
List of Respondents to the Consultation Paper on Proposed Revisions to Guidelines on Business Continuity Management (7 March 2019)

A total of 82 submissions were received of which 9 respondents requested confidentiality of their identity, 3 respondents requested confidentiality of their submission and 26 respondents requested confidentiality of both their identity and submission.

**Respondents who requested confidentiality of their identity*

#Respondents who requested confidentiality for their submitted response

Please refer to Annex B for the submissions.

1. AIG Asia Pacific Insurance Pte. Ltd
2. AL Wealth Partners Pte Ltd
3. Alpha Advisory Pte Ltd
4. Aon Singapore Pte Ltd, Aon Singapore (Broking Centre) Pte Ltd, Aon Benfield Asia Pte Ltd, Aon Hewitt Wealth Management Pte Ltd
5. Asia Cloud Computing Association (ACCA)
6. Asia Securities Industry & Financial Markets Association (ASIFMA)
7. Barclays Bank PLC #
8. Business Continuity Chapter, Singapore Computer Society
9. Cleartrade Exchange Pte. Ltd
10. Deloitte & Touche Enterprise Risk Services Pte Ltd
11. Depository Trust and Clearing Corporation
12. Eastspring Investments (Singapore) Limited
13. Fidelity International
14. Holland & Marie Pte. Ltd.
15. HSK Resources Pte Ltd
16. IG Asia Pte Ltd
17. Investment Management Association of Singapore
18. KPMG Services Pte Ltd
19. Life Insurance Association
 - i. AIA
 - ii. Aviva
 - iii. Etiqa
 - iv. FWD
 - v. Manulife
 - vi. NTUC Income
 - vii. Old Mutual Int'l
 - viii. Tokio Marine Life
 - ix. Transamerica Life
20. Lloyd's of London (Asia) Pte Ltd
21. Marsh (Singapore) Pte.Ltd.
22. Marsh Management Services Singapore Pte Ltd
23. Microsoft Operations Pte Ltd.
24. MUFG Bank, Ltd.
25. Old Mutual International
26. Oliver Wyman
27. Oversea-Chinese Banking Corp Ltd
28. Prusik Investment Management Singapore Pte Ltd
29. QBE Insurance (Singapore) Pte Ltd

-
30. Rabobank Singapore Branch
 31. RBC Investor Services Trust Singapore Limited
 32. REIT Association of Singapore #
 33. RGA International Reinsurance Company
 34. RHT Compliance Solutions Pte. Ltd
 35. Schroder Investment Management (Singapore) Ltd
 36. Securities Association of Singapore
 37. Singapore Exchange Limited
 38. SingCash Pte Ltd/Telecom Equipment Pte Ltd
 39. Sompo Insurance Singapore Pte. Ltd.
 40. Sumitomo Mitsui Banking Corporation
 41. Swiss Re Asia Pte. Ltd.
 42. Swiss Re International SE
 43. The Association of Banks in Singapore (ABS)
 44. The Northern Trust Company
 45. Transamerica Life Bermuda Ltd
 46. Validus Reinsurance Ltd
 47. Wells Fargo Bank
 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 #*

