feel the MAS may wish to consider and factor into the Guidelines: (a) The MAS indicates that these are Guidelines applicable to financial institutions (FIs). With the impending implementation of the Payment Services Act [PSA] which sets out applicable licensing and regulatory conditions for Payment Institutions [PIs], we seek clarification whether PIs under the PSA will be subject to the Guidelines. (b) We note that many PIs operate smaller scale businesses and or businesses quite different from that of a typical FI. Merchant Acquisition, for example, will require a party to be licensed under the PSA but clearly the merchant acquisition parties today may have difficulty implementing the Guidelines in full. In particular, it is envisaged that most

		of the PIs who are small and medium enterprises will not be able to fully execute the TRM. We believe that the MAS may need to provide for some calibration in the Guidelines to PIs or seek not to implement the Guidelines on such parties. (c) Where the IMDA decides that these Guidelines must be implemented by FI, we note that the Guidelines do not provide clarity on whether FIs or PIs (if the latter are expected to implement the Guidelines) are able to rely on their overall group management TRM and BCM practices. Institutions in the financial services market are increasingly less reflective of a traditional bank. Many parties in the fintech services world have origins in social media and/or other sectors where there are TRM and BCM requirements except that these may not be completely similar to those outlined in the Guidelines. However, for various reasons, these companies require their business units to adopt the overall group approach. We believe that these should also be considered as acceptable for the purpose of compliance with the Guidelines. For example, many of the potential institutions involved could have group practices relating to crisis management, BCPs, testing. These parties should be permitted to rely on their group practices than to implement new requirements. (d) Some of the requirements in the Guidelines also appear to mirror those in the Outsourcing Guidelines. Whilst we see the relevance of these requirements, it may be useful for the MAS to point out that where an institution already implements these aspects under the Outsourcing Guidelines, this will be sufficient for compliance with the TRM and /or BCM Guidelines. This avoids confusion. (e) The Guidelines require that even when usage of third party services do not constitute outsourcing, the institutions should access these accordingly and manage the risks, including proper due diligence, financial viability, track record, accreditation. Examples cited are power supply, interconnected parties etc. We believe this may not be possible in all cases. Commercially available services

		like cloud or data warehousing or even power supply are now so ubiquitous that to impose on these third party suppliers the same requirements of an Outsourced Service Provider may be impracticable. (f) Similarly, the proposal for BCP tests and CMT exercises on an annual basis appears impracticable especially end to end recovery and third party vendor participation are required. The minimum required tests should be either confined to core business functions and/or frequency should be left to FI to decide based on nature of business operation.
		Comments on cryptography: Please see above
		Comments on IT resilience: Please see above
		Comments on operational infrastructure security: Please see above
		Comments on IT project management and security-by-design: Please see above
		Comments on software application development and management: Please see above
		Comments on cyber surveillance and security operations: Please see above
		Comments on IT audit: Please see above

		Comments on application security testing: Please see above
		Comments on BYOD security: Please see above
		Comments on mobile application security: Please see above
		Comments on online financial services: Please see above
		Comments on technology risk governance and oversight: Please see above
		Comments on IT service management: Please see above
		Comments on cyber security assessment: Please see above
		Comments on access control: Please see above
		Comments on technology risk management framework: Please see above
30.	StarHub Ltd	Comments on operational infrastructure security: Comment against section 11.2. Network Security • Employees are increasingly leveraging mobile devices (mobile phones, tablets and laptops operated from outside the FIs physical offices) to conduct their business. Network security should extend to mobile devices and networks. Further, network based security services are now available

		to assess and monitor communications with mobile devices. Leveraging these services, FIs can extend greater flexibility to their staff by allowing them to utilize mobile devices while maintaining controls through which network security can be effectively implemented.
		Comments on technology risk governance and oversight: Comment against section 3.2.3 • Compliance processes should also be reviewed concurrently. Compliance recording options that were only enforceable at the desk-top phone are now available over the mobile network. Traders and relationship managers are now expected to be accessible by their clients at all hours of the day. Compliance recording solutions are now available for mobile subscriptions. Providing Traders and Relationship Managers with a mobile based compliance recording solution will give them greater flexibility without impairing the FI's compliance obligations.
31.	SWIFT	Comments on IT resilience: Section 8.1 IT resilience is largely dependent on the availability and recoverability of systems. It is therefore very important to use the highest availability platforms for the most critical services. There are many variances in recovery mechanisms and it is, ideally, best to choose the most resilient architectures (such as zero-downtime systems) for the most critical services – especially those services that immediately affect the communication with customers and correspondent network.
		Comments on software application development and management: Section 6.4 We believe that, as well as security and encryption standards, data standards can reduce risks in the development process. Specifically for Application Programming Interface (API) development, reliance on existing standards can avoid misinterpretation (of data

		models) which could lead to security gaps. We strongly recommend using the international ISO 20022 financial business data standard, which provides very specific but internationally accepted definitions for financial data elements.
		Comments on cyber surveillance and security operations: Section 12.1.4 We agree that it is very important to maintain good cyber situational awareness. All Financial Institutions should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to its business and IT environment. In addition, a process should be established for timely dissemination of cyber related information with internal stakeholders for their awareness or necessary action. However, we believe the proposed guidelines should also include the requirement to share cyber threat intelligence with its counterparts and/or its community. A cyber threat intelligence and information sharing process should be established for the sharing of cyber related information with internal and external stakeholders and counterparties, while respecting data privacy regulations (e.g. mule accounts).
		Comments on online financial services: Section 14.3.1 We recognise the importance for Financial Institutions to implement real-time fraud monitoring to identify and block suspicious or fraudulent online transactions, with specific focus on sent payment traffic. Follow-up processes should be established to ensure suspicious transactions or payments are investigated and issues are adequately and promptly addressed. We recommend operationally that: • There is clear segregation of duties between payment operations and fraud teams prevention investigations. • Payment and fraud detection environments are hosted separately to reduce the likelihood of multi-point cyber-compromise and ideally that in-network monitoring services should be used. • The solutions should have appropriate security and role

		based permissions architecture, where changes are notified, and there is separation of concerns for, for instance, rules creation and user functions. • An adequate independent record of payment history should be maintained and available to enable rapid recovery and remediation following an attack. • Detection focus should be on transactions between high risk jurisdictions, those involved in new payment corridors, and new parties, and where characteristics are unusual based on previous behaviour. In addition to fraud monitoring within the Financial Institution's production environment, monitoring of the online channel provided by the channel provider will provide a supplementary security layer. Such real-time payment controls service can complement and strengthen the Financial Institution's existing fraud controls. SWIFT's own Payment Controls Service (PCS) is one example: it is a fraud and cyber-crime prevention service that allows SWIFT customers to screen their payment messages according to their own chosen parameters, enabling them to immediately detect any unusual message flows before transmission.
		Comments on technology risk governance and oversight: Section 3.6 We agree that a comprehensive IT security awareness training programme should be established to maintain a high level of IT security awareness by all staff in Financial Institutions. It is very important that employees are fully aware of measures available to help them achieve the highest levels of security, particularly from an endpoint security perspective. We would like to emphasise that the most critical vendors typically provide product training to ensure that their customers can use all the security features at minimum workload with maximum output. SWIFT also provides a number of training courses such as the 'SWIFT Security Bootcamp', 'Manage PKI', 'Security Essentials' and 'SWIFT Customer Security Controls Framework'. The latter curriculum introduces the mandatory security controls for SWIFT users, and guides trainees through each control based on their SWIFT

		architecture type. In this training, we explain the most common risks that they can mitigate by complying with the controls.
		General Comments: SWIFT thanks the Monetary Authority of Singapore for the opportunity to provide comments on its Consultation Paper on Technology Risk Management Guidelines. SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholders, comprising more than 2,000 financial institutions. We connect more than 11,000 institutions in more than 200 countries and territories. SWIFT provides banking, securities, and other regulated financial organisations, as w ell as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest. If you wish to discuss any aspect of our response, please do not hesitate to contact us.
		Comments on technology risk management framework: Section 4.1 We agree with the recommendation that every Financial Institution should establish a strong risk management framework to manage technology risks in a consistent and systematic manner. Effective risk management practices and internal controls should be in place to achieve data confidentiality and integrity, system security and reliability, as well as resilience in the IT operating environment. However, we also believe that Financial Institutions should include risk assessments of their counterparties. As the financial community is highly networked, both at domestic as international level, weaknesses at counterparty level can invoke security issues within an institution's own

		organisation. In the SWIFT Customer Security Control Framework, we have incorporated a guideline to control business relationships.
32.	The Association of Banks in Singapore	Comments on cryptography: <10.2.4> There is increasing shift to authenticate customer password on server runtime instead of HSM to avoid microcode changes in HSM especially with cloud implementation. Could the paragraph be amended to take this into account?
		Comments on cryptography: 10.1.3 MAS proposed that FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements. This is somewhat contradicting to 10.1.1 or has unclear focus. It seems to us that this control has two areas of applicability: First, to rely on community vetting of algorithms and second, to perform the right amount of tests to ensure that any algorithm will operate smoothly in the environment. In particular, please provide examples of the expected tests.
		Comments on cryptography: 10.1.3 [page 38] The Bank would like further clarity on what is required in the testing or vetting process.
		Comments on cryptography: 10.2.1 A cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established. Comments:

		We would like to propose MAS to allow FIs to have some flexibility to record cryptographic key management requirements as technical standards as well besides the forms of policy and procedures. Please see suggested edits below: "A cryptographic key management policy or technical standard and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established."
		Comments on cryptography: 10.2.1 We note that key recovery, to the extent required in specific situations, is not explicitly covered by paragraph 10.2.1. We would like to suggest that key recovery is included in the cryptographic key management policy and procedures. Please refer to our related comment on paragraph 10.2.9.
		Comments on cryptography: 10.2.2 While we suspect it is highly unlikely to be MAS' intention, the second sentence of this paragraph practically prevents FIs from using key derivation functions (KDFs) (as defined in NIST SP800-133 paragraph 7.3) as mechanisms to generate (session) keys based on long term key material or passphrases (the latter as used in password based KDFs), as its literal interpretation would require the long term key material or the passphrase to be destroyed, which is contradictory to the legitimate purpose of applying (PB)KDFs. The second sentence similarly prevents FIs from using any modern key exchange algorithm (e.g. Diffie-Hellman or Elliptic Curve Diffie-Hellman, typically part of HTTPS/TLS), as such algorithms generate session keys based on long term keys, which ought not be destroyed in order to protect a system's continued well-functioning. Our impression is that the intention of paragraph 10.2.2 is to ensure that long term or master keys are not

		compromised through the capture of a CSPRNG's input such as system entropy and/or a CSPRNG's output in memory (e.g. transient seed key) that is used to seed the key generation algorithm. We note that market best practices in key generation are exclusively based on the use of software libraries such as, but not limited to, OpenSSL, BoringSSL, Microsoft Cryptography API: Next Generation (CNG) and (FIPS 140-2 compliant) hardware security modules (HSMs) that transparently take care of safe memory management on behalf of the system administrator. This allows the system administrator to safely abstract over such internal details, which is well aligned with the "don't roll your own crypto" mantra. Therefore, to avoid deep technical debate on mathematical topics and focus on promoting sound security behaviour, we would like to propose that the second sentence is replaced with "Key generation shall be performed by using a trusted library or trusted cryptographic subsystem, and be used and/or invoked according to the product or system manual".
		Comments on cryptography: 10.2.3 We fully recognize the importance of defining, managing and enforcing key lifetimes as MAS rightfully seeks to pursue in paragraph 10.2.3. However, we note that leading industry standardization on key lifetimes does not take data sensitivity levels as a basis to determine key lifetimes, since: 1. such data is not available to the general industry; 2. cyber security threats related to key lifetimes are generally independent of data sensitivity levels, and 3. the general starting point for using cryptography is that the data is worth protecting, regardless of the precise sensitivity label For example, the leading industry body that sets the standard for X.509 (TLS) cryptographic certificate lifetimes, the CA/Browser Forum, regularly updates such lifetimes irrespective of the use case. The most recent example is CA/Browser Forum Ballot 193, which can be located here: https://cabforum.org/2017/03/17/ballot-193-825-day-

		certificate-lifetimes/. Another observation that we would like to share is that technical capabilities to generate keys and certificates are generally shared in nature and thus typically take a standardized approach to implementing and executing key generation, again, irrespective of the use case. In our vision, the implementation of detailed security use cases such as key generation should not linearly depend on the sensitivity of the data but rather enable its application in practice in all contexts. Therefore, we would like to suggest that the appropriate lifespan of cryptographic keys is to be defined based on a comprehensive threat assessment rather than data sensitivity and criticality of individual systems, taking into account prevailing market standards with respect to key lifetimes.
		Comments on cryptography: 10.2.4 Our understanding of paragraph 10.2.4 is that it attempts to address two distinct topics: 4. hardening of systems that authenticate customer passwords, and 5. storing cryptographic keys in a tamper resistant way We note that market best practices to implement authentication of customer passwords from a storage point of view are not dependent on cryptographic keys but rather (keyless) cryptographic one-way functions, which strengthens our belief that the two topics are distinct. We are concerned that the current wording may lead to unduly wide interpretations, and as such we would like to propose to split paragraph 10.2.4 into two separate paragraphs. Additionally, we do recognize MAS' concern about protection of cryptographic keys at rest, and we indeed recognize that hardware security modules are one potential solution. Should MAS choose to follow our suggestion to split this paragraph into two separate paragraphs, then we would like to suggest that part b) is accompanied with an outlook on multiple possible solutions where the decision to design and implement HSMs specifically is based on a risk assessment. This is to ensure that the return on

		investment remains positive, as HSMs are relatively expensive to procure and operate. We would like to propose to split paragraph 10.2.4 into two separate paragraphs. Should MAS choose to follow our suggestion to split this paragraph into two separate paragraphs, then we would like to suggest that part b) is accompanied with an outlook on multiple possible solutions where the decision to design and implement HSMs specifically is based on a risk assessment.
		Comments on cryptography: 10.2.9 Additionally, we would like to remark that cryptographic keys only strictly require backup and recovery in case their structural loss of availability otherwise would permanently and irrevocably prevent access to stored data. Multiple cryptographic use cases exist where recovery of the associated business process could alternatively be facilitated in a more cost effective way by generating a new key, such as TLS based on auto-enrolment or SSH. Therefore, we would like to suggest to rephrase the second sentence in paragraph 10.2.9 into “FIs should maintain clear criteria to require the creation and management of backups of cryptographic keys for recovery purposes. Any such backups should be accorded a high level of protection.”.
		Comments on cryptography: 10.2.2 "After a key is generated, the FI should destroy sensitive materials that are used to derive the keys in the key generation process" Would suggest specifying which keys require this kind of governance as this is hard to achieve in a very distributed environment.
		Comments on cryptography: 10.2.6 If a cryptographic key is found to be compromised, the FI should revoke and replace the key and all other keys

		encrypted by or derived from the exposed key. Suggest stating which keys need replacement and have all related or protected keys being also replaced or re-encrypted. For example it should not be applicable to session keys in past session negotiations or key transfers, e.g. TLS.
		Comments on cryptography: 10.2.8 When replacing or renewing a cryptographic key, the FI should generate the new key independently from the previous key. This control cannot be applicable to all keys, e.g. the Identity-based encryption of Voltage that requires deterministic key derivation. Suggest rewording.
		Comments on cryptography: 10.2.9 Cryptographic keys can be corrupted or lost. As such, the FI should maintain backups of cryptographic keys for recovery purposes and accord them a high level of protection Backup should not be required for all keys, e.g. easily replaceable ones like asymmetric signature keys can be generated in smartcards and never leave them.
		Comments on cryptography: Paragraph 10.2.4 – For clarity, we would like to suggest the following amendments in bold: “The FI should ensure the systems that store the cryptographic keys and authenticate for authenticating customer passwords and protecting customer transaction applications (e.g. message authentication code, HMAC, digital signatures) are hardened and tamper resistant, e.g. hardware security module”.

		Comments on cryptography: The bank is supportive of the MAS proposed TRM Guidelines on Cryptography.
		Comments on cryptography: <10.2.5> We would like to seek clarify from MAS as to whether the cryptographic key mentioned in this clause are symmetric/Shared keys? Is there any expectation to also ensure Asymmetric public keys should also be distributed via out of band or secure channel?
		Comments on cryptography: 10.2.9 We would like to remark that the word “lost” could be interpreted as “deleted” but also as “leaked” in the context of data loss or data theft. In the latter case, restoring backups for recovery purposes is not an appropriate risk response. We would like to propose that the word “lost” is replaced with “deleted” in order to minimize confusion with data loss or data theft.
		Comments on IT resilience: 1. Refer to 8.2.2 - We would like to suggest MAS to rephase this as "The FI’s disaster recovery plan and other related plans (eg.walkaround procedures etc) should include procedures to recover systems from various disaster scenarios….. 2. Refer to 8.2.3 - We would like to suggest MAS to rephase this as "During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management, and avoid taking untested recovery measures which are likely to carry higher operational risks. In exceptional situations where untested recovery measures needs to be used, the FI should ensure approprioate risk assessment or controls are in place and

		proper approval has to be obtained from senior management." 3. Refer to 8.5.1 - We would like MAS to provide some guidance or examples on the defintion of significant changes in the threat landscape.
		Comments on IT resilience: 8.1 Availability We propose the scope of this section be confined to Critical Systems as defined under MAS Notice 644.
		Comments on IT resilience: 8.1.1 - Should FI include all systems or critical system only in system redundancy implementation / fault tolerant solutions? Propose this be risked based. 8.2.3 - Seek clarification to understand "untested recovery measures". 8.3.2 - Ref "criteria for measuring the success of the test" There is currently no industry-wide methodology to measure the success of an RPO. Therefore, we would recommend that further guidance be issued on this in consultation with FIs. 8.3.3 - Seek clarification for "partial shutdown or incapacitation" Is the definition consistent among all FI's. For example, partial shutdown could include HA cluster fail testing within the same data center or partial loss of a data center requiring failover to another data center. 8.3.4 - Seek definition for "extended period" Is a few hours or one day acceptable? 8.5.1 - Must the TVRA be done by an independent entity or can it be done in-house? 8.5.6a - Propose replacing "immediately" with "promptly" 8.5.6d - "Recorded, monitored, and supervised are somewhat redundant terms". Propose rewording to "Access to equipment racks should be adequately controlled and have adequate surveillance in place."
		Comments on IT resilience:

		8.1.2 We would like to seek guidance on the review scope and clarification if a review is required if a single point of failure assessment was built into a validation step in the initiation process.
		Comments on IT resilience: 8.1.2 [page 31] The Bank would like to understand if this is a one-time review or the review has to be conducted on a regular basis. 8.1.4 [page 31] The Bank would like to understand if this is a one-time testing or the testing has to be conducted on a regular basis. 8.2.2 [page 32] The Bank would like further clarity on the types of "disaster scenarios" to be included in the FI's disaster recovery plan. 8.3.1 [page 32] The Bank would like to understand MAS' expectation on the frequency of "regular testing". 8.3.2 [page 32] The Bank would like further clarity on the following: 1. What is the definition of "test scripts"? 2. Should the test script be from IT or business? 3. Does the Disaster Recovery checklist qualify as a test script? 8.3.4 [page 32] The Bank would like further clarity on the following: 4. What is the definition of "extended period"? 5. What is the scope of this clause? Is it sufficient if the Bank operates from its recovery site for selected systems for an extended period? 8.4.3 [page 33] The Bank would like to understand if a periodic read test is sufficient to address this requirement.

		8.5.2 (a) [page 34] The Bank would like further clarity on what is meant by external service provider.
		Comments on IT resilience: 8.1.2 The frequency of the holistic review of the bank's system and network architectures to identify any potential single point of failure, should be included for clarity.
		Comments on IT resilience: 8.1.4 The Bank requests clarity on whether thresholds are similar to the triggers in the proposed Revised Business Continuity Management Guidelines Consultation Paper.
		Comments on IT resilience: 8.2.1 We would like to clarify MAS' forward expectation on the IT DR requirements/criteria/testing framework whether there is an expectation on front to back IT DR testing covering applications across multiple data centres. We would prefer to have the option to conduct application testing by per data center applications. In additional further guidance on the definition of 'large scale' disruption. There could be several plausible scenarios of large scale disruption, and would FIs be expected to do a scenario analysis for some of them or all of them?
		Comments on IT resilience: 8.2.1 As this is covered under the proposed revised MAS Business Continuity Management Guidelines Consultation Paper, we suggest MAS' consideration not to duplicate similar requirements in this MAS TRM Guidelines.
		Comments on IT resilience: 8.2.3 Does this section refer to the risk of "untested

		recovery plans”? If so, such risk is already covered in Section 8.3 “Testing of Disaster Recovery Plan”.
		Comments on IT resilience: 8.3.4 The Bank suggest that the words "load-balancing and high availability" replaced with "architecture with high availability”. The regulator should allow the FI to define the extended period to operate from its recovery site. Does “operate” refer to disaster recover testing or business as usual?
		Comments on IT resilience: 8.3.4 The statement refers to the FI, which may indicate that the entire organization should perform an extended test. This would require all applications configured with high-availability and/or load balancing be expected to participate in an extended failover DR test which is not always practical, as high-availability and/or load balancing configuration is not always related to application criticality. We would propose that this citation be targeted at critical systems and propose the revision to “Critical systems should operate from its recovery site for an extended period as part of disaster recovery testing to gain the assurance and confidence that its recovery site is able to support business needs.”
		Comments on IT resilience: 8.3.4 We propose the scope of the role-swap DR test in this section be confined to Critical Systems as defined under MAS Notice 644 as a minimum requirement. The frequency of the test coverage should commensurate with the risk and criticality of the system.
		Comments on IT resilience: 8.3.5 MAS proposed that where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and verified to meet its business

		needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems.
		Comments on IT resilience: 8.4.3 We propose the periodic validation of backup restoration procedures in this section be confined to Critical Systems as defined under MAS Notice 644 as a minimum requirement, and the frequency of the validations should commensurate with the risk and criticality of the systems.
		Comments on IT resilience: 8.4.4 We note that encryption conceptually acts as an access control mechanism, since it has the purpose of ensuring that unauthorized individuals cannot compromise the confidentiality of data through read operations. To allow FIs to select the strongest security model to protect backup media, we would like to propose that "(e.g. encrypted)" is augmented to read "(e.g. encrypted and/or subjected to strict physical access control)". This is made possible by the requirement that backup media is stored at an offsite location, covered by the next sentence in the same paragraph. Encryption inevitably raises the question on how and where to manage the encryption key, a key management challenge that may affect the strength of the security model, depending on the context.
		Comments on IT resilience: 8.5.1 Additional guidance on the frequency that TVRAs should be performed would be helpful as this appears to be unclear and subjective otherwise.
		Comments on IT resilience: 8.5.1 …..The FIs should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify

		potential vulnerabilities and weaknesses…. Comments: As FIs increasing relied on cloud environments that are hosted externally, we seek clarification on MAS' expectations on whether the TVRA is still required for external cloud service providers/third party data centre facility providers. Based on the revised requirement, it seems to suggest that TVRA is required only for FIs' own data centres.
		Comments on IT resilience: 8.5.1 Is there an expected frequency for the TVRA to be conducted? We would like to propose not more frequent than every 2 years.
		Comments on IT resilience: 8.5.4 It would be helpful if there was additional guidance provided in terms of minimum standards e.g. distance between primary and DR DCs, other mitigating factors such as use of alternative telecommunications and power suppliers etc.
		Comments on IT resilience: 8.5.6 (a) 'Immediately' seems to be unreasonable given internal processes that the bank already adheres to meet other regulatory requirements where this control is performed within 24hrs.
		Comments on IT resilience: 8.5.6 (d) Please clarify on the expectation on supervision besides recording and monitoring with respect to access to equipment racks.

		Comments on IT resilience: Currently the bank's control function review do have standard clauses to recommend the Service Relationship Owner in managing the providers in this respect; however we would like to seek further guidance from MAS on commercial arrangement with the providers as this would be contingent of the T&C in contractual agreements.
		Comments on IT resilience: Para 8.3.4 of CP – Does this refer to the "Switch and Hold" test case? If so, how long is the minimal expectation to fulfill this requirement? Also, does this only apply to MAS Critical Systems?
		Comments on IT resilience: Paragraph 8.3.4 – We would like to seek confirmation that a 2-week period constitutes a sufficiently "extended period". We would also like to clarify if "recovery site" refers to the FI's disaster recovery site, as some of these sites are in the same location as the main production system in order to maintain high availability.
		Comments on IT resilience: The bank is supportive of the MAS proposed TRM Guidelines on IT Resilience.
		Comments on IT resilience: We noted the following requirement under paragraph 8.5.1: "The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment." We would like to clarify if a definition could be provided for "a significant change in the threat landscape or a material

		change in the DC's environment".
		Comments on operational infrastructure security: We refer to Paragraph 11.4 and would like to feedback that virtualisation should be secure, and not to separate data on different virtualisation cluster.
		Comments on operational infrastructure security: 11.5: Internet of Things As IOT covers many equipment and given that IOT standards may not have reached a level of maturity, we propose for the banking industry to work on a set of industry guidelines first before including these into the MAS TRM Guidelines.
		Comments on operational infrastructure security: We refer to Paragraph 11.5 and would like to feedback that in cases where the IoT device is managed by a third party, certain controls cannot be managed by the FIs directly e.g. the administrator access.
		Comments on operational infrastructure security: 11.1 [page 40] The Bank suggests replacing "Data Security" with "Information Security". 11.1.2 [page 40] 1. The Bank suggests replacing "data" with "information": "The FI should implement appropriate measures to prevent and detect data information theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI's service providers using a risk based approach." 2. The Bank would like to understand if this is applicable to all service providers regardless of inherent risk.