80. An entity #*

81. An entity #*

82. An entity #*

Annex B Submissions to the Public Consultation

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

S/N	Respondent	Feedback from respondent
1.	AIG Asia Pacific Insurance Pte. Ltd	<p>Comments on the definition of business function:</p> <p>The proposed definition of “business function” as a service that an FI ultimately provides to its customers is very wide.</p> <p>Please clarify that “customers” defined in the Guidelines means “business” customers of an FI and not other parties such as vendors, regulators etc. An FI has numerous business functions depending on which level it reviews its business functions. It may also have numerous sub-functions which support its end-to-end business function. To organise a BCP just to cover 1 business function would entail a complex plan requiring support from many sub-functions within the FI. Many of these sub-functions support most, if not all of the business functions. To include them in all the BCP for all the business functions may not be feasible or tenable.</p> <p>In view of the complexity of organising BCP for all business functions (for end-to-end service), we propose that the focus on end-to-end BCP should be on critical business functions and involve only critical sub-functions within a business function.</p> <p>The frequency of BCP to cover all business functions should also be considered in view of the above. We propose that the focus be on critical business functions where BCP should be conducted annually. For less critical or non-critical business functions, the recommendation is for a BCP to be conducted once every 2 years.</p> <p>What is MAS’ expectation for the minimum performance level, noting that this is in addition to the RTO and RPO. Depending on the business line of an FI, the minimum performance level of a business function could be the RTO or RPO.</p> <p>There is requirement for FI to establish monitoring capabilities that will enable prompt detection of reduced or intermittent service availabilities and triggers for activation of contingency plans. We propose that the focus should be on critical business functions as it is not feasible for FI to implement such monitoring capabilities for all business functions.</p> <p>Due to the complexity in mapping out the BCP under the Guidelines, would MAS allow FI sufficient time of at least 1 year to meet the new Guidelines?</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>We note the requirement for senior management to participate actively in the FI’s BCM tests. Please clarify if the expectation for active participation by senior management is referring the senior management in charge of the business function and not all the senior management. To require all senior management to participate actively in all the FI’s BCM is not tenable.</p> <p>What is MAS’ expectation in terms of the core competencies and training for CMT members?</p> <p>Comments on the scope of a BCP:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>The guidelines require future exercises to include rehearsal of scenarios for end to end business function such as system down and data loss rather just physical relocation. This will entail more time, focus and resources from IT and more active participation from all stakeholders including managers. In view of these requirements, the focus of the end-to-end BCP should be on critical business functions.</p> <p>It should be noted that, for each business function, there would be numerous scenarios for a BCP. Please clarify there is no expectation that an FI must cover all the scenarios.</p> <p>Please clarify the threshold for “plausible”.</p> <p>What is MAS’ expectation in terms of FIs taking reasonable steps to provide assurance that key service providers are capable of supporting their businesses even in disruptions, in particular service providers which have monopoly market share e.g. Singpost, SingTel, PUB etc.</p> <p>In view of the annual training requirement, please clarify that online training, classroom training or actual BCP exercise would meet the training programme stated in the guidelines.</p> <p>Comments on the type and frequency of BCM tests: Please clarify MAS’ expectations on the frequency of such BCM audits. Will it be annual audits or can the period between audits be stretched depending on the results of the prior audit and criticality of the business function?</p> <p>Comments on the conduct of regular BCM audits: Please clarify if MAS require the BCM audits to take a particular form and if so, whether MAS will be issuing any template.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Regarding paragraph 3.2: Once an initial BIA has been performed, please clarify that a review (rather than another new BIA be performed) should be done at least annually and whenever there are material changes to the business functions and an update be made, if applicable. Regarding paragraph 5.9: What is MAS’ expectation in terms of FIs taking reasonable steps to provide assurance that key service providers are capable of supporting their businesses even in disruptions, in particular service providers which have monopoly market share e.g. Singpost, SingTel, PUB etc.</p> <p>Regarding paragraph 6.4: An organisation may have many critical business function. To organize a test for each critical business function on top of crisis management and communications exercise annually may put a strain on the FI’s resources. We would propose a timeframe of at least once every 2 -3 years.</p>
2.	AL Wealth Partners Pte Ltd	<p>Comments on the definition of business function: We have no issues with the new definition.</p> <p>Comments on the roles and responsibilities of the Board and senior management: It is appropriate for the Board of Directors and the Senior Management to be involved in the design and implementation. The creation of a Crisis Management Team also makes sense.</p> <p>Comments on the scope of a BCP:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Ensuring that a comprehensive risk assessment be done prior to designing the BCP would help to align the effectiveness of the BCP. Such BCP must be tailored according to not only the assessment results but the size of the company and the criticality of the services defined. We appreciate the risk based approach but if MAS could provide examples of “severe” disruption, it would make planning easier. For most FIs, the most severe disruption would be a scenario where the entire infrastructure in Singapore is disrupted (no mobile connectivity and no internet). Does MAS expect FIs to test such a scenario? Realistically, most FIs probably only design business continuity tests based on the assumption that premises not available but the internet and telecommunication (fix and/or mobile) connectivity remains accessible.</p> <p>Comments on the type and frequency of BCM tests: In principle, annual testing is a reasonable concept. As mentioned in question 2, FIs must be given a base case scenario (e.g. disruption caused by office fire; disruption caused by pandemic etc), upon which the FI can build its action plan to allow practical processes that can be usable in actual incident.</p> <p>Comments on the conduct of regular BCM audits: Not all FIs especially the small sized boutique firms have their own in-house internal audit unit and most are using external providers. MAS should allow such firms to conduct the BCP and have their assessment reports be reviewed by either their sub-contracted internal or external auditor during their annual internal/statutory audit to fulfil this MAS expectation.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: To facilitate FIs to design the appropriate policies and procedures on a risk based basis, would MAS give some guidance as to the minimum scenarios that MAS would want to see being tested?</p>
3.	Alpha Advisory Pte Ltd	<p>General comments: We are a small team providing M&A advice. We have no reliance on any IT infrastructure nor on any office infrastructure. Our work can be performed from any office or any location. We can, and regularly do, perform our work from home or overseas.</p> <p>Comments on the definition of business function: This question is better directed at a large institution with complex functions where the challenges of business continuity are more relevant.</p> <p>Comments on the roles and responsibilities of the Board and senior management: This question is better directed at a large institution with complex functions where the challenges of business continuity are more relevant.</p> <p>Comments on the scope of a BCP: This question is better directed at a large institution with complex functions where the challenges of business continuity are more relevant.</p> <p>Comments on the type and frequency of BCM tests: This question is better directed at a large institution with complex functions where the challenges of business continuity are more relevant.</p> <p>Comments on the conduct of regular BCM audits:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		As noted in the general comments, we do not have a plan that could be audited.
4.	Aon Singapore Pte Ltd, Aon Singapore (Broking Centre) Pte Ltd, Aon Benfield Asia Pte Ltd, Aon Hewitt Wealth Management Pte Ltd	<p>Comments on the definition of business function:</p> <p>Para 3.3. Business Continuity Objective</p> <p>It is not clear how the minimum performance level can be determined. RTO has previously been determined to be the target time for specific business function to be recovered. It will be difficult to quantify the minimum performance level under the new definition. Could MAS provide some examples on how a minimum performance level may be quantified and the basis for setting a threshold for minimum performance level?</p>
5.	Asia Cloud Computing Association (ACCA)	<p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <p>Section 5.8: “Where recovery arrangements rely on other stakeholders, such as intra-group partners and third party vendors, formal service level agreements (SLAs) should be established and the appropriate redundancies agreed upon. This would include setting specific and measurable recovery expectations (e.g. RTOs), mutual participation in testing and review of SLAs on a regular basis. FIs are encouraged to share their business continuity objectives with key stakeholders to mitigate the risk of mismatched expectations. An FI should proactively assess the resilience of these stakeholders and involve them in its BCM exercises, where appropriate.”</p> <p>Comment #1: We would like to highlight that Section 5.8 of the Guidelines is not feasible in the context of FIs’ engagement of cloud service providers (CSPs). The requirement for recovery time objectives (RTOs) to be outlined in SLAs is not possible for a majority of hyperscale CSPs. This is because, such an obligation would imply that RTOs can be negotiated with each customer, which is not possible in the context of hyperscale cloud services. We therefore recommend that FIs instead be required to have understanding of the CSPs’ RTOs rather than requiring RTOs to be negotiated contract terms.</p> <p>Comment #2: FIs should have the flexibility to determine the contractual terms appropriate for the type of services they use. Laying out the details that should be covered in SLAs may appear to be overly prescriptive and would not be feasible for FIs looking to utilise hyperscale cloud computing services. Setting out specific and measurable recovery expectations (e.g. RTOs), mutual participation in testing and review of SLAs on a regular basis is not consistent with the one-to-many nature of hyperscale CSPs. Hyperscale cloud services are provided on a shared responsibility model where customers have the flexibility to determine their back-up requirements and configure the services to meet their objectives. The service configuration decisions that determine a customer’s recovery (e.g. RPO / RTO) are not made by the CSP, and are also likely to change over time as the FI changes its business use cases. It is therefore inappropriate for SLAs between the CSP and the FI to include specific recovery expectations (including e.g. RPO/ RTO).</p> <p>Comment #3: It is also not feasible for CSPs to contractually commit to joint testing of their business continuity plans (BCPs) with individual customers. Furthermore, the CSP has its own BCP and hence there are no components of the BCPs that require joint testing. The mandating of joint testing is hence not only impractical for hyperscale CSPs to abide by, but it also takes away from the intended efficiency gained by outsourcing certain services to CSPs. Similarly, CSPs should not be required to get involved with the BCM exercises of their FI</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>customers. As highlighted above, FIs and CSPs have their own BCM practices, which they can implement independently. Also, given the volume of customers, hyperscale CSPs will be unable to participate in the BCM exercises of all their FI customers.</p> <p>Comment #4: As mentioned above, hyperscale cloud services are provided to customers on a one-to-many basis, which means that the services provided operate in the same manner for all customers, and hence the SLAs for individual services are consistent across customers. Thus, in light of the above, we propose that Section 5.8 be removed in its entirety, as the relevant principles are already covered in Sections 5.7 and 5.9.</p>
6.	Asia Securities Industry & Financial Markets Association (ASIFMA)	<p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> • Scope and extraterritoriality: It is unclear from the draft Proposed Revisions to Guidelines on Business Continuity Management (“Guidelines”) if and how the proposed Guidelines apply to offshore entities, third parties, etc. We strongly encourage the MAS to reconsider the extraterritorial aspect of the revised BCM Guidelines. Instead, and as mentioned in the general comments, we strongly recommend the MAS and other overseas regulatory agencies coordinate closely to devise a global approach to operational resilience. ASIFMA members generally have global business models, have cross-border operations and have entities that are regulated in multiple jurisdictions. ASIFMA members will therefore also need clarity on the applicability (if and how) of the proposed Guidelines to: <ul style="list-style-type: none"> a. Non-material branches of foreign banks – we suggest that these should be excluded from the applicable scope of the draft Guidelines. b. Financial Market Infrastructures (FMIs): Financial institutions (FIs) rely on third party service providers including FMIs such as payment, clearing and settlement operators to ensure continuity of services to the customer. Clarity is needed on whether the end-to-end “business function” includes the FMIs and other third parties; and if so, how are the FMIs expected to be dealt with in the FI’s Business Continuity Management (BCM) plan for a “business function”, given that an individual FI will not have any control over the BCM planning and testing of the FMIs or third parties. (This is also related to Question 3 on the scope of the Business Continuity Plan (BCP). c. Outsourced 3rd-party providers in Singapore and overseas d. Discern whether the scope is functionally and/or geographically driven. Ex: functions conducting business with Singapore entities and/or Singapore based business functions. • We request that the scope be limited to critical business functions provided by the FI. If the MAS intends to extend to all business functions (including those that are non-critical) we would request an extended transition period. • Internationally consistent definitions: We recommend that there should be common definitions of terms (e.g. “service”, “business function”, “business process”, “critical business function”) to reduce potential confusion and drive international harmonization. We suggest that the MAS, its peer regulators (including BoE and FCA), multilateral agencies and relevant trade associations including the GFMA collaborate so we can agree on a harmonized approach. GFMA stands ready to support and is looking forward to soon share its white paper on this topic (see General Comments). Alignment of approaches could be achieved, for example, by supporting the development by international standard setters of a lexicon of terms and concepts related to operational resilience. Indeed, divergence in definitions is already emerging. For example,

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>“Business Service” is a term used by BoE as an end-to-end set of business processes while the MAS uses the term “Business Function” to refer to an end-to-end business service. In the US, the term (critical) function generally refers to a business process, whereas the MAS defines a critical business function as a service and based on BoE definition, Offerings is used instead of Business Service.</p> <ul style="list-style-type: none"> • Level of granularity to identify business functions: We request the MAS to provide further guidance on the level of granularity expected in the identification of business functions. For consistency of application across the industry, it would be helpful if the MAS could provide an illustrative list of business functions. • Minimum Performance Level (MPL): <ul style="list-style-type: none"> a. MPL is a good concept to incorporate as a stop gap measure. However, the focus of the BCM program should be on long term, sustainable recovery. Subsequently, all business continuity program outputs (RTO, testing, etc.) should be aligned to the business continuity strategy instead of the MPL. b. We are generally supportive of the introduction of Business Continuity Objectives as it provides guidance to FIs that MPLs, RTOs and Recovery Point Objectives (RPO) per Business Function must be determined during BCM planning. The preference is to conduct testing by validating functional recoverability vs. ability to achieve the MPLs. The functional recoverability allows for better preparedness, increased resiliency, and ability to demonstrate capability to meet stakeholder commitment. The RTO specification on individual dependencies (staff, sites, suppliers, applications) will allow an FI to discern the prioritization of dependencies in a recovery. c. If the above approach is not taken, we request that the MAS provide additional guidance on the proposed MPL requirements. Specifically, more clarity is needed in relation to the definition, guidance on how an FI should determine a MPL, the desired outcome from identification, as well as the impact on the business continuity lifecycle (dependency identifications, recovery steps, recovery objectives, etc.) • Minimum Level of Output (MLO): <ul style="list-style-type: none"> a. ASIFMA members request more clarity on the definition and scope of MLO requirements (e.g. is the concept introduced across the board, is it risk based, etc.) and to all components of the BC lifecycle (e.g. applications, third parties etc) & stakeholders (e.g. all business services, critical business services, designated Critical Operations or the equivalent). b. Incident management processes are targeted at any component of a process that is degraded rather than across an E2E business function. This ensures that an E2E business function is not unduly degraded due to existing incident escalation criteria, i.e. within any MPL that would be separately defined. We therefore recommend leveraging the traditional incident management frameworks when considering MPLs. • Referring to paragraph 2.6 of the consultation paper, our members deem it difficult to determine RTOs at business function level as there may be processes or systems that do not require the “most stringent” RTO of 2-4 hours. For example, a regulatory reporting process as part of a securities trading BF would not need a 2-4 hours RTO, but 8-12 hours or more will be more appropriate.

S/N	Respondent	Feedback from respondent
		<ul style="list-style-type: none"> • We suggest that the MAS clarifies relationship between minimum level of output and impact driven function Recovery Time Objective (RTO). <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ul style="list-style-type: none"> • Referring to para 2.9(a) of the Consultation Paper - the Board's responsibility to endorse "the FI's BCM, as well as ensure that the framework consists of comprehensive policies, processes and procedures...", we suggest the MAS to clarify the separate references to "BCM" and "framework" to avoid confusion. • Most ASIFMA members agree with the roles and responsibilities proposed for the Board and senior management. However, it is not realistic to expect that senior management participate actively in all BCM tests unless they have recovery strategies that they need to validate. We suggest paragraph 2.10(c) of the Consultation Paper (and the related parts of Annex B, the Revised Guidelines) be rephrased to "participate actively in the FIs BCM tests if there are recovery strategies that they need to validate." • In Section 4.5 in Annex B of the consultation paper, we suggest that the committee to oversee the FI's BCM can also be the Crisis Management Team (CMT) as they are responsible for managing the FI's response in executing a BCP. • Lastly, can the MAS confirm if "the Board's" responsibilities, in the context of non-material branches of foreign banks, can be performed by the Singapore branch's most senior executive/governance committee. <p>Comments on the scope of a BCP:</p> <ul style="list-style-type: none"> • (see also Question 1) We would like clarification, if a business function is expected to include third parties or FMIs that are part of the processes performed and would suggest that FMIs are not included. • End to End Business ("E2E") Function: E2E approach to BCPs appears to be a very effective way to assess and review processes, document risks/controls and services delivered to customers. Specifically, the initiative allows for a specialized, integrated resources to be engaged in working groups to avoid silos and missed handoffs. However, given the trend of having the offshore "centres of excellence" supporting various functions for different business lines and entities across a financial group, it would be challenging to conduct E2E BCP as per MAS requirement. We recommend a E2E requirement to be rolled out flexibly and allow for an opportunity to achieve the desired end state through alternate means. <ul style="list-style-type: none"> a. More specific guidance on the expected scope and granularity of E2E BF BCPs on top of individual business unit BCPs, is needed. Using a "custody" service as an example, the service-level BCP could potentially cover multiple geographic regions, products, and the entire product lifecycles, etc. We strongly encourage the MAS to reconsider the extraterritorial aspect of the revised BCM Guidelines. Instead, we recommend that the MAS and other overseas regulatory agencies coordinate closely to devise a global approach or to rely on substantively equivalent/deference to foreign regulatory regimes to achieve this outcome across more than one jurisdiction.

S/N	Respondent	Feedback from respondent
		<p>b. We are concerned that an E2E service-level BCP with its own requirements may not easily align with department level plans (e.g. an individual IT department plan would need to be adjusted to accommodate every overarching function; a trade processing system would be used E2E yet require multiple descriptions of use in the proposed business function plans).</p> <p>c. Thus, the preference is to further achieve the same goal in highlighting dependencies by capturing the handoffs between individual departments in an E2E process map as opposed to creating a function level plan on top of individual plans. The mapping of E2E processes and dependencies across a service delivery level is a sound principal. That and the identification of dependencies will substantively achieve the same end that the MAS seeks but leave firms the flexibility to achieve it by finding solutions that work within their existing BCM approach. Another preference/option is to achieve the same goal by building function/service oriented plans on the department level (avoids silos) with outputs to indicate lowest business requirements (most aggressive RTO/RPO/requirements) with further flexibility in building the overarching business function plan.</p> <p>Comments on the type and frequency of BCM tests:</p> <ul style="list-style-type: none"> • To the extent that industry wide testing is required, we would appreciate the MAS' help to help to coordinate across FMIs. • Many global institutions adopt global testing cycles, which the Singapore entity needs to be in-sync with. We suggest the MAS to allow more flexibility for testing frequency so that the Singapore entity may adhere to their global calendar and avoid introducing additional risks by testing off the cycle of the FI's global calendar of tests. • IT Resilience Testing is covered in MAS's TRM guidelines. We recommend the MAS align the BCM and TRM requirements to ensure requirements are not duplicative. For example, data restoration from backup media is detailed under IT resilience TRM guidelines (section 8.4.4), this should be aligned with BCM testing requirements. • Noted in Section 6.4 in Annex B of the consultation paper that a FI should conduct a BCP test for each critical business function, at least annually. Considering that there could be a wide range of scenarios and failure modes that can be included in a BCP, it may not be possible to cover all scenarios in a single test. We recommend that a FI to be allowed to adopt a risk-based approach to the scenario to be included in the annual BCP test. This will allow greater focus on the FI's response to each specific scenario. <p>Comments on the conduct of regular BCM audits:</p> <ul style="list-style-type: none"> • Must the BCM audit be a dedicated program audit, or can it be part of the business line function? Some jurisdictions expect a program audit. • Does it refer to an audit of the BCP or BCM? Is such audit expected after the BCM is approved by the Board/senior management committee? • It would be beneficial for the industry if the MAS do not specify that "internal audit" is responsible for conducting BCM audits. We suggest that the MAS retain the broad wording as proposed and leave it up to individual organisations

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>to decide on an appropriate team to discharge the responsibility based on their governance structure and operations.</p> <ul style="list-style-type: none"> • It is requested that the MAS consider that different organisations have different structures and risk assessment processes in place to manage their risks. The typical audit methodology in a financial institution would take into consideration the different risk areas including BCM. We do not recommend the requirement in the draft Guidelines which would require all FIs to build a separate audit process and plan centered around BCM that needs review and approval annually by the Audit Committee. This would be a very specific and narrow focus considering that there is enterprise level risks to be considered and managed for global FIs. We recommend that the MAS allows FIs the discretion to treat BCM like all other risks so that it is subject to the existing established audit framework instead of developing an audit solely around BCM. • We are supportive that there should be regular BCM audit carried out for greater assurance that the FI's BCM is effective. The audit approach should be commensurate with the FI's methodology and internal risk assessment, i.e. risk based. Those with a higher risk rating should have their BCP audited more frequently, while those with a lower risk could audit less frequently. • For BCM audits, certain reliance can also be placed on other audits and reviews, including non-BCM specific audits and reviews. For example, for BCM audits of securities trading, reliance may be placed on a non-BCM specific audit performed on the IT trading systems for that portion of the BCM testing. This will help to avoid duplication of work and help drive greater efficiency in FIs. • Section 6.3 provides an example of testing involving operating in the absence of a key third party service provider. Could the MAS give more detail on its expectations and parameters for such tests? In line with our response to Question 1, an individual FI will not have any control over the BCM planning and testing of FMIs. <p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <ul style="list-style-type: none"> • Implementation adherence and timeline: The MAS Guidelines on Business Continuity requires further detail on the proposed rollout timeframe and roadmap of the requirements. To achieve requirement readiness, it is imperative to ascertain whether the requirements will be implemented entirely on a proposed date or if the MAS will provide for a phased approach. We highly recommend a phased approach. We also seek further details on the factors to drive implementation and timeline/prioritization of deliverables to achieve adherence. If the MAS still insists on full implementation on the implementation date, ASIFMA members request more details on the roadmap/timeline to achieve requirement compliance and clarification on whether the requirements will be implemented across the enterprise or follow a specific cadence • The revised definition of business function, and mapping of E2E processes and dependencies across a service delivery level are fundamentally sound. However, given the extent of potential changes to the existing BCM programs and the size of the firms, such as global firms, we suggest the MAS consider allowing a transition/implementation timeframe of more than twelve months.