		11.1.4 [page 40] 3. The Bank would like further clarity on the definition of "mediums". 4. The Bank suggests replacing “mediums” by “channels and devices”. Please see proposed revised version: "The FI should ensure only authorised mediums channels and devices are used to communicate, transfer, or store confidential information…" 11.1.7 [page 41] 5. The Bank would like to understand if this requirement will be applicable to vendors operating a multi-tenant environment (e.g., Office 365, AWS, etc.) 6. The Bank suggests replacing “data” by “information”. Please see proposed revised version: "The FI should ensure confidential data information is irrevocably removed from IT systems and endpoints before they are disposed of." 11.2 [page 41] The Bank would like to understand if there are any mandatory controls such as multi-tier firewall or WAF. 11.2.7 [page 41] The Bank would like to understand if MAS’ expectation is on browser virtualisation (internet isolation) and/or internet separation? 11.3.6 [page 42] The Bank suggests rephrasing “should be” to “could be": “Security measures, such as application white-listing, should could be implemented to ensure only authorised software is allowed to be installed on the FI’s systems.”
		Comments on operational infrastructure security: 11.1.2 MAS proposed that FI should implement appropriate

		measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI's service providers. We would like to highlight that FIs cannot directly implement measures to prevent or detect events or breaches in information systems owned by their service providers. They can have governance and mechanisms in place to monitor and assess service providers' policies, controls and risk management practices. The guideline could be refined to reflect this more clearly.
		Comments on operational infrastructure security: 11.1.2 As there is an extension in coverage to third parties as per revised definition of "outsourcing arrangement" under the proposed revised MAS Outsourcing Guidelines Consultation Paper, we suggest MAS considers not duplicating similar requirements in this MAS TRM Guidelines.
		Comments on operational infrastructure security: 11.1.2 The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. Comments: We request minor edits suggested below for better clarity: "11.1.2 The FI should implement appropriate measures to deter and detect data theft and unauthorized modification in systems and endpoint devices."
		Comments on operational infrastructure security: 11.1.3 Databases, systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in databases, systems and endpoint devices should be encrypted and protected by strong access controls. Comments:

		Database-level encryption is a recognized technical constraint. As such, we would like to propose the term 'safeguarded' instead of encryption instead. Please see suggested minor edits below. 11.1.3 As such, confidential data stored in databases, systems and endpoint devices, should be safeguarded and protected by strong access controls.
		Comments on operational infrastructure security: 11.1.4 The FI should ensure only authorised mediums are used to communicate, transfer, or store confidential data. Comments: To add clarity to the requirement, we propose to replace "medium" with "delivery channels and storage" for this requirement.
		Comments on operational infrastructure security: 11.1.7 The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of. Comments: Confidential data should be purged prior to asset destruction as well as prior to asset transfer/re-assignment. As such, we propose the following suggested edits to provide a more comprehensive approach in handling confidential data: "11.1.7 The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of or redeployed for other use."
		Comments on operational infrastructure security: 11.2.7 "…the FI should perform a risk assessment and implement Internet surfing separation by isolating systems …. from the Internet and other systems connected to the Internet. Comments:

		We agreed with MAS that systems with internet access are at higher risk to cyber threats and a risk assessment should be performed with remediation plans put in place to mitigate the risks. As internet surfing separation is one of the possible remediation approach/solution, we would like to request for MAS to allow the FIs to assess and determine the most appropriate and holistic approach/solution (e.g. browser and email isolation, content threat removal, micro-VMs, AI/ML, etc) to safeguard online services from cyber threats. As such, we would like to propose the following suggested edits: "11.2.7..the FI should perform a risk assessment to ensure such systems are adequately ringfenced and segregated to mitigate likelihood of exploitation from Internet."
		Comments on operational infrastructure security: 11.3.2 The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner. Comments: Deviation from standard does not necessarily constitute a risk. It is a non-conformity. Suggested edits below. 11.3.2 The FI should establish a process to verify that standards are applied uniformly on systems and to identify deviations from the standards. Non-conformities arising from deviations should be addressed in a timely manner.'
		Comments on operational infrastructure security: 11.3.4 The FI should ensure anti-malware signatures are kept up-to-date and the systems are regularly scanned for malicious files or activities. Comments: We request minor edits suggested below for better clarity: "The FI should ensure anti-malware signatures .. and systems are regularly scanned for malicious files and anomalous activities."
		Comments on operational infrastructure security:

		11.5.1 Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which are connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, the networks which they are connected to and their physical locations. Comments: The Bank respectfully propose to remove Section 11.5 as IoT is a technological trend. IoT can be treated similarly as untrusted devices, e.g. customer-owned devices, kiosks and BYOD, and there should be no need to prescribe additional controls against IoT devices.
		Comments on operational infrastructure security: 11.5.2 The FI should assess and implement processes and controls to mitigate risks arising from IoT…. Comments: When performing risk assessment of IoT, we would like to recommend the need to also consider whether the IoT is persistently connected to the FI's network or the Internet. This will allow the FIs to better assess and implement processes and controls that commensurate with the risk arising from IoT.
		Comments on operational infrastructure security: 11.1 Data Security • The minor edit is suggested as there could be systemic and procedural restrictions on implementing firm tools in the endpoints or appliances provided/managed by service providers. Suggested wordings below. 11.1.2 The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI's service providers, where feasible.
		Comments on operational infrastructure security: Suggest to bring this back to the principle level that data

		should be protected without specifying specific controls. Suggested wordings below. 11.1.4 The FI hould ensure only authorised mediums are used to communicate, transfer, or store confidential data and it is protected in an appropriate way.
		Comments on operational infrastructure security: 11.2 Network Security • Suggest for the guideline to be less-prescriptive; instead of recommendating to isolate system and data from the internet. Suggested wordings below. 11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems or have strong controls in place that effectively reduce the risk of cyber threats from the internet.
		Comments on operational infrastructure security: 11.3 System Security • The guideline recommended real-time scanning of IOCS, which is resource intensitive. Suggest to revise the guideline to be less prescriptive i.e "... the FI should implement detection and response mechanisms to perform near real-time scanning of indicators of compromise (IOCs),". Suggested wordings below. 11.3.5 To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform near real-time scanning of indicators of compromise (IOCs), and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.
		Comments on operational infrastructure security: The guideline recommended "application white-listing ...", this may not be a viable approach for all FI due to the large and complex environment many FI operates on. Similar control objectives can be achieve via alternative security measures. Suggested wordings below.

		11.3.6 Security measures should be implemented to ensure only the FI 's authorised software is allowed to be installed on the FI's systems.
		Comments on operational infrastructure security: 11.5 Internet of Things • The guideline should provide clarity on the scope of IoT i.e BYOD IoT should not be in scope and its applicability. Suggested wordings below. 11.5.1 Internet of Things (IoT) includes any FI-owned electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which are connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all FI-owned IoT devices, the networks which they are connected to and their physical locations where feasible.
		Comments on operational infrastructure security: Minor revision in wordings to provide more clarity. Suggested wordings below. 11.5.2 Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with the business process/function and criticality of the data that is transmitted, collected, stored and processed by the IoT devices.
		Comments on operational infrastructure security: The guideline should acknowledge that not all devices may allow for administrator access configuration. propose revision to the guideline. Suggested wordings below. 11.5.4 The FI should manage the administrator access to the IoT devices where feasible to minimise the risk of unauthorised access. Where access control is not provided by the IoT device, the FI may select an alternative control,

		such as restricting traffic as outlined in 11.5.3. • The guideline should acknowledge that flexibility in logging is needed. Suggested wordings below. 11.5.5 The FI should log and monitor the system activities of IoT devices.
		Comments on operational infrastructure security: The guideline should acknowledge that flexibility in logging is needed. Suggested wordings below. 11.5.5 The FI should log and monitor the system activities of IoT devices.
		Comments on operational infrastructure security: Paragraph 11.1.2 – We would like to suggest the following additions in bold: "The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include the FI's systems and endpoint devices which are managed by the FI's service providers." This avoids the potential misinterpretation that the FI is to implement the measures on the service providers own systems and endpoints.
		Comments on operational infrastructure security: Paragraph 11.5.1 – We would like to clarify that if the definition of IoT refers to (i) devices connected to the FI's network OR internet, or (ii) devices connected to the FI's network AND Internet. We propose that the latter definition is more appropriate, as it addresses the risk of entry points into the FI network being created by IoT devices.
		Comments on operational infrastructure security: Paragraph 11.5.3 – We ask that MAS reconsider this requirement, as strong authentication (e.g. 2FA/MFA) may not be a viable option for IoT devices as most of them offer limited administrator capabilities.

		Comments on operational infrastructure security: <11.1.3> We would like to request for MAS to allow FIs the flexibility on the requirement of encryption of data for database and system to be based on classification of data.
		Comments on operational infrastructure security: 11.1.3 Databases, systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in databases, systems and endpoint devices should be encrypted and protected by strong access controls. It would be useful to have clarity on the data types (within the broader realm of confidential information), where encryption is expected. Or, does the guideline expect all data labeled as 'confidential' to be encrypted at all points of storage?
		Comments on operational infrastructure security: 11.1.3 The words "Confidential Data" needs to be defined as each FIs operates based on its own different definition. Encryption of Confidential Data may be expensive, the Bank suggest that the FIs be allowed to use a risk based approach to determine the usage of encryption. FIs ought to be given flexibility to implement encryption by layers based on appropriateness (e.g. physical disk layer, secure session) at rest and in motion.
		Comments on operational infrastructure security: 11.1.3 Databases and systems are secured within the data centre, so encrypting confidential data does not necessary reduce the risk, and it is always operationally challenging to encrypt all the data. Whilst encryption of data-in-transit and data-at-rest is reasonable. Does MAS also expect data-at-use to be encrypted?

		Comments on operational infrastructure security: 11.1.3 We note that databases, systems and endpoint devices have different data exfiltration threat profiles due to contextual differences in use and physical location. We would like to recommend to rephrase the second sentence of paragraph 11.1.3 to "Based on a comprehensive threat assessment, FIs should determine a robust set of mechanisms to protect confidential data stored in databases, systems and endpoint devices from being read or exfiltrated in an unauthorized manner, and may include, but not limited to, mechanisms such as strong access control, encryption, monitoring, and physical protection." 11.1.3 / 11.1.4 We note that a concise definition of "strong access controls" is required. We would like to suggest to expand MAS' definition of "strong access controls" to protect information from unauthorized disclosure under chapter 9.
		Comments on operational infrastructure security: 11.1.3 / 11.1.4 We note that a concise definition of "strong access controls" is required. We would like to suggest to expand MAS' definition of "strong access controls" to protect information from unauthorized disclosure under chapter 9.
		Comments on operational infrastructure security: 11.1.5 We appreciate that MAS seeks to instruct FIs to mitigate the risks related to users communicating and storing confidential data using unauthorized internet services. Our vision is that any effective data leakage protection strategy is built on a combination of user awareness and technology, aligned with the secure design principle of defense in depth. We note that a purely technological

		approach to data loss prevention is unlikely to be effective, given the observation that not every endpoint on the entire Internet can continuously be inspected and classified in a fine-grained manner. Additionally, we note that paragraph 11.1.5 does not explicitly define who shall authorize internet services, and for what purpose(s). We would like to recommend to rephrase paragraph 11.1.5 as “The FI should conduct a comprehensive assessment of data leakage threats in the context of Internet services, such as social media sites, cloud-based internet storage sites, and web-based e-mail services. Based on the resulting threat profile, the FI shall define and continuously maintain the authorized business purposes for the use of Internet services, and shall define an appropriate and balanced mixture of preventive and detective user awareness and technological measures.”
		Comments on operational infrastructure security: General comment: Any device connected to an FI's network must adhere to acceptable Network Security Standards. IoT brings into scope a large variety and number of devices and FI's should be aware of that . However, consider removing this section, as it is essentially covered throughout the other sections of this document. Would an employee’s own personal device that connects to corporate Wifi be considered an IoT device and subject to monitoring? 11.1.3 - Confidential data stored in Company managed infrastructure will be governed by authorized user access, and hence encryption of such data should not be mandated. Requiring encryption of data on non-Company managed infrastructure is a reasonable requirement. 11.2.2 "To minimise the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network, the FI should deploy firewalls, or other similar measures, within internal networks to protect information assets within the FI’s internal networks. Information assets could be grouped into network segments based on the criticality of the business that they support, their functional role (e.g.

		databases and applications) or the sensitivity of the information. " Ø Comment: Suggest replacing “segregate information assets” with “protect information assets” 11.2.7: Suggest using the wording from recommendation #13 of the “Report of the COI into the Cyber Attack on SingHealth”: “[…] the FI should perform a risk assessment taking into account the benefits and drawbacks of Internet surfing separation and Internet isolation technology, and put in place mitigating controls to address the residual risks.” 11.5.1 - a) Are BYOD devices considered IOT and are the FI's required to maintain an inventory of all BYOD's that end users may use? Access control can be accomplished by various methods. b) Propose that multifunction printers may not be IOT if they are only connnected to the internal networks; however, they should have adequate security, patching, and updates. 11.5.3: Comment: this paragraph is very+C15 prescriptive, not taking into account that some devices can be less or more secure than others.
		Comments on operational infrastructure security: 11.1.4 Kindly define or provide examples of “authorized mediums”.
		Comments on operational infrastructure security: 11.1.5 It may not be possible to “prevent and detect” use of unauthorized internet services if connections are not made via hardened devices owned by FI. We propose to retain the current MAS TRM Guidelines paragraph 9.1.4 where we govern via bank’s policy.
		Comments on operational infrastructure security: Proposed amendment to paragraph 11.1.5 of the

		Consultation Paper Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data such as social media sites, unapproved cloud-based internet storage sites and unauthorised web-based emails. Justification: As public cloud offerings in the Unified Communications & Collaboration space continue to mature, many in the financial services industry see this as an opportunity to deploy collaborative tools (MS Office 365 and One Drive, Gmail and Google Apps etc) to their non-regulated users. Proposed amendment to paragraph 11.2.7 of the Consultation Paper Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating logically segregating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet. Justification: Many in the financial services industry are adopting the network-zoning concept as a way of logically segregating critical business and system functions. Clarification on paragraph 11.5.1 of the Consultation Paper We note at paragraph 11.5.1 of the Consultation Paper that IoT includes smart phones that are connected to the FI's network or the Internet, and the FI should maintain an inventory of all its IoT devices. We would like to clarify whether IoT would include BYODs, and accordingly, BYODs should be maintained as part of the inventory.
		Comments on operational infrastructure security: 11.1.6 We would suggest a slight reword to: "The use of sensitive production data in non-production environment should be prohibited where controls are less stringent than in the production environment. In exceptional situations where production data needs to be used, proper approval has to be obtained from senior management. The FI should ensure appropriate controls are implemented in non-production environment to manage the access and removal

		of the data to prevent leakage of confidential data. Where possible, confidential data used in non-production environment should be masked"
		Comments on operational infrastructure security: 11.1.6 We would like to suggest clarity to exclude pseudo-production environment from the definition of “non-production environment”. These pseudo-production environments are controlled equivalent to production environments. We use such environments typically for pre-production “mock run” testing for data conversion, data migration or full regulatory reporting, which would require production data to be included for verifications.
		Comments on operational infrastructure security: 11.2.7 Clarify the meaning of “systems with internet access”? Does it refer to Internet Facing Applications?
		Comments on operational infrastructure security: 11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet. We want to highlight that it may not be feasible for FIs to isolate systems completely from the internet. Can this requirement be looked at and clarified further?
		Comments on operational infrastructure security: Para 11.2.7 of CP – we would like to clarify whether the requirements under this paragraph applies to end user computers and devices (with Internet surfing capabilities) which have a direct access to MAS Critical systems? Would this be similar to network segregation/isolation for SWIFT

		CSP 1.1 Mandatory Control Requirement “SWIFT Environment Protection”?
		Comments on operational infrastructure security: We refer to Paragraph 11.2.7 of the Consultation Paper on TRM Guideline on internet surfing separation and would like to request MAS to elaborate on the acceptable separation strategy (e.g. is physical or logical separation considered sufficient for such isolation?)
		Comments on operational infrastructure security: We refer to Paragraph 11.3.7 and would like to request MAS to provide guidance on implementing BYOD measures based on different access level of BYOD e.g. Email/contact access vs full access to Bank’s network.
		Comments on operational infrastructure security: • With respect to para 11.3.2 , while we agree that deviation from the standards should be assessed to determine the appropriate corrective action to be taken, we are of the view that in some instances such deviation does not constitute/give rise to risk.
		Comments on operational infrastructure security: With respect to para 11.3.6, we will like to suggest that the paragraph be reworded as "Depending on the risk identified during the assessment, appropriate security measures such as application white-listing (as necessary), should be implemented to ensure only authorised software is allowed to be installed on the FI’s systems."
		Comments on operational infrastructure security: With respect to para 11.5, we are of the view that Internet of Things (IoT) does not encompass just any device connected to a Network. To be considered part of Internet of Things a device needs 1) to be connected to the Internet and 2) to be subject to significant functioning capabilities changes to be applied via an Internet connection. In this

		regards, we would suggest that IoT devices be limited to FI owned devices which are connected to the Internet and employee-owned smart phones should not be considered IoT and BYOD controls will be sufficient.
		Comments on operational infrastructure security: With respect to para 11.1.3 , with advances in technology, the protection of confidential data at rest may be achieved through a combination of other controls instead of encryption of data at rest. Suggest that the statement be edited to '...confidential data stored in databases, systems and endpoint devices should be protected by robust controls such as encryption of data and strong access controls.'
		Comments on operational infrastructure security: With respect to para 11.2.3, we will appreciate if MAS can clarify its expectation on the frequency of review.
		Comments on operational infrastructure security: With respect to para 11.3.5 , we will appreciate if MAS clarify its expectations on 'real time scanning of IOCs'. Scanning of IOCs can be carried out through multiples routes, which not may meet a strict definition of 'real time' (immediately upon infection/compromise). Suggest that the statement be edited to '...the FI should implement detection and response mechanisms to detect indicators of compromise (IOCs) in a timely manner, and proactively monitor systems...'
		Comments on operational infrastructure security: With respect to para 11.3.5 , we will appreciate if MAS clarify its expectations on 'real time scanning of IOCs'. Scanning of IOCs can be carried out through multiples routes, which not may meet a strict definition of 'real time' (immediately upon infection/compromise). Suggest that the statement be edited to '...the FI should implement detection and response mechanisms to detect indicators of

		compromise (IOCs) in a timely manner, and proactively monitor systems...'
		Comments on operational infrastructure security: 11.3.5 In order to perform real-time scanning of IOCs, IOCs must be provided first rather than through discovery. Hence, we would like to suggest that this be amended appropriately. In addition, we would like to propose that proactively system monitoring be confined to MAS Notice 644 list of critical systems and systems with sensitive data only.
		Comments on operational infrastructure security: 11.3.6 The Bank suggests that it be given flexibility to adopt "alternate security measures" as opposed to "white-listing".
		Comments on operational infrastructure security: 11.3.7 BYOD is often a misunderstood term even though the guideline has provided a very clear definition. Most people will just assume it is privately owned devices without considering what they are used for and the environment that they are accessing. The recommendation is to change the term "BYOD" to "remote computing". The reason is that it should not matter whether it is a bank owned device or a staff owned device. What is important is that adequate security controls must be in place prior to allowing devices to access the corporate network remotely.
		Comments on operational infrastructure security: With reference to 11.5.1, it is not be possible to keep constant track of the physical location of mobile devices as part of the inventory maintenance. Please advise.
		Comments on operational infrastructure security: With regard to para 11.5.1, we would like seek clarifications about the inventory and what it should include. Specifically we would like to understand if it is intended to capture

		BYOD. If so, we would like to suggest that BYOD is excluded as there will be privacy concerns. In any case, all BYODs will be registered with the bank.
		Comments on operational infrastructure security: 11.5.5 The FI should log and monitor the system activities of IT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours. Recommend removing "system" from "system activities" as this could be read as too prescriptive. Some IT devices may not permit the FI to monitor their internal processing; an alternative could be to monitor the behaviour of the device on the network.
		Comments on operational infrastructure security: The bank is supportive of the MAS proposed TRM Guidelines on Operational Infrastructure Security.
		Comments on IT project management and security-by-design: Point 5.3.2 System Acquisition The FI should ensure the vendor puts in place robust software development and quality assurance practices, as well as stringent security practices to safeguard and protect any sensitive data the vendor has access to over the course of the project. Similarly, any vendor access to the FI's systems should be tightly controlled and monitored. Question: Can self-disclosures from the service provider in the nature of integrity statements qualify as compliance to this guideline.

		Comments on IT project management and security-by-design: <5.1.2> Requiring detailed IT project plans for all IT projects would be operationally cumbersome as IT projects vary in scope, scale and nature. Hence, we respectfully request MAS to allow FIs the flexibility to adopt a risk-based approach, by depending it on the scope, scale and nature of the IT project. <5.7.3> Having to set up three separate environment is operationally costly for FIs to maintain. Hence, we would like to propose MAS to determine the number of environments required, as long as the appropriate controls to ensure source pack is secured and tested during each stage of the development cycle with restricted access on a need-to basis.
		Comments on IT project management and security-by-design: 5.1 FIs ought to be given flexibility to maintain project artifacts at program level as appropriate.
		Comments on IT project management and security-by-design: 5.1.1 The project management framework should recognize that difference practices are required for different project circumstance as such, more formality is required for the more important/strategic projects and vice versa.
		Comments on IT project management and security-by-design: 5.1.2/5.4.1 Projects using the “agile” approach would not have detailed project plans with specific project phases. All delivery work will be produced iteratively through a single ‘execution’ phase.

		Comments on IT project management and security-by-design: 5.1.3 Some key documents listed e.g. feasibility analysis, are not required for in all circumstances. Some documents are evolving e.g. project and implementation plans are sometimes moving targets. It is not necessary to have every version approved. These documents do not always require formal version control or configuration management. The Bank suggests that documents be restricted to only key documentation which could be quoted as examples. In general, the Bank would like to have the flexibility to maintain project artefacts at program level as appropriate.
		Comments on IT project management and security-by-design: 5.1.4 As project risks, such as an ill-defined project scope and poor cost management, can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle. For large and complex projects that impact the business, the FI should report significant project risks to its board of directors and senior management. Comments: To allow the FIs' Board of directors and senior management to have better oversight on key IT decisions, we propose MAS to include in section 5.2 the responsibility of the project steering committee to report significant project risks and key decisions to the Board of directors and senior management. Please see suggested edits below: "5.1.4.. For large and complex projects that impact the business, the project steering committee should report significant project risks and key decisions to its FI's board of directors and senior management." ***

		5.5.2 In establishing the security requirements, the FI should assess the potential threats and risks related to the system, and determine the level of security required to meet its business needs. Comments: We request minor edits suggested below for better clarity: "5.5.2 In establishing the security requirements, the FI should assess the potential threats and risks related to the system, and determine acceptable level of security required to meet its business needs."
		Comments on IT project management and security-by-design: 5.1.4 The reporting of project risks should be to senior management and not to Board. This should be consistent with paragraph 3.1.5 which sets out the differences in responsibilities between the Board and senior management.
		Comments on IT project management and security-by-design: 5.3.2 The Bank would like seek MAS' clarification that FI can rely on independent assessment report, e.g. ISAE, on the vendor's software development and quality assurance practices. Can this be included in the paragraph for clarity?
		Comments on IT project management and security-by-design: 5.3.4 - Clarification is required for type source code escrow agreement, especially for propriety software from vendor verses software that an FI purchases for use in-house

		5.8.2 - Clarification required on the definition of 'independent Quality assurance function'.
		Comments on IT project management and security-by-design: 5.3.4 Can current acquired software with no escrow agreements in place be grand-fathered till a time when these vendors be replaced or a new agreement be re-negotiated?
		Comments on IT project management and security-by-design: 5.3.4 For commercialized off-the-shelf software from large software vendors such as IBM or Microsoft the software licensing terms and conditions are standardized for the market, is the FI required to have escrow agreement for such acquired software?
		Comments on IT project management and security-by-design: 5.4.1 The wordings maybe too prescriptive for organisations that practices different development methodologies. The Bank suggests to reword to "the framework should outline the processes and standards in line with the respective development methodology".
		Comments on IT project management and security-by-design: 5.4.3 The wording seems too prescriptive. The Bank suggests to re-word to “where relevant, the IT security function should be involved as part of the SDLC framework”
		Comments on IT project management and security-by-design: 5.5.1 Functional requirements may be collapsed under broader user stories/epics in “agile” development methodologies. The Bank suggests to change "functional

		requirements" to "user requirements" so that it applies to all developmental methodologies.
		Comments on IT project management and security-by-design: 5.6.2 There appears to be a typo in the provision; “The FI should use track and verify that requirements are met”. We welcome clarification if this is not the case.
		Comments on IT project management and security-by-design: 5.6.2 [page 20] The Bank suggests the removal of the word "use": "The FI should use track and verify that system requirements are met by the current system design and implementation…" 5.7.3 [page 21] The Bank would like to highlight that in view of User Centric Agile Testing, it is typical for testing to be conducted in a single common environment.
		Comments on IT project management and security-by-design: 5.7.1 We recognize the value of test strategies and methodologies to ensure that (IT) changes are controlled in an appropriate manner. In contemporary (IT) environments based on continuous integration and continuous delivery (CI/CD), we observe an increasing adoption of automation paired with an increase in release frequency. This trend redefines the purpose and positioning of test plans by shifting quality assurance from an individual test execution basis to the overall testing methodology, and as such the

		value of approvals on individual test plans gradually diminishes. Presumably, the intention behind seeking such approvals is ensuring quality assurance of testing and acceptance by relevant stakeholders, which can be organized on the overarching methodology level as an alternative. Therefore, we would like to propose that paragraph 5.7.1 is rewritten as follows: “A methodology for system testing should be established and approved by relevant stakeholders. The scope of tests should cover business logic, system function, security controls and system performance under various load and stress conditions.”
		Comments on IT project management and security-by-design: 5.8.2 As this section is based on security-by-design we would propose clarifying this provision to focus on security related policies, procedures and standards. The meeting of project objectives goes beyond this requirement and should be dropped from this section.
		Comments on IT project management and security-by-design: 5.8.2 Regarding the performance of quality assurance by an independent quality assurance (QA) function, we would like to seek clarification if the independence is met with the team performing the QA to be separate from the development team, or must the QA function be reporting to other than the system development function head? We think it is more practical and effective for the quality control gates be managed throughout the SDLC by another team under the system development function head
		Comments on IT project management and security-by-design: Clarification on paragraph 5.3.4 of the Consultation Paper

		We note at paragraph 5.3.4 of the Consultation Paper that MAS expects a source code escrow agreement to be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. We would like to clarify whether MAS would provide a definition for "critical acquired software", or MAS would leave it to the industry to decide on the criticality of the acquired software.
		Comments on IT project management and security-by-design: Para 5.3.4 of CP states that a source code escrow agreement should be in place so that the FI can have access to the source code in the event that the vendor is unable to support the FI. Can we clarify whether such agreements are only required for MAS Critical Systems?
		Comments on IT project management and security-by-design: Paragraph 5.1.2 – The nature of Agile software development may make it unfeasible to develop highly detailed plans. Would a 'release plan' under the Agile model constitute a "Detailed IT project plan"? It would be useful to have further guidance on what constitutes such a plan in the Agile context (e.g. minimum deliverables/documentation needed). Paragraph 5.1.4 – It would be useful if MAS could provide further guidance on what constitutes "large and complex projects". Paragraphs 5.4.2, 5.62, 5.63 and 5.8.2 – Would MAS consider allowing the FI to take a risk-based approach and limit the application of the security-by-design principle to critical systems/applications or systems with a high risk exposure (e.g. internet or customer facing systems/applications)?

		Paragraph 5.4.3 – Would MAS consider allowing the FI to take a risk-based approach in deciding whether to involve the IT security function in each phase of the SDLC, with a view to meeting the FI's security objectives? Paragraph 5.7.4 – It would be useful if MAS could provide further guidance on the required standard/level of validation "that the system continues to function properly", given that regression testing can only give a reasonable assurance of proper function.
		Comments on IT project management and security-by-design: The bank is supportive of the MAS proposed TRM Guidelines on Project Management and Security-by-Design.
		Comments on IT project management and security-by-design: We refer to Paragraph 5.8.1 of the Consultation Paper on TRM Guideline on quality assessment matrics and would like to request MAS to provide some examples of such metrics which could be used for the independent quality assurance check.
		Comments on IT project management and security-by-design: With respect to para 5.3.4, • The feasibility of having a company providing its intellectual property to its customers is questionable. • Applicability of escrow agreement guideline across all critical software vendors requires further clarification as vendors like SAP, Oracle may not come to such an agreement. • Stability of the vendor, as well as criticality of the software should also be considered in the decisions to

		require a software escrow agreement. For example, many FIs rely on critical software from Microsoft, however it will not be a good use of time and resources to require software escrow agreement in this case.
		Comments on IT project management and security-by-design: With respect to para 5.3.4, • The feasibility of having a company providing its intellectual property to its customers is questionable. • Applicability of escrow agreement guideline across all critical software vendors requires further clarification as vendors like SAP, Oracle may not come to such an agreement. • Stability of the vendor, as well as criticality of the software should also be considered in the decisions to require a software escrow agreement. For example, many FIs rely on critical software from Microsoft, however it will not be a good use of time and resources to require software escrow agreement in this case.
		Comments on software application development and management: • With respect to para 6.3.1, for clarity, we will appreciate if MAS can provide detailed definition of DevOps. • With respect to para 6.5.3, we will suggest that MAS add a footnote with examples to further clarify the definition and aid understanding of 'Shadow IT'. In this regard, we will like to understand if MAS considers end user developed applications (e.g. excels, macros) to be part of Shadow IT?
		Comments on software application development and management: 6.1.1 Propose that the standards should be risk based. 6.4.3 - Is approved API access only required for third party governance or more generally - clarify? 6.4.8 - Clarity required on the requirement to perform Real-time monitoring of APIs. What kind of suspicious activities

		need to be monitored? is this required only for critical APIs or based on the classification of data that the API handles? 6.5.1 - What is the scope of impact and definition of application developed / acquired by end user that is required approval from business and IT management approval? Propose this be risk based for all end user management guidelines in this section.
		Comments on software application development and management: 6.1.1 The Bank suggests to include the risk of "insider" threats, i.e. the Bank suggest to add the following words underlined to "Software bugs or vulnerabilities are typically targeted and exploited by hackers or insiders to compromise an IT system."
		Comments on software application development and management: 6.1.3 MAS proposed that FI should ensure its software developers are trained to apply the standards when developing software. We would be grateful for clarification on what standards are being referred to, for example secure coding, source code review and app testing only?
		Comments on software application development and management: 6.1.4 MAS proposed that FI should use a mixture of static, dynamic and interactive application security testing methods to validate the security of the software application. Where applicable, the FI should include fuzzing or fuzz testing11 as part of its dynamic or interactive application security testing. We would be grateful for definition of "mixture" and "where applicable" in that whether FIs can choose not to use some testing methods
		Comments on software application development and management:

		6.1.4 We appreciate that MAS seeks to further clarify and specify its expectations on application security testing. We observe that this is a highly complex and dynamic area where commercial forces have a significant influence on perceived market best practices compared to other security areas. Our vision is that application security testing should not be a purely technology-driven practice but rather be based on a comprehensive security verification and testing strategy, which typically includes other activities and processes. Our concern is that a general mandate to use a mixture of SAST, DAST and IAST takes a too narrow and too specific approach to security verification and testing which will drive FIs to procure increasing amounts of commercial AST tools, while security verification and testing effectiveness is first and foremost predicated on the sensible and balanced application of security verification and testing activities and processes in order to assess the effectiveness of secure design, coding and implementation. Moreover, to the best of our knowledge, industry research conducted independently from commercial AST vendors has not yet demonstrated that there is a proven benefit to an implementation of SAST, DAST and IAST in comparison to other security verification and testing strategies as outlined above. In part, this is due to the fact that market adoption of IAST is still limited. In addition, for specific technology platforms and stacks, the overly specific focus on SAST, DAST and IAST eliminates any sound alternative strategy that may have at least an equal, if not superior, capability to assess the effectiveness of secure design, coding and implementation. Finally, application security verification and testing can be reasonably expected to evolve in the nearby future under industry forces such as increased automation, artificial intelligence and machine learning – any specific focus will not remain sound for a long time. Therefore, we would like to propose that FIs are required to

		set up comprehensive security verification and testing strategies in which security verification and testing activities are tailored to the nature and composition of technology platforms and stacks in use, with the ultimate goal of preventing of vulnerabilities, weaknesses, implementation bugs and design flaws from existing in software through the assessment of the effectiveness of secure design, coding and implementation. As part of setting up such a comprehensive strategy, careful consideration should be applied as to why, when, where, who and how what security verification and testing activities shall take place, which can be broader than SAST, DAST and IAST. We note that in the area of application security testing, contemporary tooling is almost exclusively commercial-off-the-shelf. In practice, these tools already perform fuzz testing to the extent required out of the box, limiting any possibility of an FI to "include" such methodologies "as part of DAST or IAST". As such, we conclude that there is limited value in the last sentence. We would like to propose to omit the last sentence. 6.1.5 The first sentence seems to be a duplicate of 6.1.4, albeit with different terminology. We strongly agree with the need to ensure that software scanning rules are kept current. Therefore, we would like to suggest that the last sentence of paragraph 6.1.5 is appended to paragraph 6.1.4, and that paragraph 6.1.5 is wholly removed. 6.1.6 We are generally supportive of MAS' intention to track and remediate issues and software defects. However, we feel that the wording "remediated before production deployment" imposes an unduly onerous standard of

		process adherence that insufficiently appreciates or takes into account business risk appetite. Certain application security verification and testing activities, especially those where source code or system configuration is an input, may reveal a sizable number of issues and software defects of various severity, ranging from informational to low severity to critical severity, and we observe that not all uncovered issues necessarily exceed business risk appetite and/or require the same urgency of remediation. Instead of the aforementioned wording, we would like to suggest that the Technology Risk Management Guidelines mandate the FI to establish clear criteria to promote releases to production (release management), tailored to the security verification and testing strategy, and separately define a strategy to manage and reduce technical debt incurred by issues and software defects that are within business risk appetite thresholds. We would like to highlight that Agile software development, based on an iterative and incremental development model, may serve as an effective enabler for such a strategy, especially when paired with intensified automation and actionable software security metrics such as mean time to repair (MTTR). 6.3.1 We would like to highlight that enabling frequent, efficient and reliable releases of software products is not a goal of DevOps, but rather a goal of continuous integration and continuous delivery (CI/CD). In practice, DevOps and CI/CD are often paired together because both are enablers of Agile software development. We would like to refer to the following page that explains the difference in more detail: https://www.synopsys.com/blogs/software-security/agile-cicd-devops-glossary/. 6.3.2 We fully appreciate that MAS highlights to the industry that Agile software development and DevOps requires FIs to continue to incorporate necessary security practices to

		ensure the security of the application is not compromised. To add, we fully agree that a certain degree of segregation of duties remains required. However, we note that with increased adoption of automation, specifically automation of security verification and testing, the focus of such segregation of duties shifts to mitigating internal fraud risk through the deterrence of introducing malicious logic in production environments, as this is a notoriously difficult to mitigate risk area in an automated way. We would like to suggest that "the respective DevOps activities" is further defined and specified in terms of internal fraud risk, e.g. by requiring manual code review focused on malicious code before promotion to production as a means to implement segregation of duties, in order to enable FIs to further embrace CD/CI principles to accelerate software development and delivery. Moreover, we feel that "segregation of duties for the development, testing and operations functions in its DevOps processes" imposes a general standard of practice that draws required attention and focus away from sensitive operations such as promoting releases to production environments. In our view, segregation of duties should restrict itself to promotion of artefacts from non-production to production environments, as also stated in paragraph 7.6.2. Adherence to the principle of separation of environments (as defined in paragraph 5.7.3) has the side effect that promotion of artefacts from a non-production environment to another non-production environment is not designated as a sensitive operation. 6.4 Aside from the observation that FIs develop open APIs, we note that APIs are also being developed for other purposes than providing developers with a public interface and/or facilitating integration with third parties. In order to maintain an unambiguous understanding of the business context as described in paragraph 6.4.1, we would like propose to replace "API" with "open API" throughout

		paragraph 6.4. 6.4.2 We would like to suggest to expand MAS' definition of "strong controls" to authorize and control access to designated API services in order to facilitate implementation, or, alternatively, to state that the FI should adopt a comprehensive and robust security approach around the usage of open API services. We would like to suggest to expand MAS' definition of "strong controls" to authorize and control access to designated API services in order to facilitate implementation, or, alternatively, to state that the FI should adopt a comprehensive and robust security approach around the usage of open API services. 6.5.3 We appreciate that MAS seeks to instruct FIs to monitor and detect the use of shadow IT in its environment. The sentence "end user should not be allowed to use shadow IT until they have been properly assessed and approved for use" appears to be a contradictio in terminis however, since shadow IT is by definition unwanted IT. We suggest to reword this as follows: "The use of shadow IT shall be treated as an incident and responded to accordingly."
		Comments on software application development and management: 6.1.4 We would like to suggest for MAS' consideration that given the fast evolution of technology, not to prescribe any specific technological solutions in the Guidelines, and to exclude the mention of fuzz or fuzz testing in this paragraph. Otherwise, an alternative would be to replace the word "should" to "may" for the use of fuzzing or fuzz

		testing, where applicable, as part of dynamic or interactive application security testing.
		Comments on software application development and management: 6.1.5 Automated static or dynamic software scanning should be implemented to detect security vulnerabilities or coding issues, and configurations that can impact the security of IT systems. The software scanning rules should be reviewed periodically and kept current. Comments: We request minor edits as suggested below for better clarity: "6.1.5 Automated static or dynamic software scanning should be implemented to detect security vulnerabilities or coding issues, and misconfigurations that can impact the security of IT systems. The software scanning rules should be reviewed periodically and kept current." *** 6.4.1 FIs collaborate with FinTech companies and develop open APIs, which are used by third parties to implement products and services for customers and the marketplace. Hence, it is important for the FI to establish adequate safeguards to manage the development and provision of APIs for secure delivery of such services. Comments: As FIs do also collaborate with other non FinTech companies or develop the APIs in-house, we propose MAS to also consider such partners/circumstances in this requirement and not just limit to FinTech companies.
		Comments on software application development and management:

		6.1.5 MAS proposed that automated static or dynamic software scanning should be implemented to detect security vulnerabilities or coding issues, and configurations that can impact the security of IT systems. The software scanning rules should be reviewed periodically and kept current. The bank suggests the following "...The software scanning rules or capabilities should be reviewed periodically and kept current…" The reason is that we may not have much control over the rules if we are using a third party service.
		Comments on software application development and management: 6.1.5 The Bank suggest to include the risk of “malicious code”, i.e. add the following words underlined to “detect security vulnerabilities, malicious code or coding issues” and allow the Bank to implement application scanning based on FI’s asset criticality framework.
		Comments on software application development and management: 6.1.5 The Bank suggests to include a footnote or glossary on the meaning of "Dynamic software scanning". The Bank suggests to allow implement application scanning based on FI’s asset criticality framework.
		Comments on software application development and management: 6.1.5 The first sentence seems to be a duplicate of 6.1.4, albeit with different terminology. We strongly agree with the need to ensure that software scanning rules are kept current. Therefore, we would like to suggest that the last sentence of paragraph 6.1.5 is appended to paragraph 6.1.4, and that paragraph 6.1.5 is wholly removed.

		6.1.6 We are generally supportive of MAS' intention to track and remediate issues and software defects. However, we feel that the wording "remediated before production deployment" imposes an unduly onerous standard of process adherence that insufficiently appreciates or takes into account business risk appetite. Certain application security verification and testing activities, especially those where source code or system configuration is an input, may reveal a sizable number of issues and software defects of various severity, ranging from informational to low severity to critical severity, and we observe that not all uncovered issues necessarily exceed business risk appetite and/or require the same urgency of remediation. Instead of the aforementioned wording, we would like to suggest that the Technology Risk Management Guidelines mandate the FI to establish clear criteria to promote releases to production (release management), tailored to the security verification and testing strategy, and separately define a strategy to manage and reduce technical debt incurred by issues and software defects that are within business risk appetite thresholds. We would like to highlight that Agile software development, based on an iterative and incremental development model, may serve as an effective enabler for such a strategy, especially when paired with intensified automation and actionable software security metrics such as mean time to repair (MTTR). 6.3.1 We would like to highlight that enabling frequent, efficient and reliable releases of software products is not a goal of DevOps, but rather a goal of continuous integration and continuous delivery (CI/CD). In practice, DevOps and CI/CD are often paired together because both are enablers of Agile software development. We would like to refer to the following page that explains the difference in more detail:

		https://www.synopsys.com/blogs/software-security/agile-cicd-devops-glossary/.
		Comments on software application development and management: 6.2.2 This appears to be a duplicate of TRMG citation 6.2.1 and could be combined.
		Comments on software application development and management: 6.3 DevOps is a means to structure Engineering and Support organisation and is not specific to Software Development/Management. The Bank suggests to insert this regulation in a separate section, if the focus is not specific to Software Development.
		Comments on software application development and management: 6.3 [page 23] The Bank suggests extending this to set out control expectations in DevSecOps, for completeness. 6.4 [page 23] 1. The Bank suggests the inclusion of guidelines around Sandbox API which should be more flexible to support innovation and collaboration. 2. The Bank suggests the inclusion of detailed specifications of security standards to use and specifications regarding access-log-retention policy. 6.4.3 & 6.4.4 [page 24] The Bank would like to confirm our understanding that this section does not include the business partner vetting process since business should be performing due diligence on partners. The Bank would like to confirm our understanding if "third-party" is referring to "direct third-party". In API ecosystem, API can be consumed by another third-party.

		6.5.1 [page 25] The Bank suggests the following revision to provide better clarity on the approvals needed: "… Any applications developed by end users should be approved by relevant business Business management, while those acquired by end users should be approved by both Business and IT management, where appropriate. Any applications developed or acquired by end users should be and managed as part of the FI's information assets." 6.5.2 [page 25] The Bank suggests the replacement of "importance" by "risk" for better clarity. Please see proposed revised version: "The FI should establish a process to assess the importance risk of end user developed or acquired applications to the business, and ensure appropriate controls and security measures are implemented to address the associated risks…"
		Comments on software application development and management: 6.3.2 Based on the contents of citation 9.1.1 where it is stated "access to information assets so that no one person has access to perform critical system functions" and as pointed out in our general comments about SW development practices we would request for the inclusion of clauses about encouraging FI to reduce risk by automating DevOps practices. For example, so long as another human reviews all code destined for prod and everything else is automated including testing and deployment plus a manual approval step from appropriate business and tech humans then this should suffice.
		Comments on software application development and management: 6.3.2 Not all types of testing needs to be segregated,

		suggest to re-word to “user testing”. The Bank suggests that FIs should to have the flexibility to implement DevOps activities logging and reviews based on FI SDLC framework and IT service management process. The expectation to enforce segregation of duties for DevOps is to be made clear.
		Comments on software application development and management: 6.3.2 We fully appreciate that MAS highlights to the industry that Agile software development and DevOps requires FIs to continue to incorporate necessary security practices to ensure the security of the application is not compromised. To add, we fully agree that a certain degree of segregation of duties remains required. However, we note that with increased adoption of automation, specifically automation of security verification and testing, the focus of such segregation of duties shifts to mitigating internal fraud risk through the deterrence of introducing malicious logic in production environments, as this is a notoriously difficult to mitigate risk area in an automated way. We would like to suggest that “the respective DevOps activities” is further defined and specified in terms of internal fraud risk, e.g. by requiring manual code review focused on malicious code before promotion to production as a means to implement segregation of duties, in order to enable FIs to further embrace CD/CI principles to accelerate software development and delivery. Moreover, we feel that “segregation of duties for the development, testing and operations functions in its DevOps processes” imposes a general standard of practice that draws required attention and focus away from sensitive operations such as promoting releases to production environments. In our view, segregation of duties should restrict itself to promotion of artefacts from non-production to production environments, as also stated in paragraph 7.6.2. Adherence

		to the principle of separation of environments (as defined in paragraph 5.7.3) has the side effect that promotion of artefacts from a non-production environment to another non-production environment is not designated as a sensitive operation. 6.4 Aside from the observation that FIs develop open APIs, we note that APIs are also being developed for other purposes than providing developers with a public interface and/or facilitating integration with third parties. In order to maintain an unambiguous understanding of the business context as described in paragraph 6.4.1, we would like propose to replace “API” with “open API” throughout paragraph 6.4 6.4.2 We would like to suggest to expand MAS’ definition of “strong controls” to authorize and control access to designated API services in order to facilitate implementation, or, alternatively, to state that the FI should adopt a comprehensive and robust security approach around the usage of open API services. We would like to suggest to expand MAS’ definition of “strong controls” to authorize and control access to designated API services in order to facilitate implementation, or, alternatively, to state that the FI should adopt a comprehensive and robust security approach around the usage of open API services.
		Comments on software application development and management: 6.4 There are 3rd party identity provider and/or relying party for authentication (e.g. National Digital Identity (NDI)/SingPass, Google, Apple), can FI rely on

		authentication provided by 3rd party without any further validation? If the relying party is a GovTech provider (e.g. Singpass), can FI rely on the authentication, without any further validation?
		Comments on software application development and management: 6.4.1 To provide clarity, there should be clarity in the revised Guidelines on what requirements apply to Open APIs and not to Closed APIs.
		Comments on software application development and management: 6.4.2 MAS proposed that FI should implement strong controls to authorise and control access to designated API services. We would like further guidance on MAS's expectation of "strong controls". Examples would be useful.
		Comments on software application development and management: 6.4.2 Would "strong controls to authorize and control access to designated API services" be covered under the paragraphs 6.4.4 to 6.4.9? If so, then would suggest that this paragraph be removed.
		Comments on software application development and management: 6.4.3 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. The vetting criteria should take into account the third party's nature of business, security policy, industry reputation and track record amongst others. Comments:

		There is a possibility that FIs may collaborate with a start-up third-party company in implementation of API services. In such a circumstance, such third-party may not have gained the industry reputation and track record as per the recommended vetting criteria. We would like to request for FIs to be given the flexibility to vet and assess such third-party based on applicable criteria under Section 3.4. Management of Third Party Services. Please see suggested edits below: "6.4.3 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. FI should vet and assess third party's suitability based on applicable criteria under 'Section 3.4 Management of Third Party Services'."
		Comments on software application development and management: 6.4.3 We would like to seek clarification on what is expected as a "well-defined vetting process" with regards to assessing third parties' suitability in connecting to the Bank via APIs. Would it be covered by the vetting criteria mentioned in this paragraph?
		Comments on software application development and management: 6.4.4 Does the risk assessment refer to the vetting of the third party or implementation of the API?
		Comments on software application development and management: 6.4.5 A definition of the term "API keys" is requested to provide clarity.

		Comments on software application development and management: 6.4.6 We would like to seek clarification on what is expected of "strong encryption standards and key management controls" for sensitive data transmission via APIs.
		Comments on software application development and management: 6.4.7 The term 'robust security screening' is vague and we would like to suggest what screenings that are expected to be mentioned instead, e.g. Penetration Testing and/or Vulnerability Assessment.
		Comments on software application development and management: 6.4.8 It would be challenging to have visibility to detect suspicious activities on public cloud service provider APIs. We suggest removing the detection of suspicious activities, and rely on the other controls mentioned in other paragraphs in this section.
		Comments on software application development and management: 6.4.9 Based on the risk profile, we would propose that this citation be limited to internet facing applications, and the citation be revised to "mitigate denial-of-service attack for API's to applications that are internet facing."
		Comments on software application development and management: 6.4.9 For the FI to cut off the API connection by third parties, this needs to be included in the contractual terms. In addition, if the third party observes such anomalies, there is

		responsibility for the third parties to take action to mitigate further attacks and notify the FI immediately.
		Comments on software application development and management: 6.5.1 a) May we have an understanding on the expectation of the involvement of “IT management” in the approval of all applications developed or acquired by end users? b) What is the criteria/rationale that IT management should evaluate against to determine the “approval” of end user applications? It is after all required by the respective business units for their business operations.
		Comments on software application development and management: 6.5.3 Kindly clarify the meaning of “shadow IT”, does it relate to unauthorized software?
		Comments on software application development and management: 6.5.3 We would like to clarify the definition of “Shadow IT”
		Comments on software application development and management: 6.5.3 [page 25] The Bank would like further clarity on the following: 1. Please provide a clearer definition of Shadow IT to better call out the differences between Shadow IT and End User Computing and Applications. 2. Should requirements in 6.5.3 be removed and incorporated into 6.5.1 and 6.5.2 to minimize ambiguity? 3. Separately, the Bank proposes for "Shadow IT" to be replaced by "End user computing and IT applications" to minimize ambiguity. See proposed revised version below:

		"Shadow IT End user computing and or IT applications acquired and used in the FI's environment without instituting appropriate controls and seeking the approval of relevant business and IT management increase the FI's exposure to risks, such as leakage of sensitive data, or malware infection. The FI should establish measures to monitor log and detect track the use of shadow IT end user computing and IT applications in its environment. End user should not be allowed to use shadow IT computing and IT applications should not be used until they have been properly assessed and approved for use."
		Comments on software application development and management: 6.5.3 We appreciate that MAS seeks to instruct FIs to monitor and detect the use of shadow IT in its environment. The sentence "end user should not be allowed to use shadow IT until they have been properly assessed and approved for use" appears to be a contradictio in terminis however, since shadow IT is by definition unwanted IT. We suggest to reword this as follows: "The use of shadow IT shall be treated as an incident and responded to accordingly."
		Comments on software application development and management: Paragraph 6.1.5 – For consistency with paragraph 6.1.4 (read with Annex A), we propose replacing "Automated static or dynamic software scanning" with "Automated Static Application Security Testing (SAST) or Dynamic Application Security Testing (DAST)". Paragraph 6.2.1 – With the increased adoption of the Agile software development by FIs, it would be useful if MAS could specify more controls to better govern the process (e.g. minimum documentation required as highlighted in our comment on paragraph 5.1.2).