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<ul style="list-style-type: none"> • 3rd Party Testing Requirements: The MAS Guidelines on Business Continuity requires further clarification on the scope and the conditions of the 3rd party testing requirements. There is a significant importance placed on demonstrating ability to recover in the case of a supplier outage. As such, we recommend alignment of the third-party testing program with the FFIEC Appendix J guidance on testing requirements, scope, complexity and scenarios. Further guidance is desired if the MAS aims to align with the existing best practices and/or advise on specific requirements. <ol style="list-style-type: none"> a. We request a more complete definition of the 3rd party testing – recommending the definition is in line with the FFIEC Appendix J requirements. b. We request further detail on scope determinants/conditions for the 3rd party testing. • There is currently no industry-wide methodology to measure the success of an RPO for business functions that involve FMIs. Therefore, we would recommend that further guidance be issued on this in consultation with FIs. • Regarding Paragraph 3.2 Business Impact Analysis: This paragraph 3.2 requires Business Impact Analysis (“BIA”) to be performed at least annually. We suggest to the MAS that such BIA be required for “critical” business functions only and less frequently for non-critical business functions. • Regarding Paragraph 3.4 Minimum Performance Level: The minimum performance level per revised guidelines should be measurable, which may suggest that it should be a quantitative statement defining the operating level in a crisis. However, for some functions, qualitative statements may be more suitable to define what needs to be recovered. Can the MAS please clarify that the minimum performance level may be both quantitative as well as qualitative.
7.	Business Continuity Chapter, Singapore Computer Society	<p>General comments: The comments are aggregated feedback received from attendees of the Business Resiliency Exchange & Masterclasses 2019 held on 5 April 2019. A total of 4 responses were received at the time of the close of the feedback session.</p> <p>Comments on the definition of business function: Of the four respondents felt that on a scale of 1 to 5 (5 being extremely difficult to implement), three rated this proposed change to have a rating of 4. One respondent did not rate this question.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Of the four respondents felt that on a scale of 1 to 5 (1 being already in place, 5 being extremely difficult to implement), three rated this proposed change to have a rating of 4. One respondent did not rate this question. The challenge of implementing this was the definition of the allocation of adequate staff and budget.</p> <p>Comments on the scope of a BCP: Of the four respondents felt that on a scale of 1 to 5 (1 being already in place, 5 being extremely difficult to implement), two rated this proposed change to have a rating of 4, one with a rating of 5. One respondent did not rate this question.</p> <p>Comments on the type and frequency of BCM tests:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Of the four respondents felt that on a scale of 1 to 5 (1 being already in place, 5 being extremely difficult to implement), two rated as this is already in place, one rated this proposed change to have a rating of 4 and the remaining respondent rated this as 5.</p> <p>Comments on the conduct of regular BCM audits: Of the four respondents felt that on a scale of 1 to 5 (1 being already in place, 5 being extremely difficult to implement), there was one respondent each which rated this propose change as 2, 3, 4 and 5.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Some guidance on crisis communication with expected datelines for updates. In Section 6.3 of the Consultation Paper, the 5th bullet point proposes that exercises should include relying on power from onsite generators for a prolonged period. It would be good if the Authority can provide some form of guidance as to what is considered 'prolonged period' in Singapore's context that commensurate with the existing infrastructure. For Section 6.10 & 6.11, would the Authority consider including an expectation that auditors that are tasked to conduct a BCM Audit should be adequately trained in BCM? BCM is a distinct discipline but in practice, auditors tasked to do BCM audits are often IT auditors who may not have sufficient understanding of BCM principles. In some circumstances, financial auditors may be tasked to conduct BCM Audits.</p>
8.	Cleartrade Exchange Pte. Ltd	<p>General comments: Cleartrade Exchange is agreeable to the proposed new BCM guidelines and its objectives in the full context with no further comments.</p> <p>Comments on the definition of business function: Agreed with no further comments</p> <p>Comments on the roles and responsibilities of the Board and senior management: Agreed with no further comments</p> <p>Comments on the scope of a BCP: Agreed with no further comments</p> <p>Comments on the type and frequency of BCM tests: Agreed with no further comments</p> <p>Comments on the conduct of regular BCM audits: Agreed with no further comments</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: CLTX has no further comments</p>
9.	Deloitte & Touche Enterprise Risk Services Pte Ltd	<p>Comments on the definition of business function: Section 2 Definition on "Critical Business Function" We note that the Section 2 of the revised guidelines on BCM defines "critical business function" as "a business function which, if disrupted, is likely to have a significant impact on an FI, whether financially or non-financially." We wish to suggest that the definition may be specified to consider: (a) Impact to the FI's resilience to a disruption; and/or</p>

S/N	Respondent	Feedback from respondent
		<p>(b) Recovery priorities while formulating and implementing the appropriate business recovery strategies. Critical business functions should be reinstated first in order to maintain the desired level of product, service or activity delivery.</p> <p>Sub-section (3.2) – Critical Business Functions and Business Continuity Objectives We note that under section 3.2 of the revised guidelines on BCM, MAS may require financial institutions to “... consider the impact of a disruption of their business function on other FIs (e.g. other participants of a payment system) and their customers.” It may be difficult for financial institutions to evaluate and consider the impact of disruption of their business on other FIs given the differences in size, operating environment, risk management philosophy and risk appetite. As an alternative, an FI could be expected to consider how it could be impacted by a disruption, either directly or indirectly (including through possible second round effects via other FIs).</p> <p>Comments on the roles and responsibilities of the Board and senior management: Section (4) – Responsibility of the Board and Senior Management We note that MAS proposed the Board and senior management to demonstrate their commitment in order to build an organisational culture that embeds business continuity as part of an FI’s business-as-usual (“BAU”) risk management.</p> <p>On that note, MAS expects the Board and Senior Management to: (a) Sub-section 4.3(a): review and endorse, “at least annually, the FI’s BCM, as well as ensure that the framework consists of comprehensive policies, processes and procedures, appropriate oversight and escalation elements.” (b) Sub-section 4.3(b): review and endorse, “at least annually, the FI’s critical business functions, business continuity objectives and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place.” (c) Sub-section 4.4(b): The Senior Management should, review, at least annually: (i) The list of critical business functions identified and the appropriateness of their respective business continuity objectives; (ii) The key assumptions underlying the various BCPs; (iii) The extent to which the FI had tested their BCPs and crisis management plans to assure itself that the FI’s business continuity objectives can be achieved in a disruption; (iv) Whether the areas of improvement identified by BCM tests are being appropriately addressed; and (v) The adequacy of the FI’s BCM training programme for new and existing staff. We appreciate that the MAS Guidelines have enunciated a risk-based approach to be taken when a financial institution implements the Guidelines, and respectfully suggest that such reviews should be applicable when there are material changes to businesses and/or business continuity strategy and approach.</p> <p>Sub-section (4.3)(b) – Responsibility of the Board and Senior Management to review at least annually We note that the sub-section 4.3(b) may be misinterpreted as the MAS requiring the Board to “review and endorse, at least annually, FI’s critical</p>

S/N	Respondent	Feedback from respondent
		<p>business functions, business continuity objectives and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place.”</p> <p>MAS may wish to consider indicating explicitly if the expectation to review the business continuity objectives and acceptable residual risk is specific to critical business functions. We wish to also suggest to differentiate requirements specific to critical business functions and other non-critical business functions.</p> <p>Comments on the scope of a BCP: Sub-section (2.15) – “End to end BCP for each service” in addition to “BCPs at the unit, or department, level that relate more to individual process” We wish to seek guidance from MAS in the expectation to have an “end-to-end BCPs ... in addition to the need for BCPs at the unit, or department, level that relate to more individual processes”. Such an approach could hit multiple touchpoints and result in redundancy when it comes to BCP plans and testing, (i.e. consider back end processes around Regulatory Reporting, network or application recovery, database backup and recovery that support across multiple banking products).</p> <p>We seek MAS guidance on: (a) Definition of an “end to end BCP”; and (b) An end-to-end BCP should be sufficient in addressing the needs for BCP at the unit and department level. Hence, we suggest not to duplicate by requiring BCPs at the unit or department level.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Section 2 Definitions on “Disruption” We note that under Section 2 of the Consultation Paper defines the term “Disruption” to mean “when the normal performance of a business function is degraded, resulting in impact to customers. A disruption is not limited to a complete non-availability of a business function, and would include intermittent service availability as well.”</p> <p>We wish to highlight that the definition could be specified to capture any disruption where minimum performance levels of business functions or critical business functions couldn’t be maintained/achieved as opposed to all instances of intermittent service.</p>
10.	Depository Trust and Clearing Corporation	<p>Comments on the definition of business function: The switch to business process is one that is fundamentally sound. However, such a shift in focus will likely cause a change to global and complex BCM programs which may be incompatible with other jurisdictional expectations. The extent of the effort necessary to implement the change is also likely to involve significant effort, and require a project which would unlikely to be achievable within a twelve-month timeframe.</p> <p>Comments on the scope of a BCP: This change incorporates the definition of “business function” established above. The mapping of end to end processes and dependencies across a service delivery level is a sound principle that should be sought. However, the changes necessary to the implementation of such an ambitious initiative will likely be longer than the proposed 12 months. In addition, the maintenance and upkeep to ensure the documentation is updated will in costs that may not be</p>

S/N	Respondent	Feedback from respondent
		<p>fully quantified until a complete impact assessment is undertaken. Implementation of the change in large estates with global multi-jurisdictional coverage in particular could be very costly.</p> <p>Comments on the type and frequency of BCM tests: Testing and exercising should be based on a risk based approach that is core to any BCM program. The proposed prescription may not offer sufficient granularity to take into account the nuanced level of risks that different business functions provide to the sector.</p>
11.	Eastspring Investments (Singapore) Limited	<p>Comments on the roles and responsibilities of the Board and senior management: Paragraph 4.5 of the proposed revised BCM Guidelines sets out that “BCM is part of an FI’s broader operational resilience. Where an FI sets up a committee to oversee its BCM, the committee should thus be led by a senior management member with responsibility over its overall risk (e.g. the Chief Risk Officer).”</p> <p>As set out in paragraph 3.1 of the proposed revised BCM Guidelines, “A business function refers to a service provided to customers of an FI. For this service to be delivered, it will likely require a number of business processes to be performed.” Further, paragraph 2 sets out the definition of “Critical Business Function” where BCP is required, i.e. “A business function which, if disrupted, is likely to have a significant impact on an FI, whether financially or non-financially.” Given business continuity relates to the various function heads who have to ensure the smooth running of an FI’s business operations, we respectfully suggest that the composition of an FI’s BCM Committee be left to the FI’s discretion as appropriate.</p> <p>Comments on the conduct of regular BCM audits: a) It is set out under Paragraph 2.20 of the consultation paper that MAS proposes “for an FI to conduct BCM audits through a unit independent of the staff involved in the planning and execution of the BCM itself (e.g. internal audit)”. We would appreciate MAS’ confirmation that, other than independent BCM audits conducted by the internal audit function and external auditors, regular quality assurance reviews on BCM conducted by an FI’s Regional Head Office BCM function (which is independent of the FI’s staff involved in the planning and execution of the BCM itself), would suffice to meet this requirement.</p> <p>b) Paragraph 2.21 of the consultation paper sets out that “A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI’s Audit Committee. The frequency of BCM audits should be commensurate with the criticality of the business functions.”</p> <p>We would appreciate MAS’ clarification on whether MAS expects a yearly BCM audit plan to be approved by the FI’s Audit Committee and for BCM audits to be conducted at least on an annual basis.</p> <p>We further note that this question seeks comments on MAS’ expectation of FIs to conduct “regular” BCM audits. Separately, MAS has also proposed that “the frequency of BCM audits should be commensurate with the criticality of the business functions”. In this regard, we would appreciate specific guidance from MAS on the expected frequency of BCM audits to be conducted.</p>