		Paragraph 6.3.2 – The proposed segregation of duties for the development, testing and operations functions goes against the grain of DevOps, which centres on automation and integration of traditionally separate processes. Would MAS consider alternatives safeguards (e.g. peer reviews) to address the relevant concerns? Paragraph 6.4.3 – We propose replacing the word "vetting" with "due diligence", for clarity and simplicity, as the latter term is more standard and widely understood. Paragraph 6.4.8 – We would like to clarify if the real-time monitoring referred to in this paragraph refers to the security aspect or the availability/health monitoring aspect. Paragraph 6.5.1 – The management end-user computing should be based on the material impact on the FI, and is already addressed at 6.5.2. We therefore propose deleting the last sentence of paragraph 6.5.1 as follows: "The prevalence of common business application tools and software on the Internet has enabled end user computing, where business users develop or use simple applications to automate their operations, such as perform data analysis and generate reports. Any applications developed or acquired by end users should be approved by the relevant business and IT management, and managed as part of the FI's information assets".
		Comments on software application development and management: Section 6.3 (DevOps Management) We seek clarification from the MAS regarding the degree or extent to which duties need to be segregated by the Bank for the development, testing and operations functions for DevOps processes, in particular the required degree or extent of segregation of duties between the development and operations functions. We would be grateful if the MAS could provide guidance on

		the precise level(s) of segregation of duties required to be enforced by the Bank between the development and operations functions for DevOps processes.
		Comments on software application development and management: The bank is supportive of the MAS proposed TRM Guidelines on Software Application Development and Management.
		Comments on cyber surveillance and security operations: <12.3> Presently, as part of the bank's incident management framework, we are adopting the same procedure to manage cyber incidents and IT incidents. In this connection, we would like to understand whether it is MAS' intent for banks to manage cyber incidents separately?
		Comments on cyber surveillance and security operations: 12.1 Cyber Threat Intelligence and Information Sharing • The guideline should not suggest to mandate the use of a specific technology in the regulations, instead focus on the control objective that need to be achieved. Suggested wordings below. 12.1.5 The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services to facilitate evaluation and identification of online misinformation. 12.2 Cyber Monitoring and Security Operations The way anomalous user behavior is detected shouldn't be tied to a particular methodology. Profiling individual users and their behaviour leads to legal/privacy/regulatory concerns. This relate to how the data can be used, how it is shared and protected, and what

		country specific regulatory requirements will need to be addressed when storing this type of information (considering JPMC operates in many different countries). 12.3 Cyber Incident Response and Management The testing of cyber incident response plan is covered in section 13.3 (Cyber Exercises) and hence can be removed from here. To follow a risk based approach, we recommend this requirement to be periodic as determined by FI rather than annual. Suggested wordings below. 12.3.3 The FI's cyber incident response plan should be periodically reviewed and/or updated based on current cyber threat intelligence, information-sharing and lessons learned following a cyber event.
		Comments on cyber surveillance and security operations: 12.1.2 "The FI could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties." Would procuring cyber intelligence monitoring services be considered as "outsourcing" or "third party services" 12.1.5 "The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation." Would engaging external media monitoring services be considered as "outsouring" or "third party services"? Examples of this are: any wrong information about FI's products, services or attempts to misuse of FI's name, brand, products or any misinformation related to their services that can affect their reputation, brand-image, possibly misguide the public, thereof

		12.2.6 & 12.2.7: clarify if this is intended for external customers
		Comments on cyber surveillance and security operations: 12.1.5 The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation. We would like to highlight that this is a very wide scoped requirement and FIs may find it challenging to monitor the entire cyber-space and have the ability to contain/stop such information spread.
		Comments on cyber surveillance and security operations: 12.1.5 [page 45] 1. The Bank suggests the following revision: "The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace internet. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation." 2. The Bank would like to share that it is not possible to be exhaustive and comprehensive to “catch” all misinformation about the Bank in the cyberspace. For example, there may be fake images created of our senior management in pictures and videos which are unlikely to be detected. 12.2.2 [page 46] The Bank suggests the following revision: "As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block

		callbacks, which can be tell-tale suspicious signs of intrusions."
		Comments on cyber surveillance and security operations: 12.1.5 We are supportive of MAS' stance against misinformation being propagated in cyberspace. We note that widespread falsehoods and incorrect assertions on matters of public concern may harm Singapore's social fabric and/or financial stability e.g. through the erosion of customer trust. We do recognize that FIs have a certain degree of responsibility in supporting the management of misinformation, however, we note that, due to the dynamics of the dissemination of information and social media on the Internet, the FI's exposure to the risks related to the spread of misinformation in cyberspace are strongly correlated with: 1. the type of business activities employed and the corresponding type of customers; 2. the FI's market share and number of customers; 3. the spread of online financial services, and 4. the FI's social media strategy Our concern is that a strict interpretation of paragraph 12.1.5 may, for selected FIs, lead to an unduly onerous standard of practice that is potentially not commensurate with the FI's exposure to the risks related to the spread of misinformation in cyberspace. Therefore, we would like to recommend to generally state that FIs should tailor their misinformation management strategy based on a comprehensive risk assessment, taking into account influential factors such as, but not limited to, the type and size of business and customers and the FI's social media strategy.
		Comments on cyber surveillance and security operations: 12.2.1 The words "system activities" and "cyber events for critical systems" has wide implications. Please clarify if

		these words are referring to infrastructure or application stack or both?
		Comments on cyber surveillance and security operations: 12.2.3 Kindly clarify how the relevant events in the system logs are to be reviewed. Perhaps, the FI should be given the flexibility to adopt a risk based approach with specific focus on critical and transactional systems only.
		Comments on cyber surveillance and security operations:12.2.3 We request clarity on what is “consolidation and processing of system logs”? As there would be many application, database and operating system logs, we would like to propose the addition of a risk basis in deciding which system logs to be included and prioritized for security monitoring.
		Comments on cyber surveillance and security operations: 12.2.4 We would like to propose that what types of events to be correlated be determined through the FI’s risk assessment process rather than specifying “multiple events” herein.
		Comments on cyber surveillance and security operations: 12.2.6 and 12.2.7 Machine-learning security analytics is a good direction but not all FIs are ready or at the same readiness state. We propose that this be put as good practices in the Annex first, until there is some level of maturity across the FIs in the industry.
		Comments on cyber surveillance and security operations: 12.2.6/12.2.7 It is too onerous and expensive to expect baseline monitoring of all systems. The Bank suggests that it be given the flexibility to adopt alternate security measure based on risk based approach, in line with FI’s insider threat detection and management framework.

		Comments on cyber surveillance and security operations: Clarification on paragraph 12.2.9 of the Consultation Paper We would like to clarify what the system logs retention period is.
		Comments on cyber surveillance and security operations: Comments: We commend the MAS efforts to encourage industry cooperation with trusted parties on information sharing arrangements. 12.1.1 To maintain good cyber situational awareness….Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities. Comments: For better clarity to the requirement, we would recommend MAS to provide footnotes on specific terminologies such as 'situational awareness', cyber alerts' and 'cyber events'. A good source of reference is the FSB Cyber Lexicon (http://www.fsb.org/wp-content/uploads/P121118-1.pdf), released on November 2018, for these terminologies. 12.2.2 As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be tell-tale signs of intrusions. Comments: We request minor edits suggested below for better clarity: "12.2.2 As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block call-backs, which can be indicators of attempted intrusions."
		Comments on cyber surveillance and security operations: Cyber Threat Intelligence and Information Sharing The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the

		cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation. ---------- Feedback ---------- Would like to propose to remove this from TRMG as this is outside the realm of TRM. Detecting misinformation in the vast online is almost impossible - Big Tech firms already have issues managing them. If we are unable to effectively detect misinformation, FIs may not be able to effectively respond to the misinformation.
		Comments on cyber surveillance and security operations:The bank is supportive of the MAS proposed TRM Guidelines on Cyber Surveillance and Security Operations
		Comments on cyber surveillance and security operations: Under paragraph 12.1.5, MAS proposes that a FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. This would be challenging for a small foreign-incorporated bank in Singapore based on the risks associated with the contagion of misinformation and the associated systemic risk impact in Singapore. We proposed that the requirement to be imposed on banks which could have a significant impact to the broader economy.
		Comments on cyber surveillance and security operations: We refer to Paragraph 12.1 and would like to request MAS to define 'cyber intelligence monitoring services' and also 'cyber related information', and provide examples of or define "external media monitoring services". We refer to Paragraph 12.2 and would like to request MAS to clarify if the expectation on monitoring and surveillance extends to infrastructure components e.g. servers, databases. We would also appreciate it if MAS could define

		the term "real-time" monitoring. For instance, will polling every 30-seconds be close enough to "real-time"? In addition, we would like to suggest to MAS to adopt a risk based approach to determine systems that will be in scope for baselining.
		Comments on IT audit: The bank is supportive of the MAS proposed TRM Guidelines on IT Audit.
		Comments on application security testing: A.2 (a) / A.2 (c) We would like to suggest to universally maintain the term “source code, byte code and/or binaries” and keep the wording aligned with paragraph 7.6.1. We would like to suggest to universally maintain the term “source code, byte code and/or binaries” and keep the wording aligned with paragraph 7.6.1. A.2 (b) In our experience, DAST is best used in a grey box approach, as effective implementation requires a certain degree of configuration tailored to the target. We would like to suggest to replace “The tester has no prior knowledge” with “The tester has limited or no prior knowledge” C.1 There’s a ‘s’ missing in the first sentence. We propose to replace “follow” with “follows”.
		Comments on application security testing: The bank is supportive of the MAS proposed TRM Guidelines on Annexes on Application Security Testing, BYOD Security & Mobile Application Security.

		Comments on BYOD security: Annex B: BYOD Security We propose that it be clarified that the bank can adopt either of the solutions – MDM or Virtualisation.
		Comments on BYOD security: B.1 The FI should implement data loss prevention measures on personal mobile devices that are used to access the FI's information assets. Two common ways to address BYOD security are the use of mobile device management and virtualisation solutions. These solutions can be augmented with other security measures for mobile devices to provide enhanced functionalities: BYOD is often a misunderstood term even though the guideline has provided a very clear definition. Most people will just assume it is privately owned devices without considering what they are used for and the environment that they are accessing. The recommendation is to change the term "BYOD" to "remote computing". The reason is that it should not matter whether it is a bank owned device or a staff owned device. What is important is that adequate security controls must be in place prior to allowing devices to access the corporate network remotely.
		Comments on BYOD security: BYOD devices, as such, are by design not allowed any access to any component of the Bank Infrastructure. The access to information assets is rather granted on a per Application basis and hence would MAS consider adequate a MAM (Mobile Application Approach) instead?
		Comments on BYOD security: Proposed amendment to paragraph B.1(b) of the Consultation Paper Virtualisation allows staff to have on-demand access to enterprise computing resources and data from their mobile devices using strong authentication and network

		encryption. The FI's data is not downloaded into the mobile device as it is processed within the corporate data centre environment. Justification: With regional data centres consolidation trends, it is also possible that staff can connect to the resources other than those hosted in "Data Centres" – in many countries in APAC, FIs maintain smaller in-country presence (in the form of technical rooms, Server Equipment Rooms). Logical network segregation will still ensure that the security standards are not being compromised.
		Comments on BYOD security: With regard to Annex B, B.1(a), we would like to point out that the last sentence "A robust MDM solution should be implemented for all BYOD arrangements" is in conflict with the opening paragraph in B.1, in which MDM is only one of the two common ways to address BYOD security. We would like to clarify that bank can implement either one of the solutions: MDM or virtualisation
		Comments on mobile application security: Annex C, C.1 (e) [page 59] The Bank will like to understand if the expectation is that the mobile application must have its own build-in keypad or if it is only expected that the in-app keypad is only mandatory for keying in sensitive information.
		Comments on mobile application security: Annex C: Mobile Application Security – We would like to seek clarification from MAS if the requirement applies only in the event that the FI departs from using the OS keyboard.
		Comments on mobile application security: C.1 (a) Propose that the following wordings are included, '…or

		store data in the protected trusted security enclave of the mobile device.”
		Comments on mobile application security: C.1 (d) implement certificate or public key pinning to protect against MITMA; This control is in our opinion too concise and limits the options as to how a protection against MITMA can be achieved. Neither certificate nor public keys should be fixed as a regular renewal of the authentication information is expected, so this could pose operational problems. Instead, best practices for certificate validation should be proposed like validation of the combination of CN+Issuer for authorization. Public Key pinning should be considered in specific scenarios.
		Comments on mobile application security: C.1 (e) This might not be the best way to prevent malware that captures keystrokes. Stock keyboards from the mobile device manufacturers might be better at preventing such attacks.
		Comments on mobile application security: On mobile application security: Comments: Sandbox environment was mentioned in the MAS Circular No. SRD TR 02/2014 – IT security risks posed by personal mobile devices. Hence, we recommend that sandbox environment as a security measure be also included in this section.
		Comments on mobile application security: We note the list of recommended security measures in Annex C: Mobile Application Security. We would like to

		seek confirmation that these security measures are not mandatory and the Authority will leave it to the Bank to review and implement appropriate security measure(s) which should commensurate with the level of risk in the services offered through the mobile application. For example the implementation of an in-app keypad may not be necessary if the mobile application only permits viewing of statements.
		Comments on mobile application security: We refer to Annex C and would like to clarify that for Annex C item (b), must this be implemented within the mobile application or can this be performed by a third party security/anti-malware solution on the device? In addition, we would like to feedback that for Annex C item (e), this might not be feasible as the choice of input methods and applications (e.g. third party keyboards) is typically up to the user. Users have to authorise them though; however, most users usually do as they are not particularly aware of the associated risks.
		Comments on online financial services: 'Sec 14.1.5 Distribution of mobile applications or software to customers should only be performed through official mobile application stores..' Comments: FI do not distribute mobile banking application to customers but rather customers choose to download FI's mobile banking application from official mobile application stores. Please see suggested edits below: "14.1.5 FI's customers should download FI's mobile banking applications or software"
		Comments on online financial services: <14.1.6> We would like to seek clarification and guidance from MAS on scenarios that warrant reporting to law enforcement agencies, which agencies (e.g. Cyber Security Agency of Singapore, Singapore Police Force) as well as the

		channel and avenue for FIs to go about notifying such incident?
		Comments on online financial services: <14.4.1> We would like MAS to clarify: 1. On informing customers, whether it is sufficient to include a paragraph as part of the general terms and conditions. 2. With examples of what constitutes "security features" of the online financial services which customers need to be notified of.
		Comments on online financial services: 14.1 Security of Online Financial Services The guideline should be less-prescriptive. Monitoring of SMS and e-mail of customers is not feasible as it takes place outside the FI's infrastructure. It may not be practical to alert customers of every instance of Phish sites identified as there are many discovered each day. Suggested wordings below. 14.1.6 The FI should actively monitor the Internet, mobile application stores and social media websites, for phishing campaigns targeting the FI and its customers. Timely action should be taken to report the impactful phishing campaigns to the service providers and law enforcement agencies as appropriate to facilitate removal of the malicious content
		Comments on online financial services: 14.1.3 For the protection of online financial services, we recognize the need to minimize exposure to common attack vectors. However, we would like to highlight that protection against code injection attacks and cross-site scripting is sufficiently

		covered by paragraph 6.1.2 already in the form of input validation and output encoding. To help limit redundancy, we propose to remove references to code injection attack and cross-site scripting, or, alternatively, refer to paragraph 6.1.2.
		Comments on online financial services: 14.1.6 [page 52] In view of the practicality of monitoring customers' emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers, the Bank suggests for MAS to revisit expectations of this requirement.
		Comments on online financial services: 14.1.6 The bank's Security Operations Team will monitor cybersecurity threats and take actions to remove phishing or fake bank websites. However, it is impractical to some of the phishing channels (in particular mobile application stores, text messages) of which the bank is only able to take action as and when we receive feedbacks from customers or intelligence from our own sources.
		Comments on online financial services: 14.1.7 The bank detects rooted or jailbroken mobile devices when the mobile app starts and stop the mobile app when rooted or jailbroken mobile devices are detected. However, it is not within the control of the bank to block rooted or jailbroken devices from downloading and launching the bank's mobile application. Are FIs expected to block the downloads (this is controlled by Apple's App Store or Google's Play Store) and launching of the bank's mobile application?
		Comments on online financial services: 14.2.1 - What is the practice and requirement for OTP? Is

		classification required for first time login and mask? As of now all banks are showing the masked information on login without 2FA. Can this be added in the text?
		Comments on online financial services: 14.2.10 A process should be implemented to secure the issuance and enrolment of the authentication or transaction signing mechanism so as to prevent the theft of the mechanism for unauthorised access to the FI's customer's online account. The control is rather vague as to what are acceptable means for secure enrolment and issuance. Please provide definitions and examples.
		Comments on online financial services: 14.2.10 For clarification, any process will not be able to cover scenario where it is beyond the control of the FI e.g. customer gives out their credentials to the fraudsters.
		Comments on online financial services: 14.2.11 The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. In the event of interference, the FI should put in place measures to detect and terminate the session. To prevent an attacker from maintaining a hijacked session indefinitely, online session should be automatically terminated after a pre-defined time. The intent is clear but the control lacks of detail as to what is the minimum requirement for fulfilling the control.
		Comments on online financial services: 14.2.3 With the avail of MyInfo services, our customers can authenticate himself/ herself via the use of SingPass and a 2FA (sms or via soft-token) control through both account

		opening or service details update to provide the following details: • registered address (Prefilled with ICA-MyInfo; User not able to update) • mailing address (User update) • email (Prefilled with SingPass-MyInfo; User is able to update) • mobile number (Prefilled with SingPass-MyInfo; User is able to update) Using the MyInfo authentication method, (including downstream existing mitigating controls for high-risk transactional activities), are FIs still required to implement transaction-signing for update of sensitive customer data? OR would using MyInfo solely be sufficient?
		Comments on online financial services: 14.2.4 We wish to clarify whether online card payment for 3DS transaction is within the scope of Section 14 of the TRM. Section 14 relates to online financial services for banking, trading, insurance, or other financial and payment services that are provisioned via the Internet. The payment services refer to mobile/digital wallets and payments, financial and payment services offered using account and transaction APIs, etc. From Oct 2019 onwards, banks will be implementing a new version of 3DS card authentication platform. The new version 3DS 2.0, use transaction APIs which the authorisation message will carry more transaction details for banks to use Risk Based approach, in replacing OTP as a form of authentication. Under section 14.2.4 which deals with Customer Authentication and Transaction Signing, it is stated that besides login and transaction-signing for high-risk activities, the FI may apply a risk-based approach and implement appropriate risk-based or adaptive authentication that presents customers with authentication options.

		We are of the view that if risk-based approach is applicable to 3DS card transaction, the bank will have the flexibility to decide whether we can use risk-based approach, or step up with OTP or soft token to authenticate the 3DS transaction going forward.
		Comments on online financial services: 14.2.5 With regards to "…period that is as short as practicable…", this is too open ended and subject to different interpretation, please provide guidance for FIs to adopt.
		Comments on online financial services: 14.2.7 Suggest to include the words "if feasible" after the word "calibrated" in line 2.
		Comments on online financial services: 14.3.1 If the suspicious/fraudulent transaction is a false positive, and the system blocks it, does MAS expect the Bank to be accountable to the customers for losses arising from payment failures?
		Comments on online financial services: Need clarification if Section 13 (2013 TRM) - Payment Card Security (Automated Teller Machines, Credit and Debit Cards) is now under Online Financial Services. If yes, which subsection. If not under Online Financial Services, then which section in the revised TRM.
		Comments on online financial services: Paragraph 14.1.6 – As phishing attempts are typically directed at the consumer (e.g. through emails or text messages), it may not be feasible for the FI to put in place comprehensive monitoring measures. We ask that further guidance be given on the scope of an FI's responsibility to monitor and report these phishing attempts. Given the

		volume of such phishing attempts, it would also be useful to for FIs to have clear and simple channels to make the necessary reports.
		Comments on online financial services: Point 14.2 Customer Authentication and Transaction Signing Point 14.2.4 Besides login and transaction-signing for high-risk activities, the FI may apply a risk-based approach and implement appropriate risk-based or adaptive authentication that presents customers with authentication options that commensurate with the risk level of the transaction and sensitivity of the information. Question Any criteria or suggestive list of activities wherein additional authentication options need to be implemented.
		Comments on online financial services: The bank is supportive of the MAS proposed TRM Guidelines on Online Financial Services.
		Comments on online financial services: We refer to Paragraph 14.2.4 and would like to request MAS to provide some examples or common practices of adaptive authentication. We refer to Paragraph 14.2.10 and would like to share that current practices usually involve issuance/ enrolment of authentication (for login). However, for transaction signing, can MAS elaborate on the enrolment expectation?
		Comments on online financial services: 14.2.8 A soft token is a software-based two-factor authentication mechanism installed on a general-purpose

		device. Where soft token is used for customer authentication, appropriate measures, such as verifying the identity of the customer, detecting and blocking rooted or jailbroken devices, and performing device binding41, should be implemented for the soft token provisioning process. Comments: As user identity can be spoofed, FI should first alert the customer and validate if he/she is performing a soft token registration process. Please see suggested edits below: "14.2.8 A soft token is a software-based two-factor authentication mechanism installed on a general-purpose device. Where soft token is used for customer authentication, appropriate measures, such as verifying authenticity of user identity by alerting the customer, detecting and blocking rooted or jailbroken devices, and performing device binding, should be implemented for the soft token provisioning process.
		Comments on online financial services: 14.3.1 The FI should implement real-time fraud monitoring or surveillance systems to identify and block suspicious or fraudulent online transactions. Comments: For added guidance to FIs, we would request MAS to consider defining the scope and value of the fraudulent transaction as well as the respective extend to which the transaction and/or associated online functionalities should be blocked. In addition, it would be beneficial if there is a similar arrangement just like the cyber threat intelligence and information sharing for FIs to report/share phishing/fraud incidents and garner the required support and mitigative actions real time (e.g. removing/blocking of a fraudulent website within minutes of incident reporting). Other FIs informed of this incident real time may then be able to take additional precaution and measures to prevent similar incidents from occurring.