S/N	Respondent	Feedback from respondent
		<p>c) In addition, paragraph 2.21 of the consultation paper further sets out that “The FI should submit the BCM audit reports to MAS upon request.”</p> <p>We note from paragraph 1 of the consultation paper that MAS expects FIs “to adopt the Guidelines within a year following its publication”, i.e. a transition period of one year from the issuance date is provided for FIs to adopt the revised BCM Guidelines. Given a BCM audit plan for the coming year is to be developed and approved by the FI’s Audit Committee, we seek MAS’ confirmation that MAS only expects the first BCM audit report to be issued in the coming year per the audit plan, after the issuance of the revised BCM Guidelines. (For example, if the revised BCM Guidelines is issued on January 2020, FIs would need to have an approved BCM audit plan for the year 2021 by the end of 2020. The first BCM audit would then be conducted and the audit report issued in 2021.)</p>
12.	Fidelity International	<p>Comments on the definition of business function:</p> <p>We agree in principle that one should not take a silo approach when identifying business functions that are critical to the organisation. Financial institutions have generally established and conducted BCM planning and analysis along departmental lines for pragmatic reasons (e.g. ease of review and implementation). Notwithstanding, we would like to emphasise that considerable focus is being made on critical processes performed by these departments and how these processes would impact the organisation. Moreover, the interdependency between processes and steps to manage such BCM risks are tested and validated through simulation and/or table-top exercises.</p> <p>The above approaches are consistent with Principle 5 of the current MAS BCM Guidelines, which expects a financial institution to consider the interdependency risk of Critical Business Functions. We are not in favour of changing the definition of “business function” as this introduces complexity to the BCM process and creates unnecessary confusion when a financial institution implements its BCM life-cycle. To illustrate our concerns, the following are potential issues that could arise:</p> <p>1) Creates confusion on the BCM ownership coverage as there will not be a single person/department responsible for performing the Business Impact Analysis (BIA), BCM planning and testing for business functions that cut across various departments. As there will be multiple owners/approvers involved, this do not necessarily ease the implementation of the BIA, BCM planning and testing. One undesired outcome would be that the ownership and approval are being rolled up to the most senior member of the organisation (e.g. CEO or COO). Moreover, for second and third lines of defence (e.g. Compliance, Risk and Audit), where they do not contribute to specific day-to-day business services/processes, it is not clear if they are required to conduct their BIA and to participate at BCM planning/testing.</p> <p>2) MAS’ proposed definition of “business function” is inconsistent with the expectations by most regulators at foreign jurisdictions. This could cause huge implementation challenge and operational costs to global financial institutions because they usually apply group standards on their local operating entities, and their existing BCM systems and methodology are commonly built along “department” lines. Changing their global BCM systems, methodology and templates just to meet Singapore requirements will pose practical challenges and raise the implement costs.</p> <p>Comments on the scope of a BCP:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Please refer our comments to Question 1. The overall recovery process is generally addressed by a financial institution's existing Incident Response and Crisis Management Plan, which are validated during the Crisis Management Team exercises.</p> <p>Comments on the type and frequency of BCM tests: MAS should allow flexibility for financial institutions to determine the types and frequency of BCM tests that commensurate with the nature and complexity of their business. Hence, we do not agree with prescribing specific types and/or frequency of BCM tests. Taking a one size fits all approach by requiring financial institutions to carry out BCM tests once every year appears contrary to MAS' usual stance of allowing financial institutions to calibrate their BCM tests using a risk-based approach.</p> <p>Comments on the conduct of regular BCM audits: Internal Audit normally adopts a risk-based audit cycle methodology. Auditable entities/business functions maintained in the audit universe are regularly risk assessed to determine their risk rating, and thus audit frequencies. As per comments provided to Question 4, we are of the view that financial institutions should have the flexibility to determine the frequency of the BCM audits that commensurate with the nature and complexity of their business. We do not agree that prescribing BCM audits at frequency of least annually is necessarily the right approach.</p>
13.	Holland & Marie Pte. Ltd.	<p>Comments on the roles and responsibilities of the Board and senior management: We believe that an FI's Chief Executive Officer should be responsible for crisis management, involving such other staff as the circumstances of a particular crisis may require. While any business continuity crisis would be handled pursuant to the FI's business continuity plan, other crisis should be the direct responsibility of the Chief Executive Officer. We also believe the FI's Chief Executive Officer should be specifically required to participate in the FI's BCM tests.</p>
14.	HSK Resources Pte Ltd	<p>Comments on the definition of business function: To provide service wholeheartedly to neighborhood residents.</p> <p>Comments on the type and frequency of BCM tests: No comments due to small operations</p> <p>Comments on the conduct of regular BCM audits: No comments due to small operations</p>
15.	IG Asia Pte Ltd	<p>Comments on the definition of business function: MAS proposes to revise the definition of business function to a service that an FI ultimately provides to its customers.</p> <p>- Please provide more examples, other than the "securities trading" business function of a brokerage, to give greater guidance</p> <p>Comments on the roles and responsibilities of the Board and senior management: For many FIs, their Group board ensures appropriate governance and oversight of business continuity and there may be Group committees and CMT established to oversee BCM in compliance with the jurisdictional requirements</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>of the Group. For local entities that have small teams, could they satisfy the requirements as being part of the wider overall Group oversight and governance BCM framework?</p> <p>Comments on the conduct of regular BCM audits: Taking the example of small local entity offices, would the overall Group audit count towards fulfilling the local entity audit obligation?</p>
16.	Investment Management Association of Singapore	<p>Comments on the definition of business function: The revised definition of business function identifies a number of business processes which in turn may identify multiple departments that own the processes. When assigning ownership to fulfil business continuity requirements (e.g. risk assessment, contingency planning), this may dilute the accountability as compared to an organizational line (e.g. by department or unit) approach. As the business nature of each FI is different, the guidelines can keep it open for FIs to choose whether to segregate by organizational lines or service that best suits its business structure. Some business functions might be missed out if the definition is based on service that an FI ultimately provides to its customer. We propose for the definition to allow FI to have the flexibility and discretion to establish business functions along organizational lines and services as long as the dependencies among processes have been captured and identified.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Paragraph 2.11 We propose to remove the example of “Chief Risk Officer”. The senior management member with responsibility may not necessarily be the risk officer and depends on the organisation’s set up and structure. Paragraph 2.13 Please clarify if training for CMT members conducted by internal parties is acceptable or whether engaging external professional trainers is expected. ANNEX B – Revised Guidelines on BCM</p> <p>Referring to</p> <ul style="list-style-type: none"> • Paragraph 2 - “Critical Business Function” where BCP is required, i.e. “A business function which, if disrupted, is likely to have a significant impact on an FI, whether financially or non-financially.” • Paragraph 4.5 - “BCM is part of an FI’s broader operational resilience. Where an FI sets up a committee to oversee its BCM, the committee should thus be led by a senior management member with responsibility over its overall risk (e.g. the Chief Risk Officer).” • Paragraph 3.1 - “A business function refers to a service provided to customers of an FI. For this service to be delivered, it will likely require a number of business processes to be performed.” <p>Given that business continuity relates to the various function heads who must ensure the smooth running of an FI’s business operations, we suggest the composition of an FI’s BCM Committee to be left to the FI’s discretion as appropriate.</p> <p>Comments on the conduct of regular BCM audits: Paragraph 2.20 Referring to MAS’ proposal “for an FI to conduct BCM audits through a unit independent of the staff involved in the planning and execution of the BCM itself (e.g. internal audit)”. We would appreciate MAS’ confirmation on the following, please:</p> <p>a) Audits performed by external auditors would fulfil the expectation of</p>