		Comments on online financial services: 14.4.3 The FI should alert their customers to cyber threats and incidents, and educate their customers of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services. Comments: Please see minor edits to provide clarity to customers on the risk using rooted or jailbroken mobile devices: The FI should alert their customers to cyber threats and incidents, and the risks of using rooted or jailbroken mobile devices. The FI should educate their customers of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services."
		Comments on online financial services: <14.2.1> The definition of multi-factor authentication is defined under footer note 19. Hence, for clarity, in relation to paragraph 14.2.1, we would like to suggest MAS to make reference to the existing definition in footer note 19.
		Comments on online financial services: <14.2.3> a) We would like to seek MAS to provide guidance on the criteria/factors to constitute high risk activities to facilitate FIs' assessment. b) We would like to seek MAS' definition on the transaction data signing (e.g. digital signatures), and whether there are any other methods that can be considered as Transaction Date Signing (TDS)? We note that the TRM guideline states that TDS is required to change the office address (which is not the mailing address), office phone number, home phone number and email address. The bank has received feedbacks from

		customers that changes to these details need not subject to TDS since these details are not used for high risk transaction. Or we can based on our internal assessment accepting such "high risk activities"? e.g. the change of address if the user uses MyInfo to change their home address this can be accepted as without TDS. Therefore, we are seeking clarification on the absolute applicability of this section.
		Comments on online financial services: 14.2.6 & 14.2.7 [page 53] The Bank would like to understand if it includes biometric solutions implemented by mobile phone manufacturers.
		Comments on online financial services: 14.2.11 [page 54] The Bank will like to understand if the online session must automatically terminate after the pre-defined time even when the customer is still using it? Currently the Bank already has a time-out if our system detects there is no activity by customer.
		Comments on online financial services: 14.2.3 – Can they taken an account of PayNow which is not required any transaction signing. Also it is better to clarify whether merchant/bill payment is out of scope
		Comments on online financial services: 14.2.8 - Cross check and validation should be done to verify jailbroken devices.
		Comments on online financial services: Paragraph 14.1.7 and 14.2.8 – In connection to blocking rooted or jailbroken mobile devices from accessing the FI's

		mobile applications, we urge MAS to allow FIs to proactively encourage customers to switch out of jailbroken devices instead of implementing an immediate hard block.A proactive approach will allow customers who are used to performing online financial services more time to adjust and make the switch, thereby resulting in a less disruptive and much better customer experience. Given the large number of customers who use online financial services, an immediate block may potentially lead to a surge in customer complaints. We would also like to propose that FIs be allowed to stagger the implementation process according to its own risk-based prioritisation as opposed to a hard deadline once the guidelines are effective. We would like to seek MAS' clarification that the condition need not apply to an FI's overseas operations. For example, in a number of countries, rooted phones are widely used to cater for local language requirements not supported by the operating systems. In such countries, the use of rooted phones is widely accepted in society and by the local regulators. If paragraph 14.1.7 was to be applied groupwide for FIs with overseas operations, it would be impossible for Singapore banks expanding overseas to compete effectively with local players not confined by the same regulations. We would like to propose that this condition be exempted for Singapore banks operating in a foreign jurisdiction subject to the following conditions: 1. It is not a local regulatory requirement that rooted mobile devices should be blocked from accessing the FI's mobile application; 2. The Bank has conducted its risk assessment of the use of rooted mobile devices in the specific jurisdiction and is satisfied that it is within Bank's risk tolerance.
		Comments on online financial services: Paragraph 14.2.4 – It would be useful if some examples of adaptive authentication can be provided.

		Comments on online financial services: Paragraph 14.2.5 – It would be useful if some guidance on what constitutes a practical validity period of OTPs can be given.
		Comments on online financial services: Paragraph 14.2.9 – We ask that MAS reconsider this requirement: the use of a different cryptographic key for generating OTP and transaction signing code may not be technically feasible, as a token would generally only host 1 key from which all cryptographic activities are generated.
		Comments on online financial services: Paragraph 14.2.12 – We would appreciate some guidance on the frequency of performing the security risk assessments referred to in this paragraph.
		Comments on online financial services: Paragraph 14.3.1 – As FIs may serve a varied clientele, it may be challenging to design rules of real-time fraud monitoring or surveillance systems to identify and block suspicious or fraudulent online transactions specific to each customer's usual usage behaviour. It would be more practical to formulate one set of rules applicable to all customers. It would also be useful for MAS to clarify if this requirement covers all online transactions on all channels.
		Comments on online financial services: Paragraph 14.3.3 – The MAS E-Payments User Protection Guidelines was recently issued with an effective date of 30 Jun 2019, under which responsible FIs should provide transaction notifications (on a real time basis for each transaction or on a batched basis at least once every 24 hours to consolidate every notifiable transaction made in the past 24 hours), to each account holder (individuals and sole proprietors) of a protected account, and the account holder of a protected account should report any unauthorised transaction to the responsible FI as soon as

		practicable after receipt of any transaction notification alert for any unauthorised transactions. We would like to seek MAS' confirmation that the requirements this paragraph are fulfilled if the same approach is adopted for the other client segments.
		Comments on online financial services: Paragraph 14.4.1 – We propose that customers only be notified of changes made to the security features of the services which affect them.
		Comments on online financial services: Point 14.2.10 A process should be implemented to secure the issuance and enrolment of the authentication or transaction signing mechanism so as to prevent the theft of the mechanism for unauthorised access to the FI's customer's online account. Question Is this point regarding digital certificates?
		Comments on online financial services: Point 14.2.11 The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. In the event of interference, the FI should put in place measures to detect and terminate the session. To prevent an attacker from maintaining a hijacked session indefinitely, online session should be automatically terminated after a pre-defined time. Question Is it that a session should timeout even when the customer is on a long active session?
		Comments on online financial services: <14.4.3> We would like MAS to provide further guidance that "FI should alert their customers to cyber threats and incidents". This is a vague statement as it potentially covers

		all areas and customers if this is defined literally. If there is any incident with customer(s)'s accounts, we will definitely inform the customer(s). Is this suffice to satisfy this guideline?
		Comments on technology risk governance and oversight: 1.Section 3 Technology Risk Governance and Oversight outlines the expected role and responsibility of the Board of Directors and Senior Management. We welcome the revise wording of this section as it clearly outlines the regulator's expectation on the Board and Senior Management respectively. Nevertheless, the wording as it is appears to be drafted with locally incorporated bank in mind. In the case of foreign bank operating as a branch in Singapore and depending on the scale and size of such foreign bank, the local CEO or country head and his direct report (the senior management team) are tasked to manage the day to day operations and risk (including markets, credit, operational, legal, compliance and technology risks) of the branch. In addition, the branch are expected to comply and execute policies approved at the Group or Head Office. It is rather unusual for the branch to table issues or matter for the approval of the Board at Head Office as the relevant Senior Executive (usually a member of the Group CEO's Executive Committee) at the Head Office would have been tasked to manage all branch issues and risks. As an example, for matter such as 3.1.5 "The Board of Director or a committee delegated by it, is responsible for ensuring a sound and robust risk management framework is established and maintained to manage technology risks in a manner that is commensurate with the FI's risks" and the reference to "FI" in this context should refer to the branch in Singapore, the branch would develop its branch level technology risk management framework that is inline with the Group's policy and risk appetite (which is already approved at the Head Office level) and would not necessarily have to be approved by the Board at Head Office. Rather, such branch level risk framework is approved by the local risk management committee. Same for the appointment of

		Chief Information officer Chief Technology Officer or Head of Information Technology. Appointment of such position at the branch level is typically approved by the business line manager. We would therefore like to clarify with MAS if the responsibilities that are attributed to the Board (for locally incorporated bank) can be assumed by local risk committee (which is made up of local senior management and chaired by local Chief Risk Officer. 2. Refer to section of security awareness training - For foreign bank branches in Singapore, It will be challenging for the country to ensure the board of directors level to attend the training. We will ensure all designated senior managements in country to attend\complete all necessary trainings. We would like to seek for MAS's clarifition if it is aligned with MAS expectation.
		Comments on technology risk governance and oversight: 3.1.1 [page 9] The Bank would like MAS to consider the below revision for better clarity on responsibility of Board and senior management: "It is vital that the FIs' board of directors and senior management are fully responsible for ensuring ensure effective internal controls, and …."
		Comments on technology risk governance and oversight: 3.1.5 [page 9] The Bank suggests including a sub-paragraph for clarity on the differences in roles/ responsibilities between IT Security and Technology Risk. Please see following proposed sub-paragraph for consideration: "Appointing a Head of Technology Risk, with the requisite expertise and experience, to be responsible for the FI's overall Technology Risk strategy and management"
		Comments on technology risk governance and oversight: 3.1.5 (j) [page 10]

		The Bank would like further clarity on MAS' expectations of Board (or designated committee) in assessing management competencies for developing policies to manage technology risks.
		Comments on technology risk governance and oversight: 3.2.2 [page 11] The Bank suggests the below revisions, to minimize ambiguity on role of senior management with respect to risks associated with deviations: "The FI should ensure risks associated with deviations are thoroughly assessed, and ensure they are reviewed and approved by senior management…"
		Comments on technology risk governance and oversight: 3.3.1 [page 11] The Bank suggests the below revisions, to allow FIs some flexibility as part of their implementation to meet this requirement (e.g,. incorporating in existing framework, standards, etc): "To have an accurate and complete view of its IT operating environment, the FI should establish an appropriate information asset management framework practices that includes the following..."
		Comments on technology risk governance and oversight: 3.1.2 What would qualify as requisite "knowledge to understand and manage technology risks" for board of directors and senior management? Are they expected to possess related work experience such as technology risk management, IT audit or IT compliance?
		Comments on technology risk governance and oversight: 3.1.2: For a small branch office, at the Group level, there is an appointed Group CIO which oversees all technology risks associated with the Group. Locally, there is senior management accountability in the form of a local risk committee which has oversight of all technology risks

		impacting the local branch. This sufficiently ensures that any technology risks is addressed at the local and Group level.
		Comments on technology risk governance and oversight: 3.1.3: Key IT decisions are made at the Group level and subsequently rolled out globally. However, consultation is sought from each jurisdiction to ensure that all local regulations are taken into account.
		Comments on technology risk governance and oversight: 3.1.5 (c) and (d) Regarding Board's approval for appointment of CIO, CTO or Head of Information Technology, CISO or Head of Information Security, is the expectation that these requirements apply to similar roles in overseas entities of the banking group, or are they applicable based on local country requirements?
		Comments on technology risk governance and oversight: 3.1.5 What are the areas expected to be covered in the technology risk management strategy?
		Comments on technology risk governance and oversight: 3.1.6 Regarding the need for clear delineation of staff who has responsibility in managing technology risks, clarity is needed on whether this is between Line 1 and Line 2, or /and between Line 1 functions in Systems Development, Operations, Security, etc. This paragraph should also be considered for consistency with para. 4.1.2 which would refer to Information Technology, which is a Line 1 function, that is accountable to manage technology risks.
		Comments on technology risk governance and oversight: 3.2.1 Suggest that the definition of "Information Assets" in

		footnote 3 excludes data with little risk of exposure, such as tokenized or anonymized data. In addition, suggest that for information assets used by service providers, which the definition should be restricted to where sensitive information applies only. The reason is that FI may not have visibility to or ability to influence to have all the controls over information assets used by all service providers where the information is not considered sensitive.
		Comments on technology risk governance and oversight: 3.3.1 Should assets owned and hosted by service providers that do not directly store or process customer data and/or confidential corporate data be excluded from this Information asset management framework requirement?
		Comments on technology risk governance and oversight: 3.3.1 Should shared payment gateway providers such as SWIFT, NETS, Visa and MasterCard, which support FI's business and delivery of financial services be excluded from the scope of this requirement?
		Comments on technology risk governance and oversight: 3.3.2 - The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes. *** Comments: We agreed with MAS that it is important to establish an information asset management framework to cover the information assets that support the FI's business and delivery of financial services. We seek clarification if this requirement also applies to any shared information assets not limited to those within the FI's environment (e.g. on the Cloud infrastructure).

		For FIs that have global financial footprints, there are challenges in maintaining an inventory to cover all information assets on a periodic basis. As such, we would like to request for MAS to allow the FIs the flexibility to also consider the security classification and business impact criticality of the information assets when performing periodic review and updates.
		Comments on technology risk governance and oversight: 3.4 Management of Third Party Services Suggest to re-align this statement from para 11.1.2 for consistency. Suggested wordings below in italics. 3.4.1 The use of certain third party services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks.This should include systems and endpoint devices managed by the FI's service providers."
		Comments on technology risk governance and oversight: 3.4.1 As the recent MAS Consultation Paper on Outsourcing has extended coverage to third parties as per revised definition of "outsourcing arrangement", we suggest that MAS' consider not to duplicating similar requirements in this MAS TRM Guidelines.
		Comments on technology risk governance and oversight: 3.4.1 The definition of "Third Party" is broad and the extent of

		assessment is extensive. Are we expected to cover all aspects (as in Para 3.4.1 and Para 3.4.2) in the assessment for "non-standardised services and products that are typically not considered outsourcing (power supply, telecommunications lines, commercial hardware and software, etc.)"?
		Comments on technology risk governance and oversight: 3.4.2 - Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognised by the industry, before entering into a contractual agreement or partnership with the service provider. Comments: We agreed that use of certain third-party services as pointed out in 3.4.1 could result in significant risks to the FIs and proper due diligence should be performed on such service providers prior to the start of the services. We would like to request for MAS to also allow the FIs to assess the degree of due diligence to be performed as proportionate with the materiality of the third-party service arrangements. For example, the due diligence performed for FI's partnership with Fintech start-up firms to develop a Proof-of-Concept innovation solution (without customer information) will differ from the FI's engagement of a third-party service provider for outsourcing arrangement. In view that FIs will continue to onboard more non-outsourcing Fintech service providers in the upcoming years, MAS may consider appointing a centralised certifying process that can facilitate 1st level due diligence. Once service providers are certified as a pre-requisite, FIs would proceed to conduct internal due diligence prior to entering into a contractual agreement or partnership with the FinTech service providers. The benefits include: - A centralised due diligence methodology that can be continuously updated in accordance to the evolving

		technology risks. This approach mitigates risk arising from the varying standard gaps across FIs - FIs individual due diligence process will be shorter and smoother, increasing the speed to onboard service providers - Certifying body will have an independent lens with the sole objective of completing due diligence accurately Specifically, for data centre facilities service providers and cloud hosting service providers, we seek clarification on whether MAS is expecting FI perform TVRA or request for TVRA report as part of due diligence for such service providers.
		Comments on technology risk governance and oversight: 3.4.2 Propose that the new certification and accreditation requirements be considered not as a mandatory requirement but may be considered where available, as not all service providers may have this. Time may be needed for the service providers who do not yet have these certifications or accreditations to acquire them. Also, can third party service providers that the FIs already use currently be grand-fathered, as the FI would have assessed their track record over time?
		Comments on technology risk governance and oversight: Sec 3.6.2 ..the training programme should be conducted at least annually for all staff, contractors and service providers.. Comments: A more effective training programme should take into consideration role-based training requirements. E.g. for high-risk privileged users and specialised roles such as system developers and security administrators, the training focus and the content should be customised to their job

		nature as compared to those targeted for end-users. As such, we propose MAS to take this into consideration for this requirement.
		Comments on technology risk governance and oversight: 3.5.2 - Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who has access to the FI's data and systems, should be performed to minimise this risk. Comments: We agreed with MAS to view insider threat as one of the key risks and background check is a standard control used by FIs to address this risk. We seek clarification whether MAS is specifically concerned over personnel who have access to FI's critical data or system in the production and data recovery environment instead of the background screening performed for staff, contractors and service providers in general. This combined with a strong Operational Infrastructure Security framework (section 11) should minimise the risk of theft of confidential, sabotage of systems or fraud by staff, contractors or service providers. We also propose that for added clarity, background check should minimally cover past employment history, criminal records, bankruptcy and credit history of the personnel.
		Comments on technology risk governance and oversight: 3.5.2 Suggest that background checks on "service providers" be covered under the proposed revised MAS Outsourcing Guidelines Consultation Paper, as the coverage of third parties been extended as per revised definition of "outsourcing arrangement".

		Comments on technology risk governance and oversight: 3.6.1, 3.6.2 Suggest consistency be used in 3.6.1 - “all staff in FI”, “all personnel in FI” and 3.6.2 – “all staff, contractors and service providers”. For service providers, suggest that the same restriction on “information assets” be made as for 3.2.1, and to exclude third-party service providers – for third parties to be governed via the proposed revised MAS Outsourcing Guidelines, as per extended coverage of third-parties in the revised definition of “outsourcing arrangement”.
		Comments on technology risk governance and oversight: As a branch of a bank incorporated outside Singapore, can the roles and responsibilities of the “Board” in the proposed Consultation Paper be discharged by a member of the senior management or a management committee of the Branch in Singapore?
		Comments on technology risk governance and oversight: Comment: A comprehensive paper with overall proposed changes that are relevant to the current financial technology landscape and aligned to our objectives of ensuring a robust risk framework. *** 3.1.5. The board of directors or a committee delegated by it, is responsible for…: Comments: As the corporate governance structure may vary across different FIs, we request that MAS rephrase section 3.1.5 to allow the FI’s board of directors to designate/delegate relevant committees where necessary, instead of just one committee.
		Comments on technology risk governance and oversight:

		3.3.1 (b) classification of an information asset based on its security classification or criticality; Comments: We presumed MAS' reference of criticality of information asset is based on the definition of "critical system" in MAS Notice 644 Technology Risk Management. As for "security classification", we seek further guidance from MAS as this terminology may differ across different FIs.
		Comments on technology risk governance and oversight: Footnote 3 [page 11] 1.The Bank would like further clarity on the following: 1. Does data here refer to physical data, digital data, or both? 2. Do information assets include those that are hosted and/ or processed by service providers to facilitate their delivery of services to the FI? 3. Please provide some examples of information assets that meet this requirement --> "They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI" 2.The Bank suggests the below revisions, to give more clarity and better ringfence the requirement: "Information assets include data, hardware and software. Information assets are not limited to those that are owned by the FI. They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI. Adapted from CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures, June 2016." 3.3.1 (b) [page 12]

		The Bank suggests the following revision, for better clarity: "classification of an information asset based on its security information classification or system criticality;" 3.4.2 [page 12] The Bank would like further clarity on the following: 4. In view of this requirement around financial viability and track record which some start-up or Fintech companies may have challenges in meeting them, is MAS expecting that Bank should not engage any start-up or a Fintech company whereby we are unable to determine their financial viability, track record, etc? 5. Based on this requirement on service requirement, are FIs now expected to perform due diligence for non-standardised services such as power supply and telecommunication lines?
		Comments on technology risk governance and oversight: It is stated under paragraph 3.1.2 that MAS is proposing that both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. We would like to clarify if the Banks are required to demonstrate that the members possess such knowledge through any form of certification or past working experiences.
		Comments on technology risk governance and oversight: Management of Third Party Services The use of certain third party services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third

		party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks. ---------- Feedback ---------- Under some circumstances, the banks may not be able to audit 3rd party vendors for system-related risks, especially when they are the Big Tech. Suggest to amend the clause to : The use of certain third party services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third party. Hence, the FI should engage third party services that are suitably certified to meet various technology risks associated with the loss of data confidentiality, integrity and service availability.
		Comments on technology risk governance and oversight: Para 3.1.5 (d) of CP - This paragraph touches on the appointment of a Chief Information Officer, or Head of Information Security. We would like to check with MAS on whether this can someone with a regional or global role who sits in the local board or senior management team in the bank's SG entity?
		Comments on technology risk governance and oversight: Paragraph 3.1.5(d) – The remit of the Chief Information Security Officer should cover information security strategy and programme, and not just be limited to IT security strategy and programme. We propose that the guidelines be amended to read: "(d) appointing a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT information security strategy and programme".

		Paragraph 3.2.2 – We propose replacing the term "attendant risk" with "residual risk" for clarity and simplicity, as the latter term is more standard and widely understood. Paragraph 3.3.2 – The current guidelines at paragraph 4.1 make reference to "information system assets". With the proposed adoption of the term "information assets", could MAS clarify whether the requirement to inventory would then include logical aspects such as interfaces. Paragraph 3.4.2 – We would like clarification on whether there would be a list of relevant certification or accreditation considered to be "recognised by the industry". Further, it is unclear if this industry recognition refers to industry that the service provider is in, or the industry that the service recipient is in.
		Comments on technology risk governance and oversight: Paragraph 3.6.2 We are supportive of MAS' proposal to periodically reinforce security awareness of all staff, contractors and service providers who have access to the FI's information assets through a comprehensive IT security awareness programme. In general, we note that in larger organisations, a comprehensive awareness programme may consist of multiple components or modules, each focused on an individual section of the prevailing cyber threat landscape. We would like to suggest that instead of mandating the entire training programme be conducted at least annually, the Technology Risk Management Guidelines would enable FIs to define more granular approaches by tailoring the intensity and rigor of the programme to existing job roles and their expected exposure to particular threats in the prevailing threat landscape, thereby ultimately paving the way for increased effectiveness and efficiency of the overall programme. Based on an assessment, this may mean that

		certain programme components or modules are repeated more frequently than annually, less frequently, or perhaps not periodically at all, depending on the aforementioned expected exposure for the job role in question. 3.6.3 We would like to inquire whether it is MAS' intention to declare that this extension of the training programme to the Board of Directors ought to be managed under the same frequency as defined in paragraph 3.6.2. The last sentence "The training programme for the board of directors […]" seems to suggest that MAS is not principally opposing separate training programmes for the board of directors and other roles. This, however, is strongly correlated with our suggestion on allowing FIs to tailor the frequency to particular job roles as outlined above. 3.6.4 We see no correlation between currency and relevance of the training programme on the one hand, and effectiveness of the training programme on the other hand. Both highly effective as well as highly ineffective training programme components and modules can equally well be current and relevant. Therefore, to ensure the training programme remains current and relevant, which appears to be MAS' intended objective behind paragraph 3.6.4, a review of effectiveness is not strictly required. We would like to suggest to describe training programme effectiveness in a separate paragraph that stipulates that a periodic measurement and review of effectiveness is used to continuously improve the content of the training programme.
		Comments on technology risk governance and oversight: Point 3.4.1 Management of third party services The use of certain third party services by FIs may not constitute outsourcing. However, as many of these services

		are provisioned or delivered using IT or may involve confidential customer information being held by the third party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks Question : Any suggestive list or nature of services or activities that may not constitute IT outsourcing
		Comments on technology risk governance and oversight: Role of the Board of Directors and Senior Management Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which will include risks posed by cyber threats. ---------- Feedback ---------- It would be quite onerous for a person in the role of BOD to understand and manage technology risks. However, if this clause could not be removed, would suggest that to be consistent, the board of directors' additional role and responsibilities in understanding and managing technology risks should be inserted into the MAS Code of Corporate Governance (2018) instead of inside the new TRM.
		Comments on technology risk governance and oversight: Section 3.5 (Competency and Background Review) We seek clarification from the MAS regarding the precise level of competence and skills expected of relevant personnel for the purposes of performing IT functions and

		managing technology risks. We would be grateful for guidance from the MAS on how the level of competence and skills is to be assessed by the Bank at the outset (i.e. prior to engagement or employment) and maintained throughout the relevant period of engagement or employment. For example, would professional certifications, accreditations or awards, or the fulfilment of annual continuous professional development requirements, contribute towards meeting this competence standard? We would also be grateful for guidance from the MAS on the types of training programmes required to be conducted for IT personnel for the purposes of ensuring they have the requisite level of competence and skills to perform IT functions and manage technology risks. We seek clarification from the MAS in relation to the scope and nature of the background checks on personnel required to be conducted by the Bank. For example, we note that the MAS has published Guidelines on Fit and Proper Criteria for relevant persons who carry out regulated activities. In the same vein, we would be grateful if the MAS could provide specific guidance on the applicable criteria for such personnel for the purpose of conducting these background checks.
		Comments on technology risk governance and oversight: The bank is supportive of the MAS proposed TRM Guidelines on Technology Risk Governance and Oversight.
		Comments on technology risk governance and oversight: Under paragraph 3.5.2, MAS proposes a background check on personnel who have access to the FI's data and systems to minimise internal fraud. We would like to clarify if the FI can rely on the it's current ‘fit and proper’ assessment and also the vendor’s internal due diligence process on these personnel, in order to fulfil this background check requirement.