S/N	Respondent	Feedback from respondent
		<p>conducting regular BCM audits.</p> <p>b) Other than independent BCM audits conducted by the internal audit function and external auditors, regular quality assurance reviews on BCM conducted by an FI's Regional Head Office BCM function (which is independent of the FI's staff involved in the planning and execution of the BCM itself) would suffice as well.</p> <p>Paragraph 2.21</p> <p>a) Referring to "A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI's Audit Committee. The frequency of BCM audits should be commensurate with the criticality of the business functions."</p> <p>We would appreciate MAS' clarification on whether MAS expects a yearly BCM audit plan to be approved by the FI's Audit Committee. We further note that this question seeks comments on MAS' expectation of FIs to conduct "regular" BCM audits. Separately, MAS has also proposed that "the frequency of BCM audits should be commensurate with the criticality of the business functions". In this regard, we would appreciate specific guidance from MAS on the expected frequency of BCM audits to be conducted, such as whether it would suffice for BCM audits to be conducted at least once a year.</p> <p>b) Referring to "The FI should submit the BCM audit reports to MAS upon request."</p> <p>We note from paragraph 1 of the consultation paper that MAS expects FIs "to adopt the Guidelines within a year following its publication", i.e. a transition period of one year from the issuance date is provided for FIs to adopt the revised BCM Guidelines.</p> <p>Given a BCM audit plan for the coming year is to be developed and approved by the FI's Audit Committee, we seek MAS' confirmation that MAS only expects the first BCM audit report to be issued in the coming year per the audit plan, after the issuance of the revised BCM Guidelines. (For example, if the revised BCM Guidelines is issued on January 2020, FIs would need to have an approved BCM audit plan for the year 2021 by the end of 2020. The first BCM audit would then be conducted and the audit report issued in 2021.)</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <p>We propose for MAS to provide more practical examples of the minimum performance level which must be recovered by the RTO as stated in paragraph 3.3 under ANNEX B</p> <p>– Revised Guidelines on BCM.</p>
17.	KPMG Services Pte Ltd	<p>Comments on the definition of business function:</p> <p>With the release of the proposed revisions to Guidelines on Business Continuity Management ("BCM"), we noted that MAS has placed greater emphasis on business resiliency with regards to responding to emerging cyber threats.</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>KPMG recommends that the definition of business function should not be limited to the services being provided to the customer, but should also cover supporting services, which may be critical in order to meet the requirements of the customers (e.g.: IT).</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Comments on the conduct of regular BCM audits: KPMG recommends regular audits on Business Continuity Management. The independent audit and/or expert assessment may be performed by the FI's internal auditor or external consultants. The addition of external consultants will allow some FIs that lack resources and/or skills to review BCM processes to augment their internal capabilities. Furthermore, the scope of the audit should include an evaluation of any outsourcing arrangement that supports critical business functions.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: MAS Technology Risk Management ("TRM") Notice requires 4 hours Recovery Time Objective ("RTO") for MAS critical systems. KPMG recommends MAS to consider elaborating this requirement in the MAS Business Continuity Management ("BCM") Guidelines.</p> <p>Furthermore, we recommend MAS to:</p> <ul style="list-style-type: none"> - Reference the Security Incident Response Plan requirement in MAS TRM Guidelines to the recovery process of MAS BCM Guidelines; - Provide guidance on the financial and non-financial impact of the business functions in the Business Impact Analysis. This should also cover (but not be limited to) operational, financial, legal and regulatory, reputational and customer impact; - Explicitly extend the MAS BCM requirements to the outsourced service providers supporting critical business functions.
18.	LIA (AIA)	<p>General Comments: 1. The guidelines require clarity when differentiating the requirements for service and business functions. The term seems to be used interchangeably and confusing if we were to adhere to the guidelines. As such, we suggest that it is better to have a separate definition for service instead of lumping it all together.</p> <p>We propose to add a new definition "Service" instead of revising the definition of business function. The definition of Business Function should stay put, as it is a universal BCM term which is applicable throughout the organisation.</p> <p>A Service or Critical Service can be mapped to several business functions. A Service or Critical Service can be supported by multiple business functions. Examples of a Critical Service could be:-</p> <ol style="list-style-type: none"> 1.1 Claims Processing and Payment 1.2 Premium Collection and Policy Payment 1.3 Call Centre and Counter Services <p>2. Will MAS be linking or aligning MAS Notice 127 to the business function as set out in the guidelines? For example, an application for online policy premium payments is down, would this be considered an IT incident in MAS Notice 127 context?</p> <p>Comments on the definition of business function: 1. Annex B, Paragraph 3.1 A business function refers to a service provided to customers of an FI. For this service to be delivered, it will likely require a number of business processes to be performed. Not all business processes in the FI can be tagged clearly to a service provided to customers e.g. HR functions (Staff Payroll) or Administrative functions (Strategic Planning). These are departments with no interaction with customers. How should they be documented under the new proposed guidelines?</p>

S/N	Respondent	Feedback from respondent
		<p>2. Annex B, Paragraph 3.4 FIs should ensure that the minimum performance level for each business functions is suitably defined, clear and measurable. Are there examples of the minimum performance level?</p> <p>3. Annex B, Paragraph 3.5 FIs may face scenarios where the performance of a business function is intermittent. This may arise, for example, due to intermittent network connectivity or faulty hardware, and the root cause may not be immediately apparent. To manage such scenarios, FIs should have monitoring capabilities that will enable prompt detection of reduced or intermittent service availabilities and clearly articulate triggers for the activation of contingency plans (e.g. fail over to a secondary data centre). These triggers should take reference from the minimum performance level for a given business function.</p> <p>If the main point of this paragraph is to use the minimum performance level for a given business function to trigger the activation of contingency plans or to highlight the need for established monitoring capabilities, this paragraph should focus on these points and not the type of scenario (due to intermittent network connectivity or faulty hardware).</p> <p>Comments on the roles and responsibilities of the Board and senior management: Paragraph 2.11 BCM is part of an FI's broader operational resilience. Where an FI sets up a committee to oversee its BCM, the committee should thus be led by a senior management member with responsibility over its overall risk (e.g. the Chief Risk Officer). In this regard, is there any expectation on how the BCM function to be set up?</p> <p>Comments on the scope of a BCP: 1. See earlier comments related to the new proposed Business Function as described in our response to Point 1.</p> <p>2. Annex B, Paragraph 5.1 ... BCPs are typically established at the organisational unit level (e.g. by department or unit), but should also be established at the business function level. BCPs should cover the full recovery process: immediate response to the resumption of output to minimum performance levels, and the subsequent restoration to BAU levels. This chapter focuses on business functions, but the same principles apply to unit-level BCPs.</p> <p>Having an end-to-end BCP in addition to BCPs at unit, or department, level duplicates the effort of documentation required. We suggest that if the end-to-end approach is preferred, it should form the main BCP document with supplementary material for additional areas which may not be addressed.</p> <p>3. Paragraph 2.15 ... We propose for FIs to review and, where necessary, enhance the robustness and comprehensiveness of their BCPs by covering the full recovery process for a given business function from immediate response to the resumption of business functions to minimum levels, and the subsequent restoration to BAU levels.</p> <p>Does Paragraph 2.15 mean:- (i) Each service is required to indicate minimum performance level or/and (ii) Each business function is required to indicate minimum performance level or/and</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>(iii) Each department is required to indicate minimum performance level i.e. multiple business functions but single minimum performance level. The paragraph indicates that MAS requires FIs to cover the full recovery process for a given business function from immediate response to resumption to BAU. Does it mean MAS also requires FIs to cover the full recovery process for a service from immediate response to resumption to BAU?</p> <p>Comments on the conduct of regular BCM audits:</p> <p>1. Annex B, Paragraph 6.11 ... A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI's Audit Committee. The frequency of BCM audits should be commensurate with the criticality of the business functions. We are of the opinion that a separate BCM audit plan may not be necessary as BCM should already be an auditable area which is assessed for audit coverage on a rotational basis based on the severity and likelihood of risk. We suggest that the proposed guidelines should instead require "An audit plan, comprising BCM as one of the auditable areas of the coming year, should be developed by the FI. The audit plan should be approved by the FI's Audit Committee. The frequency of BCM audits should be commensurate based on the audit risk assessment result."</p> <p>2. Annex B, Paragraph 6.11 An FI should also ensure that the scope of BCM audits is sufficiently comprehensive and includes all critical business functions.</p> <p>In regard to the scope of coverage for the audit on BCM, we suggest to revise to "An FI should also ensure that the scope of BCM audit includes the evaluation of the effectiveness of the internal controls relevant to BCM, including governance over the identification and BCM drills of the critical business functions." This would provide a proper coverage on the overall BCM controls framework including assessing whether management has governance process in place to ensure the critical business functions have been identified, sufficiently and comprehensively covered in the BCM drills.</p>
	LIA (Aviva)	<p>General Comments:</p> <p>We would like to seek clarity on some of the proposed changes so as to better understand MAS' expectations as outlined in the consultation paper. This will help in ensuring appropriate process are put in place to comply with the revised Guidelines when it takes effect.</p> <p>Comments on the definition of business function:</p> <p>Comments on the definition of business function:</p> <p>Paragraph 2.5 MAS proposes to revise the definition of business function to a service that an FI ultimately provides to its customers. We agree with the definition of "business function". However, we would like to seek clarity as there may be department(s) with processes that do not directly support any service(s) to FI customers. Is the scope of definition intended to cover this?</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>Paragraph 2.9 ... To achieve this effectively in the current threat environment, we propose that the Board take on additional responsibilities to:</p> <p>a) Review and endorse, at least annually, the FI's BCM, as well as ensure that the framework consists of comprehensive policies, processes and procedures, appropriate oversight and escalation elements;</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>b) Review and endorse, at least annually, the FI's critical business functions, business continuity objectives and the level of residual risk it is willing to accept after the relevant business continuity measures have been put in place; and</p> <p>c) Satisfy itself that adequate resources, including budget, technology, and staff are allocated to facilitate the implementation of an effective BCM.</p> <p>From a risk perspective, we agree on the involvement of the Board. However, we would like more clarity on the extent of involvement required by the Board in the endorsement and review of the BCM, processes and procedures.</p> <p>Comments on the scope of a BCP: MAS proposes that the BCP covers dependencies for a service, and spell out the recovery process from immediate response to minimum levels and BAU levels, and this sits on top of BCPs at the unit, or department, level that relate more to individual processes. Can the service-level BCP document be a high level BCP that maps the interdependencies of the various business processes, while the individual unit/department's BCP would be made reference to/for the detailed recovery processes and objective? The high level BCP would then be co-signed off by the various process owners in relation to the service rendered. In addition, with reference to Point 2 above, we would like to seek MAS' guidance in relation to the Board's responsibility in the review of both the overarching high-level BCP and individual department's detailed BCP.</p> <p>Comments on the type and frequency of BCM tests: We agree with the proposed type and frequency of BCM tests.</p> <p>Comments on the conduct of regular BCM audits: Annex B, Paragraph 6.10 An FI should develop an audit process for greater assurance that their BCM is effective. Is there an expectation for FIs to develop a separate audit process in relation to BCM?</p> <p>Annex B, Paragraph 6.11 ... A BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The BCM audit plan should be approved by the FI's Audit Committee. Is there an expectation to develop a separate audit plan specifically on BCM?</p> <p>In addition, further clarification on "auditable areas" in relation to BCM will give better understanding to the requirements.</p>
	LIA (Etiqua)	<p>Comments on the definition of business function: Paragraph 2.5 MAS proposes to revise the definition of business function to a service that an FI ultimately provides to its customers.</p> <p>The proposed definition of business function only include services that FIs ultimately provide to their customer. Should the business impact analysis include back-end support functions or routine tasks that a department need to complete and meet its responsibility within FI? E.g. Information Technology, Human Capital, Procurement and etc</p> <p>Comments on the roles and responsibilities of the Board and senior management: Besides implementation, it is recommended that the Board shall be ultimately responsible to provide oversight and ensure the maintenance of an effective BCM programme.</p> <p>Comments on the scope of a BCP:</p>