		Comments on technology risk governance and oversight: We are a wholesale bank in Singapore with a simple structure and not overly-complex business model. Our Head Office has a Cyber Security unit, which has been tasked by our board of directors to organise and coordinate cybersecurity roles and responsibilities within the bank, and covers overseas branches as well. This unit is responsible for establishing a cybersecurity framework and security strategy, overseeing risk assessment as well as the development of policies, standards, and procedures with regards to cyber security. Being a branch, we are required to adhere to any policies and procedures as well as implementing the necessary measures as prescribed by this unit. If that is the case, does MAS expect the appointment of a Chief Information Security Officer at the branch level?
		Comments on technology risk governance and oversight: We noted that the definition of "information assets" is revised to the following under paragraph 3.2.1: "Information assets include data, hardware and software. Information assets are not limited to those that are owned by the FI. They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI." We would like to clarify if the definition of "information assets" can stay unchanged as "data, systems, network devices and other IT equipment" or be slightly changed to "data, hardware and software owned by the FI".
		Comments on technology risk governance and oversight: We noted the following requirement under paragraph 3.3.1: "To have an accurate and complete view of its IT operating environment, the FI should establish an information asset

		management framework that includes the following: (b) classification of an information asset based on its security classification or criticality;” We would like to clarify the difference between security classification and criticality.
		Comments on technology risk governance and oversight: We refer to Paragraph 3.4.2 of the Consultation Paper on TRM Guideline on proper due diligence on service provider. In this regard, we would like to check if FI's reliance on service provider’s external audit reports or certification (such as ISO27001, ISAE/SSAE reports, SOC reports) will be sufficient to fulfil this requirement? In addition, given that such third party service providers may not provide critical services or access confidential data, we propose that the need for an assessment commensurate with the risk level of such services.
		Comments on technology risk governance and oversight: With reference to 3.5.1, please define the scope of "Service Providers" in the requirement for assessment of whether personnel have the requisite level of competence and skills, or for background checks. For 3rd party services (including outsourcing), it may be a challenge to obtain information of the competence level or background checks of individuals involved in the provision of the service.
		Comments on technology risk governance and oversight: With reference to 3.6.2, please define the scope of "Service Providers" in the requirement for training programmes to be conducted. For 3rd party services (including outsourcing), it may be a challenge to conduct training for individuals involved in the provision of the service.
		Comments on technology risk governance and oversight: With regard para 3.1.6.c, we would like to seek

		confirmation that RACI is not mandatory. Banks should be provided flexibility in terms of demostrating compliance in other forms that are more appropriate considering the bank's business operations and set-up.
		Comments on technology risk governance and oversight: Would the development of the training requirements for delivery to Board members be at the discretion of the FI? Could this will be distinct and separated from the company wide training program?
		General Comments: For implementation, transition period of 24 months should be given due to potential system/ applications changes/ implications.
		General Comments: General comments: • Given that the revised BCM guidelines has a 1 year transition period, we would be grateful if the authority will also apply a similar 1 year transition period for FIs to adopt the changes in the revised TRM guidelines. • As it is practically difficult to find Board members who have the requisite in-depth knowledge of evolving cyber-security and information technology threats & counter-measures, most FIs would establish committees under the Board that comprises senior employees with the requisite knowledge. Such committees would work with stakeholders to ensure that risk appetite thresholds and related measurement criteria addressing emerging technological and cyber risk exposures are implemented to give the Board comfort. At such, we would like to clarify if the authority allows the Board to delegate IT and cyber oversight to a separate committee.
		General Comments: Overall Feedback:

		1. We note the the guidelines attempt to encourage adoption of certain emerging technologies. We recommend a less-prescriptive approach to allow FIs flexibility to determine the appropriate technologies that best meet their respective business needs. 2. We recommend the guidelines to be less-prescriptive and allow FIs the flexibility to research and determine the appropriate guidelines, controls and frequency respective FIs deem appropriate for their organisation, taking a risk-based approach.
		General Comments: The Bank would like to understand how a clause that uses "should" compared to a clause that uses "could" or "could consider" should be interpreted.
		General Comments: The bank do not have any other aspects of TRM that warrant further guidance from MAS.
		General Comments: We noted that the proposed revisions to Technology Risk Management Guidelines are significant. For example, many control requirements are extended to FI's service providers. In order to ease the FI's compliance process against the revised Technology Risk Management Guidelines to be published, we would like to suggest that other relevant guidelines from ABS are updated concurrently to address MAS' new requirements, such as "Guidelines on Control Objectives & Procedures for Outsourced Service Providers"
		General Comments: We would like to enquire from MAS as to whether the proposed revised TRM guideline has taken into consideration the development of API Marketplace requirements?

		General Comments: We would like to request that MAS specify the implementation timeline for the proposed guidelines, as some measures may require significant adjustments to the current processes. We would also like to propose that FIs be allowed to stagger the implementation process according to its own risk-based prioritisation as opposed to single hard deadline when the guidelines become effective.
		General Comments: We would like to understand the expected transition time for complying with the revised Technology Risk Management Guidelines. The FI may require a necessary period of time to achieve full compliance with the significantly revised requirements.
		General Comments: Are the TRM Guidelines expected to be applicable to the following categories? i. Overseas branches and subsidiaries of FIs that provides financial services ii. Overseas subsidiaries of FIs that provides services to FIs. iii. Overseas subsidiaries of FIs that provides non-financial services. iv. Singapore based subsidiaries of FIs that provides non-financial services.
		General Comments: As there are other consultation papers currently under review for Outsourcing and Business Continuity Management Guidelines, we recommend that these requirements are not to be duplicated in the TRM Guidelines.
		General Comments: In addition, some initiatives require extensive implementation across the FI, e.g. web isolation. We

		request for the implementation grace period for this revised TRM Guidelines be a minimum of 24 months from the issuance date.
		General Comments: We support MAS' direction in strengthening controls, in particular, in monitoring and detection of cyber security events. However, as not all the FIs may be in the same state of readiness, e.g. in user-behavioural analytics and IOT security, we recommend that more time be given for the development in this space. It would be good for industry guidelines or standards be developed first prior to having these requirements in the TRM Guidelines.
		Comments on IT service management: <7.4.2> With reference to the definition of "information assets" under footer note 3 which include data, hardware and software, we would like to seek clarity whether it is MAS' intent for FIs to apply patches on "data" as patches cannot be applied to data. Hence, we would like to request for MAS to exclude "data" for this requirement.
		Comments on IT service management: 7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g., fixes for security vulnerabilities and software bugs are implemented within a timeframe that is commensurate with the criticality of the patches to the FI's systems. Comments: Apart from just considering criticality of patches when prioritising patch deployment, we would propose for FIs to also include the security classification and asset placement of the FI's systems (e.g. critical and internet-facing systems) which would increase the risk exposure of exploitation for unpatched systems. Please see suggested edits below:

		"7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with patch criticality and in accordance to security classification and asset placement of the FI's systems." *** 7.4.2 All patches should be tested before they are applied to the information assets in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system. Comments: We agreed that testing of patches is necessary before being applied on production systems. The definition of 'Information asset' is too wide under Page 11 as it covers customer-owned and third-party systems of which FI does not have access to their production environment to perform verification. As such, we propose the suggested edits as below: "7.4.2 All patches should be tested before they are applied to the FI's systems in the production environment..'
		Comments on IT service management: 7.2.1 [page 26] The Bank would if the "hardware and software" include network devices such as firewalls and routers.
		Comments on IT service management: 7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g., fixes for security vulnerabilities and software bugs are implemented within a timeframe that is commensurate with the criticality of the patches to the FI's systems.

		Comments: Apart from just considering criticality of patches when prioritising patch deployment, we would propose for FIs to also include the security classification and asset placement of the FI's systems (e.g. critical and internet-facing systems) which would increase the risk exposure of exploitation for unpatched systems. Please see suggested edits below: "7.4.1 A patch management process should be established to ensure functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with patch criticality and in accordance to security classification and asset placement of the FI's systems." *** 7.4.2 All patches should be tested before they are applied to the information assets in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system. Comments: We agreed that testing of patches is necessary before being applied on production systems. The definition of 'Information asset' is too wide under Page 11 as it covers customer-owned and third-party systems of which FI does not have access to their production environment to perform verification. As such, we propose the suggested edits as below: "7.4.2 All patches should be tested before they are applied to the FI's systems in the production environment..'
		Comments on IT service management: 7.5.3 Please clarify if testing and user sign off requirement is for application only or including infrastructure changes

		(i.e. router/switch/Firewall, DNS, etc) We would like to highlight that testing infrastructure change in test environment is not always practical and could be inefficient for infrastructure changes for some minor and low risk changes such as Firewall and DNS changes. Hence would proposed for MAS to consider a tiered approach for minor and low risk infrastructure changes.
		Comments on IT service management: 7.5.4 For business management representation on the Change Advisory Board, we request to add designated Technology and Operations function representatives whose role is to addresses business requirements and have the requisite technology skills and knowledge to participate effectively at the Change Advisory Board.
		Comments on IT service management: 7.5.7 Please clarify or provide precise guideline how to ensure the logging facility is enabled to record activities. Would be grateful if MAS can clarify if there is an expectation that each change activity includes a step to verify the activities are received into logging facilities?
		Comments on IT service management: 7.6.1 Based on the contents of citation 9.1.1 where it is stated “access to information assets so that no one person has access to perform critical system functions” and as pointed out in our general comments about SW development practices we would request for the inclusion of clauses about encouraging FI to reduce risk by automating DevOps practices. For example, how is this to be applied with teams adopting automated testing, automated deployments, and human reviews of all code destined for production? Alternatively, additional guidance around what constitutes the types of

		environments are in scope for "one environment to another" is this UAT to Prod?
		Comments on IT service management: 7.7.2 MAS proposed that as part of its incident management framework, the FI should identify and engage the external assistance that it needs to augment its resources to manage IT incidents. This is to ensure sufficient resources are available to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber-attack investigation, and provide 24/7 incident response capability. Please clarify that expectations re external assistance.
		Comments on IT service management: 7.7.4 We propose to confine the requirement for system events or alerts to be configures to provide early indication of system performance, availability and security issues to critical systems as defined under MAS Notice 644, as it would have taken into consideration the severity of the impact to customers, business operations and the bank's reputation.
		Comments on IT service management: 7.8.2 As this is a "good practice" for lessons learnt from past incidents, we propose to move this to an Annex for "good practice" reference instead of making it as a mandatory requirement.
		Comments on IT service management: Incident Management As part of its incident management framework, the FI should identify and engage the external assistance that it needs to augment its resources to manage IT

		incidents. This is to ensure sufficient resources are available to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber-attack investigation, and provide 24/7 incident response capability. ---------- Feedback ---------- Suggest to have broader definition of "external assistance" to include vendors or head office resources.
		Comments on IT service management: Para 7.5.3 We are supportive of MAS' proposal to ensure that all changes are adequately tested. However, we would like to see that sufficient alternatives to performing testing in the test environment are not ruled out. In our view, the critical consideration should be that testing is not performed in the production environment, regardless of the labeling or naming of the environment where such testing occurs. Therefore, we would like to propose that "in the test environment" is replaced with "outside the production environment". We would like to propose to replace "test plans" with "test methodology", similar to our earlier comment on paragraph 5.7.1. We would like to propose to replace "test plans" with "test methodology", similar to our earlier comment on paragraph 5.7.1. In line with contemporary Agile software development methodologies, we note that it is highly unusual that test results are accepted and signed off by users, especially when the group of users consists of external customers, is very large or highly dynamic in composition. This is not to

		say that the voice of the customer is not important – we would like to emphasize that we are in full support of business strategies based on customer intimacy or customer excellence, especially in a digital era where business success is predicated on building primary relationships with customers. Rather, in our view the current industry best practice for accepting changes before deployment to production is to have this performed by the business asset owner, (Scrum) product owner, or other company representative or delegate with sufficient understanding of customer expectations. We would like to suggest that, instead of requiring users to sign off on test results, such sign off can be performed by a business representative with sufficient understanding of customer expectations. 7.5.5 We recognize that recovery strategies are crucially important to safeguard the continuity of business processes and functions in the face of business or IT change. However, we feel that a general mandate to perform a backup of the information asset before every change unduly prevents FIs from selecting superior recovery strategies where available. For example, applications with a stateless design (such as is very common in a service-oriented architecture or micro-services architecture) benefit from a simplified recovery strategy since they can be recreated by redeploying an artefact (possibly after recompiling and/or rebuilding source code) without restoring any backup. Therefore, we would like to recommend that paragraph 7.5.5 is rephrased in terms of defining and applying a (demonstrably effective) recovery or rollback strategy, which may or may not be based on backup technology, depending on the technology platform or stack in question. 7.5.7

		We appreciate that MAS' seeks to emphasize that audit and security logs contain useful information which facilitates investigations and troubleshooting. However, the precise mechanism to realize the general existence and availability of log files may vary from system to system, and may not be fully known when dealing with closed source applications and libraries. Therefore, the requirement to "ensure the logging facility is enabled" is in our view too specific and draws attention away from the goal of ensuring that log files exist and are made available. Therefore, we would like to recommend to rephrase the second sentence to "As such, the FI should define and implement logging requirements to record activities that are performed during the change process". 7.6.1 / 7.6.2 We are not familiar with the term "software codes" as a widely recognized industry term to refer to software artefacts being promoted from one environment to another. We would like to suggest to universally replace "software codes" with "source code, byte code and/or binaries". This has the added benefit of abstracting over the difference between compiled and interpreted programming languages, which is a debate to be avoided in this context. This also better aligns with the terminology used in Annex A, sub A.2(a). 7.6.1 We are supportive of MAS' intention to require a certain degree of segregation of duties in the software release process. However, as also stated under paragraph 6.3.2, we note that with increased automation, specifically automation of security verification and testing, the focus of such segregation of duties shifts to mitigating internal fraud risk through the deterrence of introducing malicious logic in production environments, as this is a notoriously difficult to

		mitigate risk area in an automated way. We feel that "segregation of duties in the software release process" imposes a general standard of practice that draws required attention and focus away from sensitive operations such as promoting releases to production environments. In our view, segregation of duties should restrict itself to promotion of artefacts from non-production to production environments, as also stated in paragraph 7.6.2. This is further strengthened by adherence to the principle of separation of environments (as defined in paragraph 5.7.3).
		Comments on IT service management: Paragraph 7.8.2 – While we agree that a record of all past incidents should be kept, practically there would only be "lessons learnt" from significant incidents. We propose making this clearer in this paragraph.
		Comments on IT service management: The bank is supportive of the MAS proposed TRM Guidelines on IT Service Management.
		Comments on IT service management: We noted the following requirement under paragraph 7.7.2: "As part of its incident management framework, the FI should identify and engage the external assistance that it needs to augment its resources to manage IT incidents." We would like to clarify if "the external assistance" is still required even if the FI has adequate resources to manage IT incidents.
		Comments on IT service management: 7.2.2 [page 26] The Bank suggests the replacement of "information assets"

		by "hardware and software" for clarity as data has no configuration information. Please see proposed revised version below: "The FI should review and verify the configuration information of its information assets hardware and software on a regular basis to ensure they are accurate and kept up to date."
		Comments on IT service management: 7.3.2 [page 26] The Bank suggests the replacement of "dispensation" by "deviation" to be consistent with clause 3.2.2. Please see proposed revised version below: "… The FI should obtain dispensation deviation approval from its management for the continued use of outdated and unsupported systems."
		Comments on IT service management: 7.4.2 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity as patching in this case may not apply to "data": "All patches should be tested before they are applied to the information assets hardware and software in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system."
		Comments on IT service management: 7.5.1 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity and applicability:

		"The FI should establish a change management process to ensure changes to information assets hardware and software are assessed, tested, reviewed and approved before implementation."
		Comments on IT service management: 7.5.2 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity and applicability: "… The analysis should cover factors such as security and implications of the change in relation to other information assets hardware and software."
		Comments on IT service management: 7.5.4 [page 27] The Bank would like to understand if the business representative be appointed from IT by Business to sit in the Change Advisory Board as a key stakeholder.
		Comments on cyber security assessment: <13.3> Presently, cyber exercise is one of the key scenario in the bank's annual BCP exercise. In this regard, we would like to seek clarity whether it is MAS' intent for FIs to separate the two exercises? We respectfully request for MAS to allow FIs to combine the two exercises for purpose of economics of scale. <13.4 & 13.5> Given both paragraph 13.4 and 13.5 are on the topic of Adversarial Attack Simulation, we would like to suggest, in our view, to subsume paragraph 13.5 Intelligence-Based Exercise under paragraph 13.4 Adversarial Attack Simulation Exercise.

		Comments on cyber security assessment: 13.1.2 When performing system VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, as well as applications and services that are not approved by business, IT management and other key stakeholders. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities, such as SQL injection and cross-site scripting. Comments: Vulnerability assessment is unable to identify / assess legitimacy of running applications and services. As such, we would like to propose the following suggested edits: "13.1.2 While performing system VA, the scope should minimally include… identification of weak security configurations and open high-risk network ports and services. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities, such as SQL injection and cross-site scripting." 13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment. Comments: For better clarity to the requirement as well as consistency to the ABS Penetration Testing Guidelines document, we would like to propose the following suggested edits with reference to the ABS Penetration Testing Guidelines: "13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment. However, should the nature of the test be intrusive which may result to an outage, a PT can be conducted in UAT or Pre-Production environment."

		13.5.1 To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on real cyber incidents. Comments: For better clarity to the requirement, we would recommend MAS to provide footnote on “red team” by drawing reference to the ‘ABS Guidelines for the Financial Industry in Singapore, Red Team: Adversarial Attack Simulation Exercises’.
		Comments on cyber security assessment: 13.1.2 [page 48] The Bank would like to understand if "service" refers to a system process. 13.2.2 [page 48] The Bank would like to highlight that such programme may result in potential concerns over confidentiality and trust of the customers. 13.2.3 [page 48] The Bank suggests the following revision: "To obtain a more accurate assessment of the robustness of the FI’s security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment. However, should the nature of the test be intrusive or intensive and may result in the possibility of an outage, the specific test could be conducted against the UAT/Pre-Production environment." 13.5.1 [page 50] The Bank suggests changing from "based on real cyber incidents" to “based on major reported incidents”, as there are insufficient details in the open on the factuality of real cyber incident. Please see proposed revised version: “To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed

		and based on real cyber incidents major reported incidents.”
		Comments on cyber security assessment: 13.1.2 We welcome MAS’ positioning of VA as a process to conduct regular vulnerability assessments on the FI’s systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. We note that, specifically for web-based systems, the required checks on common web-based vulnerabilities as stated in paragraph 13.1.2 are in practice already covered by DAST as outlined in paragraph 6.1.4. To help limit redundancy, we propose to remove the last sentence in paragraph 13.1.2, or, alternatively, refer to DAST as described in paragraph 6.1.4.
		Comments on cyber security assessment: 13.1.2 We propose that the scope of “system” VA be confined to critical systems, web-based and internet-facing ones.
		Comments on cyber security assessment: 13.2 Penetration Testing • PT may not necessarily provide in-depth evaluation of security posture, rather helps in identifying gaps in cybersecurity defences. Suggested wordings below. 13.2.1 The FI should carry out penetration testing (PT) to identify gaps in cybersecurity defences of its IT environment. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT. • The guideline may lead to significant risk to FI and we recommend this to include production-like environment as well. The production-like environment should have similar

		hardware/software/application configuration as that of Production. Suggested wordings below. 13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production or equivalent production-like environment. Proper safeguards should be implemented when PT is conducted on the production environment.
		Comments on cyber security assessment: 13.2.3 It would be useful to get more clarity on the extent to which PT is expected in production environment. Could it be done on limited systems or is the expectation to cover all key systems in production environment?
		Comments on cyber security assessment: 13.2.3 Unlike Technology firms and product development firms, FIs may find it challenging to offer bug-bounty programmes on their infrastructure, and manage the associated process. Can this requirement be re-assessed or clarified further in terms of expectations
		Comments on cyber security assessment: 13.3.1 Please clarify "regular" scenario-based cyber exercises and allow the FIs flexibility to define their expected frequency to carry out such exercises.
		Comments on cyber security assessment: Para 13.3.1 of CP – We would appreciate it if MAS could clarify on its expectations on the scope and frequency of local cyber exercises. In addition, we would like to check whether enterprise led exercises with local participation, rather than local exercises, could be used to fulfil the requirements under this paragraph.
		Comments on cyber security assessment: Para 13.3.1 of TRM Guidelines – We would appreciate it if MAS could clarify on its expectations on the scope and

		frequency of local cyber exercises. In addition, we would like to check whether enterprise led exercises with local participation, rather than local exercises, could be used to fulfil the requirements under this paragraph.
		Comments on cyber security assessment: Point 13 Cyber security assessment Point 13.2.2 Penetration Testing A bug bounty programme is another mean by which an FI could discover vulnerabilities in their systems by inviting and incentivising ethical or "white hat" hackers to test their systems. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT. Question Can the Bank consider alternatives to the Bug bounty programme to increase its coverage of testing their systems and discovering vulnerabilities?
		Comments on cyber security assessment: The bank is supportive of the MAS proposed TRM Guidelines on Cyber Security Assessment.
		Comments on cyber security assessment: We refer to Paragraph 13.2 and would like to clarify if the go live condition can be based on penetration testing results in a non-production environment such as UAT for new or enhanced system rollouts.
		Comments on cyber security assessment: We refer to Paragraph 13.2.2 and would like to feedback that bug bounty program has down sides in regards to public communication of potential bugs. Hence, we suggest that MAS considers whether this is the most appropriate

		method for FIs.
		Comments on cyber security assessment: With respect to the recommendation on carrying out regular scenario-based cyber exercises, the Bank would like to seek clarity whether participation in industry-wide (financial services sector) business continuity exercise could be considered as part of the cyber exercise road map for the Bank (this is subject to whether the scenarios testing during the said exercise is per the intended scenario testing planned by the Bank for the year).
		Comments on access control: 9.1.1 and 9.1.5 We suggest avoid using the term "critical system functions" to avoid confusion with "critical system" as defined under MAS Notice 644.
		Comments on access control: 9.1.1 The Bank suggests that the words underlined be added: "The principles of 'never alone', 'segregation of duties', and 'least privilege' should be applied when granting staff access to information assets so that no one person has access to perform all critical system functions."
		Comments on access control: 9.1.1 Access rights and system privileges should be granted according to the staff's role and job responsibilities. Comments: Apart from staff, the requirement should also apply to contractors. Please see suggested edits below: "9.1.1 Access rights and system privileges should be granted according to the staff's and contractors' role and job responsibilities."

		Comments on access control: 9.1.2 …. Access rights should be authorised and approved by the information asset owner". Comments: Line manager is accountable to ensure that staff is granted with user access relevant to his/her role and responsibilities. Please see suggested edits below to capture such accountability. "9.1.2 ..Access rights should be authorized and approved by information asset owner and user's line manager."
		Comments on access control: 9.1.6 The FI should ensure information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. Comments: Information asset owners are not in a position to determine appropriateness of user access e.g. internal transfer, redeployment by line manager to perform different functions, etc. The appropriate party should be the line managers instead. Please see suggested edits below. 9.1.6 The FI should ensure line managers perform periodic user access review to verify the appropriateness of privileges that are granted to their staff and contractors.'
		Comments on access control: 9.1.7 The FI should ensure users are granted system access rights on a need-to-use basis. Existing access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly. Comments: We request minor edits as suggested below for better clarity: "9.1.7 The FI should ensure users are granted system access rights on need-to-use basis. Existing access rights that are

		no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment) should be revoked or disabled promptly. "
		Comments on access control: 9.2.1 Users granted with privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Comments: As not all privileged users will end up abusing their privileged accesses, we would like to suggest the edits below: "9.2.1 Users granted with privileged system access have administrative privileges to support and manage changes in FI's IT environment."
		Comments on access control: 9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. Comments: FI cannot harden employee-owned personal mobile devices used for remote access, hence BYOD security policy applies. As such, we propose to draw reference to the Annex B in the draft consultation paper. Please see below suggested edits: "9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to the FI's security standards. For personal-owned mobile devices, please refer to Annex B: BYOD Security."
		Comments on access control: 9.1.1 [page 36] The Bank suggests, for clarity, the use of the definitions used (e.g. "never alone") under section 11.0.1 of the 2013

		TRMG.
		Comments on access control: 9.1.2 & 9.1.6 [page 36 and 37] The Bank would like further clarity on who should be the actual authorisers and approvers as there are differences in responsibilities between system owners and data owners. Typically access rights are approved by the application or system owner.
		Comments on access control: 9.1.3 [page 36] The Bank would like to understand if the user access refers to end/business user access or administrator access.
		Comments on access control: 9.1.5 [page 36] 1. The Bank would like further clarity on the difference between Critical system and critical system function? Can this be limited to Critical System instead of Critical System Function? 2. Further elaboration on the definition of critical system function will be appreciated. Please cite examples.
		Comments on access control: 9.1.8 [page 37] "The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel." The Bank would like to understand if this applies to all 3rd party service subscriptions regardless of materiality and nature of service subscribed.
		Comments on access control: 9.1.5 If standalone workstations not connected to Internet are

		used to access critical system functions, is multi-factor authentication still required?
		Comments on access control: 9.1.5 "Multi-factor authentication should be implemented for users with access to critical system functions to safeguard the systems and information from unauthorised access" Is this is referring to the bank user or the customer user ?
		Comments on access control: 9.1.6 The Bank suggests to replace the words “incorrectly provisioned access rights” with “inappropriate access rights”
		Comments on access control: 9.2.2 The Bank suggests that a risk based approach based on asset criticality framework be adopted.
		Comments on access control: 9.3.2 As remote access can be done via BYOD, e.g. mobile phones, the devices will not be hardened according to the FI’s security standards. This should be clarified this section does not cover remote access via BYOD which will be covered under Annex B – BYOD Security.
		Comments on access control: Clarification on paragraph 9.1.3 of the Consultation Paper We would like to clarify what the user access and management activities logs retention period is.
		Comments on access control: Clarification on paragraph 9.2.1 of the Consultation Paper We would like to clarify what the privileged accounts access logs retention period is.

		Comments on access control: Proposed amendment to paragraph 9.3.2 of the Consultation Paper The FI should ensure remote access to the FI's information assets is only allowed from devices that have been hardened according to meet the FI's security standards. Justification: Annex B: BYOD Security in the Consultation Paper allows the use of personal mobile devices e.g. mobile phones and iPads through MDM controls, as well as allows on-demand remote access from personal computers as long as the FI information is accessed remotely and the data is not downloaded to the personal devices.
		Comments on access control: Para 9.3.2 of CP – We would like to clarify whether this is requirement is meant to imply and prohibit the use of personal/non corporate managed device and Virtual Desktop Infrastructure (VDI) solution? If so, this may potentially impact Business Continuity Management Plans if FI relies on remote access via home desktops or personal smart devices.
		Comments on access control: We would like to seek MAS' clarification on whether VDI (Virtual Desktop Infrastructure), where remote access is facilitated via an intermediate, fully FI controlled (locked down to the end user), desktop interface, is considered a sufficient implementation of paragraph 9.3.2.
		Comments on access control: Paragraph 9.1.1 – The principles of principles of 'never alone', 'segregation of duties', and 'least privilege' are not universally applicable to all applications. We propose that this paragraph need only provide as follows "The principles of 'never alone', 'segregation of duties', and 'least privilege' should be applied when granting staff access to information assets so that no one person has access to perform critical

		system functions. Access rights and system privileges should be granted according to the staff's role and job responsibilities."
		Comments on access control: Paragraph 9.1.6 – The performance of periodic user access reviews need not necessarily be done by the asset owners – as long as proper checks and approvals are in place, we propose that the FI have the flexibility to assign such reviews to other appropriate parties.
		Comments on access control: Paragraph 9.1.8 – We would be grateful for some guidance from MAS on the expected level of monitoring of the FI's own personnel.
		Comments on access control: Paragraph 9.2.2 – The scope of this paragraph would be clearer if "system" and "service accounts" were defined.
		Comments on access control: Paragraph 9.3.2 – We would like to raise for MAS' consideration that differing security standards and setups can be catered for under this paragraph. Technology such as mobile device management for BYOD secures the FI's data and access to the FI's environment, regardless of the underlying security standard of the devices.
		Comments on access control: Point 9 Access control 9.1.5 User access management Multi-factor authentication should be implemented for users with access to critical system functions to safeguard the systems and information from unauthorised access.

		Question Any criteria or suggestive list by the regulator to identify critical system functions. There might be also technical challenges and product limitations in implementing multi-factor authentication for all applications.
		Comments on access control: The bank is supportive of the MAS proposed TRM Guidelines on Access Control.
		Comments on access control: This section is for FI user access control and not for customer. 9.1.1 - What is the definition and scope of 'never alone'? Is that maker/checker or that staff should be supervised at all times for based on risk. 9.1.2 "The FI should establish a user access management process to provision and revoke access rights to information assets. Access rights should be authorised and approved by the information asset owner or delegate." Comment: add "delegate" 9.1.6 "The FI should ensure information asset owners or delegates perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as incorrectly provisioned access rights. Exceptions noted from the user access review should be resolved as soon as practicable." Comment: Add delegate" 9.3.1 - Should BYOD email such as Blackberry be classified as remote access assets since they do not have access to internal networks? 9.3.2 - Virtual Devices (e.g., VDI) that are accessed through secure channels including from BYOD should be allowed.

		Comments on access control: With regard to para 9.1.4, we would like to suggest that password controls, as indicated in footnote 18, do not apply to multi-factor authentication where one of the factor is based on what the user knows (i.e. pin/ password). In fact, paraphrase has been recommended in the US, and we would like to suggest that this is also considered as an alternative of strong password control.
		Comments on access control: With regard para 9.3.2, we would like to sugggest that alternative controls such as remote access solution via VDI/ Citrix/ harderned sandbox solution are acceptable as well. Hardening of BYOD may not always be feasible.
		Comments on access control: Para 9.3.2 of TRM Guidelines – We would like to clarify whether this is requirement is meant to imply and prohibit the use of personal/non corporate managed device and Virtual Desktop Infrastructure (VDI) solution? If so, this may potentially impact Business Continuity Management Plans if FI relies on remote access via home desktops or personal smart devices.
		Comments on technology risk management framework: <3.2.1> We would like to seek clarity from MAS as to whether information assets under third party vendors (e.g. power supply vendors, cloud service provider and etc.) will fall within scope of the definition of "information assets", specified in footer note 3. <3.4.1> We would require MAS's guidance on how robustness and comprehensive the assessment should be. Technically if it is not classified as outsourcing, there should be minimal or zero data flow. We would like to request for some examples or best practice for review.

		<3.4.2> We would require MAS's guidance as to how comprehensive the due diligence should be. Are world check (include negative news screening) and registration of company names search sufficient? We would like to request for some examples or best practice for review.
		Comments on technology risk management framework: 3.5.2 Initial checks are performed by vendors or managed service providers at the onboarding stage. However, if there is no follow-up check then this insider threat risk potential goes unchecked for a number of years. We propose for MAS to consider setting an additional requirement for regular background checks.
		Comments on technology risk management framework: 3.6.1 Foundational training and awareness on Technology and Information Security risks and policies should be a requirement for all staff within an FI. However, more detailed and focused trainings around laws/regulations and technical aspects should be targeted only at staff in specific IT roles such as developers, administrators, asset owners, security officers and risk managers etc. A requirement to carry out such detailed training for all staff in a FI would not significantly reduce risk and may be counter-productive in diluting depth of training in order to deliver breadth. We therefore propose that MAS considers recommending appropriate levels of training based on roles and responsibilities of staff.
		Comments on technology risk management framework: 4.1.2 Who does the "risk owner" refer to -- would it be the owner of the business application or the technology team responsible for fixing the risk issue? What is meant by "authority to manage technology risks"?

		Comments on technology risk management framework: 4.2.1 FIs cannot directly identify or manage threats, vulnerabilities and risks faced by information assets owned by their service providers. They can have governance and mechanisms in place to monitor and assess service providers' policies, controls and risk management practices. The guideline should be refined to reflect this more clearly.
		Comments on technology risk management framework: 4.2.1 Please define and provide examples of "other dependent third parties" referred on footnote 7
		Comments on technology risk management framework: 4.2.2 - "Security threats such as internal sabotage, malware, data theft and "unauthorized financial transactions" could have a severe impact on an FI and its stakeholders." It may not be feasible for the Technology Risk Management Group ("TRMG") to be monitoring unauthorised financial transactions, there are other control groups that will be monitoring such transactions. Perhaps, monitoring "unauthorised access" may be a more meaningful and relevant an exercise for TRMG.
		Comments on technology risk management framework: 4.2.2 We recognize MAS' concern about security threats such as internal sabotage, malware, data theft and unauthorized financial transactions, and their potential severe impact on an FI and its stakeholders. We note that paragraph 4.2.2 is part of section 4.2, the Risk Identification phase of the technology risk management framework as defined in paragraph 4.1.3. In this light, we would suggest to further clarify or reword the potentially ambiguous term 'monitoring' in the context of risk identification in order to maintain a sound

		separation of risk identification from risk monitoring as described in paragraph 4.5. While we recognize MAS' concern about security threats such as internal sabotage, malware, data theft and unauthorized financial transactions, we note that these four specific threats should already be included in the threat identification phase as described in paragraph 4.2.1. Our concern is that an overly specific focus on these four threats will draw the required attention away from other prioritized threats obtained from threat identification as described in paragraph 4.2.1. We would like to propose that this paragraph is either replaced to state that the FI should be vigilant in monitoring all identified and prioritized security threats that have a severe impact on the FI and its stakeholders, or that the paragraph is removed altogether, depending on how MAS decides to respond to our previous comment on paragraph 4.2.2 as stated above.
		Comments on technology risk management framework: 4.4.7 The guideline suggests that all residual/accepted risks should be formally endorsed by the senior management. We request that FIs should be permitted to follow a tiered approach whereby residual risks within an FI's risk appetite and beyond a pre-defined threshold require senior management endorsement and monitoring, while those falling below the threshold would not be required to be endorsed nor monitored by senior management.
		Comments on technology risk management framework: 4.5.2 We would be grateful for guidance on the minimum requirements for a risk register to facilitate the monitoring and reporting of technology risks.
		Comments on technology risk management framework: 4.5.3 To facilitate risk reporting ….FI could consider risk

		events and audit observations, as well as refer to regulatory requirements. Comments: We request minor edits suggested below for better clarity: "4.5.3 To facilitate risk reporting ….FI could consider risk events and audit observations, and applicable regulatory requirements."
		Comments on technology risk management framework: Sec 4.4.1.. For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of information assets, level of risk tolerance. Sec 4.5.3.. To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure… Comments: Business criticality determines the information asset's availability requirements which has to be considered when developing and implementing risk mitigations and control strategies. We suggest that para 4.4.1 and para 4.5.3 be amended to include the criticality of service as follows. 4.4.1 - For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of information assets, level of risk tolerance and the criticality of service. 4.5.3 – To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure, and those that support business critical service. ***

		4.4.5 The FI should refrain from implementing a system or acquiring an IT service where threats to the safety and soundness of the FI cannot be adequately controlled and the risks out-weigh the benefits. Comments: We agreed with MAS that a risk assessment should be conducted before implementing a system or acquiring an IT service. If the residual risk exceeds the FIs' risk appetite or tolerance limit, then the FI should refrain from implementing the system or acquiring the IT service. As such, we would like to propose the following edits to be more aligned to section 4.3: "The FI should refrain from implementing a system or acquiring an IT service that falls outside FI's risk appetite or tolerance limit."
		Comments on technology risk management framework: Section 4 of CP – For greater clarity and to implement a robust IT governance model, would MAS consider to state the roles and responsibilities of the three lines of defence?
		Comments on technology risk management framework: Section 4.5 (Risk Monitoring, Review and Reporting) We seek clarification from the MAS regarding the specific types of technology risk metrics that are required to be developed by the Bank to facilitate risk reporting to management. We would be grateful if the MAS could provide guidance on the technology risk metrics to be developed, and whether there is a market or industry standard that may be used (or adapted for use) by all FIs.
		Comments on technology risk management framework: Suggest rewording to make it more clear: The FI should identify the threats and vulnerabilities, as well as the risks

		posed to its IT environment. The risks posed to information assets that are maintained or supported by third party service providers should be assessed in an appropriate way.
		Comments on technology risk management framework: Under S3.3, MAS is proposing to extend the obligations on FIs to manage information assets (data, hardware and software) to include those used by non-outsourced service providers to deliver services to banks Banks are unable to directly manage risks and safeguard information assets owned by their service providers. We recommend that MAS amends the requirement to focus on appropriate governance and mechanisms to monitor and assess service providers' policies, controls and risk management practices. Similarly, it is not possible for banks to obtain a complete view, and maintain an inventory, of all information assets held by third party providers.
		Comments on technology risk management framework: Under S3.4, MAS is proposing to extend the requirement to conduct due diligence and to assess and manage technology risks relating to non-outsourced service providers and their services to include utility providers and FMIs. Banks may not be in a position to be able to meet this requirement due to the nature of non-outsourcing arrangements with third party providers. In the case of dominant market providers, it is important to recognize that banks may not be in a position to directly assess risks and may need to rely upon provider-assessed and third party audits and reports. It is reasonable for banks to place some degree of reliance upon services provided by regulated entities. Echoing the comments in connection with management of information assets, we recommend that MAS amends the

		requirement to focus on appropriate governance and mechanisms to monitor and assess service providers' policies, controls and risk management practices.
33.	Transamerica Life Bermuda Ltd	Comments on operational infrastructure security: For 11.3.6, we would like to clarify "application white-listing" is just one of the examples to ensure FI has security measures in place to restrict the installation of authorised software. We may implement similar security measures to achieve the same objective based on our system security framework.
		Comments on technology risk governance and oversight: For 3.1, with respect to the point on both BOD and senior management need to have members with necessary skills and understanding of technology risks, further guidance on the extent of expected skills and knowledge of technology risks would be helpful.
34.	Cleartrade Exchange Pte. Ltd	Confidential
35.	JLT Asia Pte. Ltd.	Confidential
36.	QBE Insurance (Singapore) Pte Ltd	Confidential
37.	PayPal Pte. Ltd. (3PL)	Confidential
38.	Anonymous	Comments on IT Project Management and Security-by-Design: In relation to Para. 5.3.3, is the MAS able to clarify the instances where a commercial off-the-shelf solution that does not meet the FI's requirements would still be deployed even though it is not suitable?
		Comments on IT Audit: While we can understand that the proposed TRM Guidelines appear to be geared generally to all financial institutions which includes larger operations with larger

		systemaic effects, is the MAS able to provide other helpful scalable alternatives for small setups with headcount of less than 10 to fulfill the audit requirements within the proposed TRM Guidelines?
		General Comments: How would the Checklist for TRM Guidelines line up with the proposed revised TRM Guidelines and the proposed Notice on Cyber Hygiene which was in consultation?
		Comments on Technology Risk Management Framework: In relation to Para. 4.1.2, can we clarify that the "risk owner" is the one who decides on what IT controls to be implemented and enforces it and is not the person carries out the IT function or process?
		Comments on Technology Risk Governance and Oversight: In relation to Para. 3.1.5 (c) and (d), appointing a Chief Information Officer, Chief Technology Officer or Head of Information Technology might, Chief Information Security Officer or Head of Information Security would be more appropriate for a large financial institution where IT systems are complex and operations are large enough to have separate specific headcounts for different areas of IT and security. Is the MAS able to provide some guidance or direction for smaller financial institutions with a headcount of less than 10? In a small FI setting, should there be a specific designated IT headcount to be in charge for all IT and security matters?
39.	Anonymous	Comments on Cyber Surveillance and Security Operations: While misinformation relating to a financial institution may cause some reputational issues to the financial institution concerned, in practice, it is extremely challenging to detect everything that may be related to the said financial institution propagated in cyberspace and all modes of information transfer channels, assess them and determine the appropriate follow-up action. Should it be brought to the financial institution's attention, we agree that a suitable

		response by the financial institution can and should be done.
		Comments on Technology Risk Governance and Oversight: While we can appreciate the impetus of requiring that the board of directors and senior management of the licensed entity be sufficiently equipped with the necessary skills and understanding of technology risks, including risks posed by cyber threats, in order for them to provide oversight over technology risks, we have to be mindful and draw a distinction between broad appreciation of such risks in order to make a judgment call and deep detailed understanding of such risks, such as having a technical IT person on the board of directors or as senior management. We read this expectation to commensurate with the nature of business, risks and size of the firm. We appreciate MAS' further clarification if our understanding is inaccurate.
40.	Anonymous	Comments on IT Resilience: • Refer to 8.4.1, "Unintentionally deleted. "and "intentionally deleted" events are rather vague or can be so vast when come to defining scenario or scope for a backup strategy and developing a backup plan. Examples or scope of these events should be suggested in order to ensure events that covers in FIs' backup strategy and plan is sensible and cost effective.
		Comments on IT Project Management and Security-by-Design: • Refer to 5.2.1, is project steering committee required for all IT projects? Or applicable based on criticality or the project budget, it would be good to clarify on the requirement to set up a project steering committee. • Refer to 5.4.2, "... The security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling." . Some legacy systems

		and/or simple/small systems which may not explicitly covering all these key control areas such as security event tracking and exception handling. Would it be acceptable for the residual risk of these systems to be managed through the 4.1 Risk Management Framework?
		Comments on Technology Risk Governance and Oversight: • Refer to 3.3, The definition of Information assets mentioned on footnote 3 include data, hardware and software. Information assets are not limited to those that are owned by the FI....". This maybe a theoretically sound risk treatment, however, it will be extremely challenging for FIs to put a value on all information assets particularly when the information assets is data. Further guidance on this quantitative approach should be provided to FIs. Moreover, information assets used by service providers to deliver the service provided to the FI are also included in scope, this seems very onerous from the service provider. It will be better to use some form of independent accreditation/assessment on the information assets used by service provider to provide the assurance that they meet the requirement of the TRM guidelines.
		Comments on Technology Risk Governance and Oversight: • Refer to section 3.4.1, FI should be able to rely on independent accreditation/assessment on the assessment of third party service provider. The other way to look at it can FI rely on certain industry regulatory requirements that they have to comply with? For example, a Telco service in Singapore will have to comply with the Cyber security Act and our external legal advisors will have to comply with their relevant PDPA requirements to protect personal information etc?
		Comments on Technology Risk Governance and Oversight: • Refer to 3.5.2, can the FI rely on external vendor's background checks? FI will remind their vendors' of this risk and request that background checks be performed on their staff who has access to the FI's information.

41.	Anonymous	Comments on IT Resilience: 8.1.1 - Should FI include all systems or critical system only in system redundancy implementation / fault tolerant solutions? Propose this be risked based. 8.2.3 - Seek clarification to understand "untested recovery measures". 8.3.2 - Ref "criteria for measuring the success of the test" There is currently no industry-wide methodology to measure the success of an RPO. Therefore, we would recommend that further guidance be issued on this in consultation with FIs. 8.3.3 - Seek clarification for "partial shutdown or incapacitation" Is the definition consistent among all FI's. For example, partial shutdown could include HA cluster fail testing within the same data center or partial loss of a data center requiring failover to another data center. 8.3.4 - Seek definition for "extended period" Is a few hours or one day acceptable? 8.5.1 - Must the TVRA be done by an independent entity or can it be done in-house? 8.5.6a - Propose replacing "immediately" with "promptly" 8.5.6d - "Recorded, monitored, and supervised are somewhat redundant terms". Propose rewording to "Access to equipment racks should be adequately controlled and have adequate surveillance in place."
		Comments on Operational Infrastructure Security: General comment: Any device connected to an FI's network must adhere to acceptable Network Security Standards. IoT brings into scope a large variety and number of devices and FI's should be aware of that . However, consider removing this section, as it is essentially covered throughout the other sections of this document.

		Would an employee's own personal device that connects to corporate Wifi be considered an IoT device and subject to monitoring? 11.1.3 - Confidential data stored in Company managed infrastructure will be governed by authorized user access, and hence encryption of such data should not be mandated. Requiring encryption of data on non-Company managed infrastructure is a reasonable requirement.
		Comments on Operational Infrastructure Security: 11.2.2 "To minimise the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network, the FI should deploy firewalls, or other similar measures, within internal networks to protect information assets within the FI's internal networks. Information assets could be grouped into network segments based on the criticality of the business that they support, their functional role (e.g. databases and applications) or the sensitivity of the information. " Comment: Suggest replacing "segregate information assets" with "protect information assets"
		Comments on Operational Infrastructure Security 11.2.7: Suggest using the wording from recommendation #13 of the "Report of the COI into the Cyber Attack on SingHealth": "[…] the FI should perform a risk assessment taking into account the benefits and drawbacks of Internet surfing separation and Internet isolation technology, and put in place mitigating controls to address the residual risks."
		Comments on Operational Infrastructure Security: 11.5.1 - a) Are BYOD devices considered IOT and are the FI's required to maintain an inventory of all BYOD's that end users may use? Access control can be accomplished by various methods. b) Propose that multifunction printers may not be IOT if they are only connnected to the internal networks; however, they should have adequate security,

		patching, and updates. 11.5.3: Comment: this paragraph is very prescriptive, not taking into account that some devices can be less or more secure than others.
		Comments on Operational Infrastructure Security: 11.5.3: Comment: this paragraph is very prescriptive, not taking into account that some devices can be less or more secure than others.
		Comments on IT Project Management and Security-by-Design: 5.3.4 - Clarification is required for type source code escrow agreement, especially for propriety software from vendor verses software that an FI purchases for use in-house 5.8.2 - Clarification required on the definition of 'independent Quality assurance function'.
		Comments on Software Application Development and Management: 6.1.1 Propose that the standards should be risk based. 6.4.3 - Is approved API access only required for third party governance or more generally - clarify? 6.4.8 - Clarity required on the requirement to perform Real-time monitoring of APIs. What kind of suspicious activities need to be monitored? is this required only for critical APIs or based on the classification of data that the API handles? 6.5.1 - What is the scope of impact and definition of application developed / acquired by end user that is required approval from business and IT management approval? Propose this be risk based for all end user management guidelines in this section.
		Comments on Cyber Surveillance and Security Operations:

		12.1.2 "The FI could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties." Would procuring cyber intelligence monitoring services be considered as "outsourcing" or "third party services" 12.1.5 "The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation." Would engaging external media monitoring services be considered as "outsouring" or "third party services"? Examples of this are: any wrong information about FI's products, services or attempts to misuse of FI's name, brand, products or any misinformation related to their services that can affect their reputation, brand-image, possibly misguide the public, thereof 12.2.6 & 12.2.7: clarify if this is intended for external customers
		Comments on Annex C: Mobile Application Security: Annex C: (e) "implement 'a secure in-app keypad' to mitigate against malware that captures keystrokes; and" Comment: this is quite prescriptive, suggest rewording to use 'security measures' instead.
		Comments on Online Financial Services: 14.2.1 - What is the practice and requirement for OTP? Is classification required for first time login and mask? As of now all banks are showing the masked information on login without 2FA. Can this be added in the text? 14.2.3 – Can they taken an account of PayNow which is not required any transaction signing. Also it is better to clarify whether merchant/bill payment is out of scope

		14.2.8 - Cross check and validation should be done to verify jailbroken devices.
		Comments on Access Control: This section is for FI user access control and not for customer. 9.1.1 - What is the definition and scope of 'never alone'? Is that maker/checker or that staff should be supervised at all times for based on risk. 9.1.2 "The FI should establish a user access management process to provision and revoke access rights to information assets. Access rights should be authorised and approved by the information asset owner or delegate." Comment: add "delegate" 9.1.6 "The FI should ensure information asset owners or delegates perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as incorrectly provisioned access rights. Exceptions noted from the user access review should be resolved as soon as practicable." Comment: Add delegate" 9.3.1 - Should BYOD email such as Blackberry be classified as remote access assets since they do not have access to internal networks? 9.3.2 - Virtual Devices (e.g., VDI) that are accessed through secure channels including from BYOD should be allowed.
		Comments on Technology Risk Management Framework: Suggest rewording to make it more clear: The FI should identify the threats and vulnerabilities, as well as the risks posed to its IT environment. The risks posed to information assets that are maintained or supported by third party service providers should be assessed in an appropriate way.

42.	Anonymous	Comments on Cryptography: 10.1.3 [page 38] The Bank would like further clarity on what is required in the testing or vetting process.
		Comments on IT Resilience: 8.1.2 [page 31] The Bank would like to understand if this is a one-time review or the review has to be conducted on a regular basis. 8.1.4 [page 31] The Bank would like to understand if this is a one-time testing or the testing has to be conducted on a regular basis. 8.2.2 [page 32] The Bank would like further clarity on the types of "disaster scenarios" to be included in the FI's disaster recovery plan. 8.3.1 [page 32] The Bank would like to understand MAS' expectation on the frequency of "regular testing". 8.3.2 [page 32] The Bank would like further clarity on the following: 1) What is the definition of "test scripts"? 2) Should the test script be from IT or business?

		3) Does the Disaster Recovery checklist qualify as a test script? 8.3.4 [page 32] The Bank would like further clarity on the following: 1) What is the definition of “extended period”? 2) What is the scope of this clause? Is it sufficient if the Bank operates from its recovery site for selected systems for an extended period? 8.4.3 [page 33] The Bank would like to understand if a periodic read test is sufficient to address this requirement. 8.5.2 (a) [page 34] The Bank would like further clarity on what is meant by external service provider.
		Comments on Operational Infrastructure Security: 11.1 [page 40] The Bank suggests replacing “Data Security” with “Information Security”.
		Comments on Operational Infrastructure Security: 11.1.2 [page 40] 1. The Bank suggests replacing “data” with “information”: “The FI should implement appropriate measures to prevent and detect information theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI’s service providers using a risk based approach.” 2. The Bank would like to understand if this is applicable to all service providers regardless of inherent risk.