S/N	Respondent	Feedback from respondent
		<p>Annex B, Paragraph 5.8 Where recovery arrangements rely on other stakeholders, such as intra-group partners and third party vendors, formal service level agreements (SLAs) should be established and the appropriate redundancies agreed upon.</p> <p>We believe the existing SLA between FI and vendor would have covered the needs of FI in handling daily BAU activities. In addition, there is a challenge for FI to negotiate the SLA with common infrastructure providers (e.g. telecommunication providers) in terms of testing participation and recovery time objectives. As such, the need of having explicit SLAs to support FI's BCP is not necessary.</p> <p>Comments on the type and frequency of BCM tests: Paragraph 2.19 MAS continues to expect an FI to conduct different types of testing to gain the confidence that they will be able to continue to operate reliably, responsively, and efficiently as planned. Specifically, an FI should, at minimum, conduct the following annually:</p> <ul style="list-style-type: none"> • A crisis management and communications exercise involving all CMT members and their alternates; and • A test relating to the BCP for each critical business function. <p>Test plans should be equipped with predetermined test goals and test criteria, using near to realistic simulations. Since the Board is ultimately responsible for the implementation of BCM programme, test objectives should be approved by the Board to ensure proper alignment with the expectation of Board in reflecting to the evolving risk environment of an FI.</p> <p>It stated that communication exercise involving all CMT members and their alternates should be conducted annually. It is recommended that more clarity to be provided on the communication exercise. E.g. call-tree activation only, communication with external parties and etc.</p> <p>Further, the requirement in Paragraph 6.3 in Annex B on operating from a disaster recovery site for a defined duration may be a potential challenge to smaller scale FIs due to resources constraints (i.e. manpower and budget). These wordings should be refined to ensure the feasibility of all FIs in planning for upcoming BCP testing exercise. Nevertheless, it is recommended that the type and frequency should also be approved by Board annually to ensure proper alignment with the expectation of Board in reflecting to the evolving risk environment of an FI.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: It is observed the proposal Guidelines contain various terminologies used to define alternate site of primary business premise of FI (i.e. alternate site, disaster recovery site, recovery site, and secondary site). To avoid any confusion and ensure consistency, it is recommended that the same terminology is used throughout.</p>
	LIA (FWD)	<p>Comments on the definition of business function: Paragraph 2.5 MAS proposes to revise the definition of business function to a service that an FI ultimately provides to its customers. For this service to be delivered, it will likely require a number of business processes to be performed. For example, the "securities trading" business function of a brokerage could entail the following processes: (i) Trade Initiation; (ii) Trade Execution; (iii) Trade Capture; (iv) Trade Validation; (v) Trade Agreement; (vi) Trade Settlement; and (vii) Trade Reconciliation. Each process, in turn, requires specific resources and expertise (e.g. IT systems, personnel) to be performed.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Business function could be misleading and create confusion among the departments. The new definition is meant on Critical Business Process which may be performed across three to four Business Functions. Suggest to change it to Critical Business Process.</p> <p>Currently, the BCP is drafted under each Department which specified the critical process for the department. Is our understanding correct that it is still the same or the BCP should be drafted as per Critical Business Process (i.e. each Critical Business Process required one detailed BCP)?</p> <p>Comments on the roles and responsibilities of the Board and senior management: Paragraph 2.13 An FI should review the adequacy of training for CMT members at least annually and ensure that they are competently prepared for their roles and responsibilities.</p> <p>Is the annual BCP testing sufficient to address as the training program to the staff? A Call Tree exercise and fire evacuation exercise for example would involve all of the staff including new staff, however, the specific BCP testing might not require all staff to perform testing in the alternate site.</p> <p>Comments on the scope of a BCP: Paragraph 2.17 An FI should establish a formal training programme to ensure that all relevant personnel are familiar with their roles and responsibilities in relation to a BCP. The adequacy of training for all relevant staff should also be reviewed at least annually.</p> <p>Is the annual BCP testing sufficient to address as the training program to the staff? A Call Tree exercise and fire evacuation exercise for example would involve all of the staff including new staff. However, the specific BCP testing might not require all staff to perform testing in the alternate site.</p> <p>Comments on the type and frequency of BCM tests: Seek clarification with MAS on frequency of test for non-critical business function.</p> <p>Comments on the conduct of regular BCM audits: Paragraph 2.21 ... The frequency of BCM audits should be commensurate with the criticality of the business functions.</p> <p>We are of the view that the regular BCM audit frequency should depend on the size of the FI instead of criticality of the business functions. For example, Tier 1 insurers should conduct the BCM audit once every 2 years and Tier 2 Insurance Company to conduct the audit once every 3 years.</p>
	LIA (Manulife)	<p>Comments on the definition of business function: Seek clarification from MAS on function that has no relation to customers of an FI.</p> <p>Comments on the conduct of regular BCM audits: Seek clarification from MAS on the frequency of BCM audit for an FI.</p>
	LIA (NTUC Income)	<p>General comments: 1. Annex B, Paragraph 2: Definitions – Minimum Performance Level We would like MAS to advise if there is any benchmark for the evaluation of performance level. 2. Annex B, Paragraph 2: Definitions – Residual Risk</p>