		Comments on Operational Infrastructure Security: 11.1.4 [page 40] 1. The Bank would like further clarity on the definition of "mediums". 2. The Bank suggests replacing “mediums” by “channels and devices”. Please see proposed revised version: "The FI should ensure only authorised channels and devices are used to communicate, transfer, or store confidential information…"
		Comments on Operational Infrastructure Security: 11.1.7 [page 41] 1. The Bank would like to understand if this requirement will be applicable to vendors operating a multi-tenant environment (e.g., Office 365, AWS, etc.) 2. The Bank suggests replacing “data” by “information”. Please see proposed revised version: "The FI should ensure confidential information is irrevocably removed from IT systems and endpoints before they are disposed of."
		Comments on Operational Infrastructure Security: 11.2 [page 41] The Bank would like to understand if there are any mandatory controls such as multi-tier firewall or WAF.
		Comments on Operational Infrastructure Security: 11.2.7 [page 41] The Bank would like to understand if MAS’ expectation is on browser virtualisation (internet isolation) and/or internet separation?
		Comments on Operational Infrastructure Security: 11.3.6 [page 42] The Bank suggests rephrasing “should be” to “could be": “Security measures, such as application white-listing, could be implemented to ensure only authorised software is allowed to be installed on the FI’s systems.”
		Comments on IT Project Management and Security-by-Design:

		5.6.2 [page 20] The Bank suggests the removal of the word "use": "The FI should track and verify that system requirements are met by the current system design and implementation…" 5.7.3 [page 21] The Bank would like to highlight that in view of User Centric Agile Testing, it is typical for testing to be conducted in a single common environment.
		Comments on Software Application Development and Management: 6.3 [page 23] The Bank suggests extending this to set out control expectations in DevSecOps, for completeness. 6.4 [page 23] 1. The Bank suggests the inclusion of guidelines around Sandbox API which should be more flexible to support innovation and collaboration. 2. The Bank suggests the inclusion of detailed specifications of security standards to use and specifications regarding access-log-retention policy. 6.4.3 & 6.4.4 [page 24] The Bank would like to confirm our understanding that this section does not include the business partner vetting process since business should be performing due diligence on partners. The Bank would like to confirm our understanding if "third-party" is referring to "direct third-party". In API ecosystem, API can be consumed by another third-party. 6.5.1 [page 25] The Bank suggests the following revision to provide better clarity on the approvals needed: "… Any applications developed by end users should be

		approved by relevant Business management, while those acquired by end users should be approved by both Business and IT management, where appropriate. Any applications developed or acquired by end users should be managed as part of the FI's information assets." 6.5.2 [page 25] The Bank suggests the replacement of "importance" by "risk" for better clarity. Please see proposed revised version: "The FI should establish a process to assess the risk of end user developed or acquired applications to the business, and ensure appropriate controls and security measures are implemented to address the associated risks…" 6.5.3 [page 25] The Bank would like further clarity on the following: 1) Please provide a clearer definition of Shadow IT to better call out the differences between Shadow IT and End User Computing and Applications. 2) Should requirements in 6.5.3 be removed and incorporated into 6.5.1 and 6.5.2 to minimize ambiguity? 3) Separately, the Bank proposes for "Shadow IT" to be replaced by "End user computing and IT applications" to minimize ambiguity. See proposed revised version below: "End user computing and or IT applications acquired and used in the FI's environment without instituting appropriate controls and seeking the approval of relevant business and IT management increase the FI's exposure to risks, such as leakage of sensitive data, or malware infection. The FI should establish measures to log and track the use of end user computing and IT applications in its environment. End user computing and IT applications should not be used until they have been properly assessed and approved for use."

		Comments on Cyber Surveillance and Security Operations: 12.1.5 [page 45] 1. The Bank suggests the following revision: "The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the internet. The FI may consider engaging external media monitoring services thto facilitate evaluation and identification of online misinformation." 2. The Bank would like to share that it is not possible to be exhaustive and comprehensive to "catch" all misinformation about the Bank in the cyberspace. For example, there may be fake images created of our senior management in pictures and videos which are unlikely to be detected. 12.2.2 [page 46] The Bank suggests the following revision: "As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be suspicious signs of intrusions."
		Comments on Annex C: Mobile Application Security: Annex C C.1 (e) [page 59] The Bank will like to understand if the expectation is that the mobile application must have its own build-in keypad or if it is only expected that the in-app keypad is only mandatory for keying in sensitive information.
		Comments on Online Financial Services: 14.1.6 [page 52] In view of the practicality of monitoring customers' emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers, the Bank suggests for

		MAS to revisit expectations of this requirement. 14.2.6 & 14.2.7 [page 53] The Bank would like to understand if it includes biometric solutions implemented by mobile phone manufacturers. 14.2.11 [page 54] The Bank will like to understand if the online session must automatically terminate after the pre-defined time even when the customer is still using it? Currently the Bank already has a time-out if our system detects there is no activity by customer.
		Comments on Technology Risk Governance and Oversight: 3.1.1 [page 9] The Bank would like MAS to consider the below revision for better clarity on responsibility of Board and senior management: "It is vital that the FIs' board of directors and senior management are fully responsible for ensuring effective internal controls, and …."
		Comments on Technology Risk Governance and Oversight: 3.1.5 [page 9] The Bank suggests including a sub-paragraph for clarity on the differences in roles/ responsibilities between IT Security and Technology Risk. Please see following proposed sub-paragraph for consideration: "Appointing a Head of Technology Risk, with the requisite expertise and experience, to be responsible for the FI's overall Technology Risk strategy and management" 3.1.5 (j) [page 10] The Bank would like further clarity on MAS' expectations of Board (or designated committee) in assessing management competencies for developing policies to manage technology risks.

		Comments on Technology Risk Governance and Oversight: 3.2.2 [page 11] The Bank suggests the below revisions, to minimize ambiguity on role of senior management with respect to risks associated with deviations: "The FI should ensure risks associated with deviations are thoroughly assessed, and ensure they are reviewed and approved by senior management…"
		Comments on Technology Risk Governance and Oversight: 3.3.1 [page 11] The Bank suggests the below revisions, to allow FIs some flexibility as part of their implementation to meet this requirement (e.g,. incorporating in existing framework, standards, etc): "To have an accurate and complete view of its IT operating environment, the FI should establish appropriate information asset management practices that includes the following..." Footnote 3 [page 11] 1. The Bank would like further clarity on the following: 1) Does data here refer to physical data, digital data, or both? 2) Do information assets include those that are hosted and/ or processed by service providers to facilitate their delivery of services to the FI? 3) Please provide some examples of information assets that meet this requirement --> "They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI" 2. The Bank suggests the below revisions, to give more clarity and better ringfence the requirement: "Information assets include data, hardware and software.

		Information assets are not limited to those that are owned by the FI. They also include those that are used by service providers to deliver their services to the FI." 3.3.1 (b) [page 12] The Bank suggests the following revision, for better clarity: "classification of an information asset based on its information classification or system criticality;"
		Comments on Technology Risk Governance and Oversight: 3.4.2 [page 12] The Bank would like further clarity on the following: 1) In view of this requirement around financial viability and track record which some start-up or Fintech companies may have challenges in meeting them, is MAS expecting that Bank should not engage any start-up or a Fintech company whereby we are unable to determine their financial viability, track record, etc? 2) Based on this requirement on service requirement, are FIs now expected to perform due diligence for non-standardised services such as power supply and telecommunication lines?
		General Comments: The Bank would like to understand how a clause that uses “should” compared to a clause that uses “could” or “could consider” should be interpreted.
		Comments on IT Service Management: 7.2.1 [page 26] The Bank would like to confirm our understanding if the “hardware and software” include network devices such as firewalls and routers.

		Comments on IT Service Management: 7.2.2 [page 26] The Bank suggests the replacement of "information assets" by "hardware and software" for clarity as data has no configuration information. Please see proposed revised version below: "The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure they are accurate and kept up to date."
		Comments on IT Service Management: 7.3.2 [page 26] The Bank suggests the replacement of "dispensation" by "deviation" to be consistent with clause 3.2.2. Please see proposed revised version below: "… The FI should obtain deviation approval from its management for the continued use of outdated and unsupported systems."
		Comments on IT Service Management: 7.4.2 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity as patching in this case may not apply to "data": "All patches should be tested before they are applied to the hardware and software in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system."
		Comments on IT Service Management: 7.5.1 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity and

		applicability: "The FI should establish a change management process to ensure changes to hardware and software are assessed, tested, reviewed and approved before implementation."
		Comments on IT Service Management: 7.5.2 [page 27] The Bank suggests the replacement of "information assets" by "hardware and software" for better clarity and applicability: "… The analysis should cover factors such as security and implications of the change in relation to other hardware and software."
		Comments on IT Service Management: 7.5.4 [page 27] The Bank would like to understand if the business representative be appointed from IT by Business to sit in the Change Advisory Board as a key stakeholder.
		Comments on Cyber Security Assessment: 13.1.2 [page 48] The Bank would like to understand if "service" refers to a system process. 13.2.2 [page 48] The Bank would like to highlight that such programme may result in potential concerns over confidentiality and trust of the customers. 13.2.3 [page 48] The Bank suggests the following revision: "To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on

		the production environment. However, should the nature of the test be intrusive or intensive and may result in the possibility of an outage, the specific test could be conducted against the UAT/Pre-Production environment." 13.5.1 [page 50] The Bank suggests changing from "based on real cyber incidents" to “based on major reported incidents”, as there are insufficient details in the open on the factuality of real cyber incident. Please see proposed revised version: “To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on major reported incidents.”
		Comments on Access Control: 9.1.1 [page 36] The Bank suggests, for clarity, the use of the definitions used (e.g. “never alone”) under section 11.0.1 of the 2013 TRMG. 9.1.2 & 9.1.6 [page 36 and 37] The Bank would like further clarity on who should be the actual authorisers and approvers as there are differences in responsibilities between system owners and data owners. Typically access rights are approved by the application or system owner. 9.1.3 [page 36] The Bank would like to understand if the user access refers to end/business user access or administrator access. 9.1.5 [page 36] 1. The Bank would like further clarity on the difference between Critical system and critical system function? Can this be limited to Critical System instead of Critical System Function? 2. Further elaboration on the definition of critical system function will be appreciated. Please cite examples.

		9.1.8 [page 37] The Bank would like to understand if this applies to all 3rd party service subscriptions regardless of materiality and nature of service subscribed.
		Comments on Technology Risk Management Framework: Footnote 5 [page 14] The Bank suggests the removal of “etc”, to minimize ambiguity: "Data confidentiality refers to the protection of sensitive or confidential data such as customer details from unauthorised access, and disclosure" 4.4.2 [page 16] The Bank suggests the following revision, for better clarity: "… The FI should also assess impact due to damages and losses in the event that a given risk-related event materialises."
43.	Anonymous	Comments on Cryptography: The generation and distribution of cryptographic keys should be automated so as to reduce the accessibility of the keys to human operators.
		Comments on IT Resilience: 8.1.3 It is particularly important for a FI which operates systems that support real-time transactions to proactively design its system for scalability, stability and resilience, and continuously monitor the utilisation of its system… State-dependant application architectures are typically difficult to scale and fail-over effectively, while stateless designs facilitate the scaling, relocating and recovery of the systems. FIs hosting critical services should consider the capacity of their system to scale and recover as part of their

		Technology Refresh plans. 8.3 With the pace of software changes enabled by Agile and DevOps practices as well as the increased interconnectivity of FIs, conducting an annual disaster recovery test is no longer sufficient for critical services. Complex organisations cannot conduct comprehensive tests of all potential failure scenarios unless the exercise is continuous and pervasive. Leading organisations are proactively testing their systems and continuously improving their resilience by practising proactive controlled failure injection (Chaos Engineering). FIs hosting services on which other FIs depend should be expected to conduct such continuous exercises so as to ensure the stability of the entire financial ecosystem.
		Comments on Operational Infrastructure Security: 11.2.2. Proper segmentation of the network is better achieved by segmenting by business function rather than by criticality. Separate systems with a similar criticality but of different business functions should not be hosted in the same segment in order to reduce lateral movement risk. Ideally, FIs should consider the implementation of micro-segmentation or “zero trust network” mutual authentication of systems for their critical functions and their dependencies. 11.x Containers (often called Cloud Native technology) provide an additional layer of abstraction, increased density, strengthened resilience, and better control of the application workloads. However, the increased number and distribution of workloads can create additional complexity and risks if not properly automated and managed. FIs adopting container platforms should establish strong orchestration frameworks to manage the scalability, stability, segmentation and security of the container infrastructure as well as of the application workloads hosted in containers.
		Comments on IT Project Management and Security-by-Design:

		Project / Product Management and Steering Committees: Traditional fixed-term fixed-deliverable project management is decreasingly used for critical systems and business deliveries. Instead, the focus on user-centric design and the adoption of Agile and Lean (i.e. DevOps) principles have driven leading organisations to move towards a focus on products (business functions) that are continuously delivered. It is increasingly common to see transformation exercises based on extreme programming and user-centric design approaches: focused on business outcomes, product owners are continuously adjusting the scope of delivery based on user and stakeholders feedback. Such an approach to product development has proven to ultimately reduce the risk of IT project delivery by increasing the frequency of deliveries and reducing their size. Feasibility and cost-benefit are built on the feedback from the first few versions of a product (MVP) rather than prior to the beginning of the project (blueprint approach). While traditional project management thresholds are seldom applicable in this context of discovery and continuous improvement, key maturity metrics (such as lead time, release frequency, change failure and mean time to recovery) are commonly used. FIs using Agile and DevOps approaches should establish such key metrics and monitor their evolution over time to ensure they remain within acceptable thresholds. Opposite to Project Management-focused approach where Project Manager and PMOs are typically just reporters of risks, Product owners are ultimately responsible for all aspects of their delivery, from productivity and business outcomes to risk and security management. To facilitate the choice of the most appropriate approach for FIs, the guideline should consider extending the framework to Product Management and Product Steering Committees, in which the requirement for predefined project plans is reduced in favour of planned outcomes, risk thresholds, and control coverage. The risk and thresholds to pull out of a product should however be acknowledged by management and a product steering committee, independent from the product team, should oversee the deliveries, risk and outcomes achieved.

		Security-by-design: The more development and integration teams have to build security features, the more likely implementation variations and errors are to happen. Multiple implementations increase the operational overheads for security teams to review and detect flaws in the services provided. Also, introducing a manual security review by IT security at each stage of the SDLC has proven to be reducing agility and resilience and increasing friction. As such, the effective delivery of security-by-design principles requires each security feature to be standardized and made available for easy consumption by developers and platform operators. The minimal security requirements listed in the guideline (access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling) are all services which are readily available in modern application platforms, reducing the risk of errors while increasing operational effectiveness, resiliency and scalability. FIs should identify the common security functions for their critical and public-facing systems, ensure they are delivered in a consistent manner across systems and aim to continuously improve them in line with the FIs' risk and threat landscape. Resilience-by-design: Applications are often highly dependant on other systems. This may result in unplanned outages even though the system has been designed for high-availability. In line with the heightened expectations of the BCM guideline, FIs should integrate resiliency patterns and dependency tracking into their System Development Lifecycle. 5.8.2: An increasing number of organisations are practising a combination of Pair Programming and Test Driven Development, where a pair of programmers are producing both the test and the code, and deliver and heightened delivery quality. To facilitate the adoption of these practices similar to an "assurance by design", the guideline should recommend the quality assurance should be

		conducted independently rather than by a separate function.
		Comments on Software Application Development and Management: 6.1.4 & Annex A: Secure testing practices are diverse and evolve rapidly. For a number of projects, Software Composition Analysis is more appropriate than SAST/DAST/IAST. Runtime Application Security solutions are increasingly able to cover for the capabilities of IAST/DAST. As such, the guideline should leave FIs with the flexibility of solutions implemented in order not to block future evolutions towards Cloud Native & Agile approaches. The enforcement of SAST/DAST/IAST technologies by IT Security functions is often producing counter-productive effects when these solutions are not perfectly fine-tuned to the development framework: a reduction in velocity and increase in cross-functional friction due to a high false-positive rate. Rather than security testing solutions, the major contributor to security issue reduction is the collaboration of developers and IT security towards a common set of security outcomes, and the appropriate incentive of all stakeholders towards continuous security prioritization. FIs should be expected to clearly define and track the evolution of security outcomes being pursued (e.g. reduction of vulnerabilities produced, mean time to discovery, mean time to recovery, and change failures). The addition of Agile and DevOps practices is a great advancement in the support for leading development practices. However, it remains short of the practice of Continuous Delivery which allows development teams to release several times a day. A properly designed continuous delivery leveraging immutable infrastructures is significantly reducing security risks, operational overheads while increasing business resilience. However, it requires the adaptation of vetting, security testing and change management practices. FIs adopting continuous delivery practices should consider

		the implications on other processes to ensure the risk introduced remains acceptable, and implement guardrail controls to minimise the risk of each change. As manual security reviews cannot follow the daily cadence, FIs delivering continuously should implement continuous “off-cycle” active testing of their systems by means of regular penetration testing, bug bounties and chaos engineering exercises.
		Comments on Cyber Surveillance and Security Operations: 12.2.x FIs should develop and test periodically their capacity to promptly resume their critical systems to their last known good state 12.3.3. “Lesson learnt” should be conducted for Cyber incident drills as well, as for each penetration test, bug bounty finding and AASE exercise in order to drive the continuous improvement of detection and remediation times. In order to increase collaboration, exhaustiveness and transparency, such “retros” should be conducted in a blameless environment providing a safe environment to speak and challenge.
		Comments on IT Audit: No comment regarding IT Audit, however, FIs should consider adopting Audit as Code practices to free audit resources for tasks that require human analysis (process/control design issues).
		Comments on Annex A: Application Security Testing: While very useful, the use of SAST/DAST/IAST solutions has proven to be challenging for many organisations, due to the high operational overhead, long testing times and high rate of false positives. Besides, the adequacy of such tools is very variable from one project to another. IT Security functions trying to introduce "one size fits all" mandatory application security controls for all projects have more often than not introduced increased friction and

		are seen as slowing the development of digital services. If technology solutions should be recommended, Software Composition Analysis and Runtime Application Security solutions should be similarly considered by FIs as part of their defence program as they provide a high accuracy rate and low friction to deployment. The guideline should be cautious not to introduce false expectation of effectiveness from these tools. The diversity of architecture patterns and technologies require controls to be adaptable and tailored (reference, Gartner's CARTA model for adaptive controls). Some development teams practising systematic TDD (Test-Driven Development) are able to appropriately capture the potential vulnerabilities as part of their tests rather than by adding additional solutions. Avoiding additional solutions to maintain ultimately increases the flexibility and agility of the organisation by removing new dependencies to maintain while the project evolves. Another adverse effect of the focus on security testing solutions is the false sense of security provided by the reports. Rather than focusing 100% of their efforts on preventing vulnerabilities, FIs should improve their active testing practices (PT, bug bounty, AASE) and drive the improvement of their detection and response to anomalous activity. The experience of CSOC teams to detect and respond may make the difference between an attack and a breach. Collaboration, continuous testing and a focus on improving the time to discovery and time to remediation, are often more effective than security solutions of which the reports are ignored due to the unbearable amounts of findings. FIs should identify the appropriate security testing mechanism to detect vulnerabilities (before they go to production as well as vulnerabilities which made it through to production), work iteratively to remediate and prevent

		reoccurrence, and develop a collaborative culture between software architects, testers and security subject matter experts.
		Online Financial Services require the highest level of trust to minimize the risk of compromise by external and internal actors. Unfortunately, the longer a system lives, the higher the chance of compromise and the more difficult it is to detect anomalies, despite numerous security solutions. To increase the trust in the financial services and reduce operational overheads, FIs should host their online financial services frontends on immutable systems reducing the risk of configuration drift and persistent malicious payloads, and aim to rebuild each endpoint as frequently as possible.
		Comments on Technology Risk Governance and Oversight: Nil.
		General Comments: The guideline provides a major step forward towards facilitating the agile enterprise and introducing modern practices which have proven effective, such as bug bounty and adversarial attack simulation. Leading organisations, however, have passed beyond the practices of Agile and DevOps, and aim to deliver continuously to respond promptly to their customers' needs and the changing risk landscape. To operate effectively, these modern delivery practices require the tight and collaborative integration of development, operations and controls to increase the flow of delivery, reduce waste and defects (including security vulnerabilities), and automate controls. The leading technology companies entering the FI market today are also bringing some modern IT resilience enhancement practices (such as Chaos Engineering and Site Reliability Engineering), which I believe can help increase the sustainability and strength of FIs while reducing

		operational costs. I would like to suggest some considerations below to extend the guideline to continuous delivery models.
		7.4 Unfortunately, current patching practices are reactive and not efficient, and several independent reports highlight that current practices only enable to fix about 10% of overall vulnerabilities. As newly discovered vulnerabilities are exploited increasingly fast, there is a need to review and shift the approach to patch management. Systems facing the Internet or end-user computing stations are typically exposed to a heightened risk of direct attack, yet their patching often remains challenging due to manual processes. To increase the resilience of the financial ecosystem, the components of critical systems facing the Internet, other FIs or end-users should be expected to be capable of zero-downtime patching and should employ comprehensive testing frameworks to enable reliable patching at any time. Such practices are already in use in leading organisations but often suffer from a lack of knowledge internally to be prioritized appropriately. 7.5 Change Management for Continuous Delivery Leading organisations are typically shipping code several times a day to adjust to their customers' demands and risk landscape. In order to maintain an acceptable level of controls while avoiding the challenge of a systematic CAB approval, FIs aiming for fully automated deliveries should identify and implement 1/ appropriate criteria for such a continuous authority to operate, 2/ guardrail controls to prevent the introduction of unexpected risk, and 3/ the conditions under which to trigger an additional review of changes.
		Comments on Cyber Security Assessment: 13.2.2 Bug bounty programs are of primordial importance for continuously delivered products, where periodical penetration tests do not provide timely and continuous

		feedbacks to drive the continuous improvement mechanism. Each finding reported by a security researcher should lead to a review of security tests conducted to prevent this vulnerability to reoccur, as well as a review of the detective controls. 13.2.x Senior Management should provide oversight and incentive of all stakeholders to measure and reduce the time to discovery and time to remediation of security findings.
		9.1.x To reduce the risk of improper implementation of access control systems, FIs should aim to standardize their authentication and authorization systems, and to make them easily consumable by other applications. 9.2.2 The FI should establish a process to periodically rotate (change) the passwords and certificates used by system and service accounts. The frequency of the rotation should be commensurate with the criticality of the system and its exposure to end-users, both public and internal. 9.2.x Unauthorized access using privileged account remains an important risk in all organisations, which can be reduced by removing the need for administrators to access the systems. This not only reduces the attack surface but also facilitate the detection of suspicious privileged account activity. FIs should aim to automate their operations and to transform their critical systems into immutable infrastructures, where direct changes in production are an exception formally tracked, reviewed and replaced by automation.
		Comments on Technology Risk Management Framework: Continuous improvement and feedback loops Risk and threat landscapes are highly evolutive by nature: assumptions taken during an initial assessment may not be aligned in future context; new threats previously unknown may arise and IT systems may rapidly evolve. This is particularly evident in Agile development context.

		To complement the risk review listed in 4.4.8, FIs risk management framework should capture significant events from threat intelligence, incident events and results from active tests (penetration tests, bug bounties, AASE, Chaos engineering feedback), and trigger a review of existing risk assessments where relevant. In addition to conducting risk assessments and risk reviews, risk functions should play an active role in the testing and validation of risk control effectiveness by establishing a risk testing framework.
44.	Anonymous	Comments on Technology Risk Management Framework: The suggestions seem reasonable, but again, FIs must be allowed to right size their approach.
		Comments on IT Audit: Frequency and intensity to be governed by the size and business structure.
		Comments on Online Financial Services: No comment as we do not provide such services.
		Comments on Technology Risk Governance and Oversight: Please see comments above. Expectations need to be commensurate with the size of the Company and the complexity of the business subject to Technology risks.
		General Comments: The TRM guidelines have obviously been designed with large FIs in mind. Some suggestions like annual penetration testing are not realistic for small FIs and particularly in the case of FIs that do not offer any client facing interface, it would not make sense to impose such costly requirements. Also, it is appropriate for a company to require it's Board of

		Directors to remain aware of technological advances and to ensure the Company is implementing sufficient controls to protect the confidential data that it manages, but it would not make sense for a Company to specifically go out and hire a cyber specialist if the business risk is assessed to be low. We are supportive of MAS taking a pragmatic approach by allowing FIs who are not systemically important FIs to implement programmes based on a risk based approach.
		Comments on Cyber Security Assessment: See comments above.
		Comments on IT Resilience: Allow FIs to right size the solutions and use the risk based approach.
		Comments on T Project Management and Security-by-Design: Smaller sized FIs would not usually have projects of the same magnitude as large banks needing to roll out apps and services to multiple users. But if any project is implemented, the security issues should be assessed as suggested.
		Comments on Software Application Development and Management： See comment above
		Comments on Cyber Surveillance and Security Operations: Allow FIs to design using the risk based approach, and again, to right size the frequency and intensity of tests to be conducted.
45.	Anonymous	Confidential

46.	Anonymous	Confidential
47.	Anonymous	Confidential
48.	Anonymous	Confidential
49.	Anonymous	Confidential
50.	Anonymous	Confidential
51.	Anonymous	Confidential
52.	Anonymous	Confidential
53.	Anonymous	Confidential
54.	Anonymous	Confidential
55.	Anonymous	Confidential
56.	Anonymous	Confidential
57.	Anonymous	Confidential
58.	Anonymous	Confidential
59.	Anonymous	Confidential
60.	Anonymous	Confidential
61.	Anonymous	Confidential

62.	Anonymous	Confidential
63.	Anonymous	Confidential
64.	Anonymous	Confidential
65.	Anonymous	Confidential
66.	Anonymous	Confidential
67.	Anonymous	Confidential
68.	Anonymous	Confidential
69.	Anonymous	Confidential
70.	Anonymous	Confidential
71.	Anonymous	Confidential
72.	Anonymous	Confidential
73.	Anonymous	Confidential
74.	Anonymous	Confidential
75.	Anonymous	Confidential
76.	Anonymous	Confidential
77.	Anonymous	Confidential

78.	Anonymous	Confidential
79.	Anonymous	Confidential