S/N	Respondent	Feedback from respondent
		<p>We would like MAS to advise if there is any benchmark on levels of “residual risks” and “extended period of time”.</p> <p>Comments on the definition of business function: Annex B, Paragraph 3.1 A business function refers to a service provided to customers of an FI. We would like MAS to advise on the term “customers” in the definition of business function. Does it include both internal and external customers?</p> <p>Comments on the scope of a BCP: 1. Annex B, Paragraph 5.11: Notification to MAS on disruption of critical business function We would like MAS to advise/share the instructions on incident notification and reporting to MAS. 2. Annex B, Paragraph 5.14: Relevant portions of communication plan to align with the crisis communication protocols established by industry associations We would like MAS/LIA/GIA to share the crisis communication protocols established by the industry associations with the FIs. 3. Annex B, Paragraph 5.18: Formal training programme and adequacy of training We would like MAS to advise/share on the benchmark for assessing training adequacy and examples of training programme.</p>
	LIA (Tokio Marine Life)	<p>General Comments: Making reference to Principle 6 of the existing BCM Guidelines: “Institutions should plan for wide-area disruptions.” and Principle 7 of the existing BCM Guidelines: “Institutions should practise a separation policy to mitigate concentration risk of critical business functions.”</p> <p>We note that the majority of principles 6 and 7 have been diluted from this proposed revision. Our company opines that these are still important principles that FIs should strive to uphold. In leaving principles 6 and 7 out, MAS may unintentionally be giving the incorrect impression that these principles are no longer relevant to the financial sector. These principles, for example, can be included in an appendix under good practices that a FI should consider as well, or weaved into the reorganised sections of the guidelines.</p> <p>Comments on the definition of business function: There should be more clarity over the definition of a “business function”. This is because stating that it is “a service that an FI ultimately provides to its customers” can be rather vague. Indirect services, such as the Investment function of an insurer, may inevitably fall outside the scope, which we believe is not the intention of MAS. In addition, simple and mundane services, such as the provision of cheque books, may be deemed “business function” under the revised definition.</p> <p>Our company suggests that MAS retain “business function” as it is, but to come up with an acronym, such as “Business Function and Interdependent Processes” (BFIP), to highlight (where necessary) the focus of the requirements. For example, for paragraph 3.2 in Annex B, it can be reworded as “In a crisis, it might not be practical to recover all BFIP at the earliest opportunity”.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Annex B, Paragraph 4.4(b)(iii)</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>It may be hard to demonstrate and review the “extent to which an FI had tested their BCPs”. Instead, we propose to reword the clause to “The completeness and comprehensiveness to which the FI had tested their BCPs... achieved in a disruption. In addition, where there are parts that were not tested due to certain reasons, FIs are to introduce mitigating controls to reduce the risks that arise from it.”</p> <p>Comments on the scope of a BCP: Paragraph 2.15 and Annex B, Paragraph 5.1 Establishing an end-to-end BCP for business functions is a good enhancement to the comprehensiveness and robustness of the current BCPs that most FIs have developed. However, it may not be practical and too complicated to establish it for each business function and interdependent process. We would like to propose clarifying this clause to be applicable only to business functions and interdependent processes that the FI deems to be critical in the provision of key services to its customers. Annex B, Paragraph 5.9 ... but reasonable steps should still be taken to provide assurance ... in disruptions.</p> <p>We propose the following changes to provide more clarity to FIs: “... but reasonable steps should still be taken for FIs to satisfy themselves that key service providers can support their businesses even in disruptions. An example of such assurances includes requiring service providers to obtain relevant industry certifications.”</p> <p>Comments on the type and frequency of BCM tests: Paragraph 2.19 and Annex B, Paragraph 6.4 It may not be practical to conduct a BCP test for each critical business function annually. Instead, we propose that BCP tests be conducted to focus on different critical business functions annually, and to ensure that all critical business functions are tested over a predefined number of years.</p> <p>Comments on the conduct of regular BCM audits: Paragraph 2.21 and Annex B, Paragraph 6.11 Ensuring that audits are conducted on critical business functions is a good enhancement to ensure the quality and comprehensiveness of BCPs. However, instead of having separate and standalone BCM audits on critical business functions, it would be more practical to incorporate the auditing of critical business function’s BCP as part of the normal business audits that the Internal Audit Department conducts during BAU.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: We hope that MAS can provide further guidance with regard to the level of BCM requirements FIs should put in place to ensure that their vendors uphold their responsibilities and the level of joint/combined testing that should be performed with the FI’s vendors (e.g. should sub-contractors also need to be involved in joint testing?).</p>
	LIA (Transamerica Life)	<p>Comments on the scope of a BCP: Annex B, Paragraph 5.9 Some interdependency risks are beyond an FI’s direct control to mitigate completely (e.g. unavailability of telecommunications networks, etc.), but reasonable steps should still be taken to provide assurance that key service providers are capable of supporting their businesses even in disruptions.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>With respect to interdependency risks beyond FI's direct control, e.g. unavailability of telecommunications network, a general assumption in local BCM framework is that core public infrastructure such as utilities (water, electricity) and those of monopoly in nature, would remain available in event of a crisis impacting FI. It may be inefficient for individual FI to approach those service providers to assess BCM standard and their disaster recovery service level. It would be helpful if MAS could provide further guidance in terms of the extent of assurance FIs are expected to obtain from those service providers of this nature.</p> <p>Annex B, Paragraph 5.14 Relevant portions of these communication plans should be aligned with crisis communication protocols established by industry associations so that there is consistent messaging to the public in a wide-spread disruption. Suggest further guidance on relevant protocols described in paragraph 5.14.</p> <p>Comments on the conduct of regular BCM audits: We would like to confirm our interpretation that the expected regularity of BCM audit can be aligned with FI's risk profile and internal audit roadmap based on risk priorities / maturity of the company, i.e. not necessarily on an annual basis.</p>
19.	Lloyd's of London (Asia) Pte Ltd	<p>Comments on the definition of business function: We agree that a focus on the continuity of business services is an appropriate approach for FIs that are material to the operational resilience of the financial system and may add value to other firms when considering operational resilience.</p> <p>At Lloyd's in Singapore, the continuity of services rests not only with Lloyd's but also the managing agents and brokers. Accordingly, we agree that the business function is appropriate to mean the service that the "FI provides to the customer".</p> <p>Comments on the roles and responsibilities of the Board and senior management: We agree with the board and senior management roles and responsibilities. It is important that they take ownership of the function and provide strategic direction. Currently, business continuity is signed off annually by senior management including business impact analysis data, plans and exercising. This is then fed into the overall Lloyd's business continuity function operated from London so that the Executive Risk Committee are also informed.</p> <p>Comments on the scope of a BCP: Lloyd's is fully supportive of producing business continuity plans and testing along critical business service lines. There are already detailed business continuity plans in place at the process level and for crisis management purposes. There is also a clear escalation process to the Corporation crisis management teams who can provide additional support. Key roles have been trained for this purpose. To ensure robustness, it is agreed that the identification of plausible scenarios and interdependencies of systems and processes through the risk assessment process will ensure an acceptable level of continuity of service provision.</p> <p>Comments on the type and frequency of BCM tests: Lloyd's has a comprehensive business continuity and crisis management testing programme in place. This includes annual remote working, crisis management</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>and business recovery exercises. A disaster recovery testing regime is in place for all critical systems in use. Information regarding the efficacy of the business continuity arrangements in place are submitted as part of the quarterly reporting to the Executive Risk Committee.</p> <p>It should be noted that the provision of end-to-end service provision is provided by a number of individual entities which will require further co-ordinated testing.</p> <p>Comments on the conduct of regular BCM audits: BCM audits are an essential part of any business continuity regime. Agree with the expectation to conduct regular BCM audits.</p>
20.	Marsh (Singapore) Pte.Ltd.	<p>Comments on the definition of business function: While Marsh(Singapore) Pte. Ltd agrees with the definition proposed by MAS regarding critical business function (Clause2.2,2.5 &2.6), we would prefer the guideline to be non-prescriptive which allows organizations the flexibility to scope/structure their business entity for business continuity planning and documentation.</p> <p>Comments on the scope of a BCP: It is in our view that Intermittent Outages (Clause 2.7) are under the technology regime already incorporated in the TRM guideline. Business Continuity Management guideline should focus its coverage in the risk management arena dealing with accidental and sudden operational disruption/outages. Planning effort should be focused on worst case scenario.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: MAS should consider sector specific guidelines, for example, Insurance Broking versus Banking and Finance. This would help focus regulation to risk.</p>
21.	Marsh Management Services Singapore Pte Ltd	<p>Comments on the definition of business function: For captive and SPRV insurers, the key business functions comprise insurance, claims, accounting and compliance. There is no headcount for these entities as the operations of these entities are typically outsourced to an insurance manager.</p> <p>Under the Outsourcing Guidelines, business continuity management is one of the risks identified for the Board and the senior management to review, assess and ensure that it is appropriately in place. Therefore, the Board and the senior management will need to agree the minimum performance level with the outsourced service provider.</p> <p>Comments on the roles and responsibilities of the Board and senior management: While it is important for the Board and senior management to have an oversight of the BCM function, given that it is outsourced, it is important that the Board and senior management are kept informed of the BCM policies of the outsourced service provider; i.e. including the type and frequency of the test. That said, as noted above, the outsourcing guidelines cover this aspect so we do not believe there is anything further required. Given the nature of captives and SPRV, they do not have public interest elements and often the potential issues from BCM events are limited due to the infrequent nature of policy issuance and a lighter regulatory touch.</p> <p>Comments on the scope of a BCP:</p>

S/N	Respondent	Feedback from respondent
		<p>Refer to answer in Qn#2</p> <p>Comments on the type and frequency of BCM tests: Refer to answer in Qn#2</p> <p>Comments on the conduct of regular BCM audits: Given that the risks underwritten by captives are all in house corporate risks and unlikely to affect the general public who are not the stakeholders or interested parties of the captives, we are of the opinion that regular BCM audits are not required.</p> <p>Having said that, the Board and the senior management should be kept informed at all times of the BCM policies and plan that its service provider have in place to ensure there is no lapse in the continuity of their service; i.e. in the form of an attestation. This forms part of the annual outsourcing review that is conducted by the Board of the captives as we believe is sufficient for these types of vehicles.</p> <p>The same would apply to SPRV structures, as once they are established, there is limited on going transactions that are susceptible to BCM issues (as there are various failsafe's in place).</p>
22.	Microsoft Operations Pte Ltd.	<p>General Comments: Microsoft would like to thank the Monetary Authority of Singapore (the "MAS") for the opportunity to provide comments on the proposed revisions to Guidelines on Business Continuity Management ("BCM"). Microsoft supports the purpose and the risk-based approach of the revised BCM Guidelines and views this as a positive step by MAS to highlight the importance of appropriate BCM by financial institutions. Accordingly, Microsoft has only minimal suggested revisions to the BCM Guidelines.</p> <p>Comments on the scope of a BCP: While Microsoft agrees with the proposal by the MAS for financial institutions to have robust business continuity plans, the proposed Section 5.8 of the BCM Guidelines is not practical in the context of financial institutions' engagement of cloud service providers ("CSPs").</p> <p>First, the obligations for RTOs to be set forth in service level agreements is not feasible for most hyperscale CSPs. Such an obligation implies that RTOs can be negotiated with each customer, which is not possible in the context of hyperscale cloud services.</p> <p>RTOs speak to catastrophic loss only. RTOs can vary from configuration to configuration and, by definition, deal with catastrophic scenarios outside of normal operations, and therefore should not be included in standard service level agreements.</p> <p>For our PaaS/IaaS offering, we offer technical configuration options to give the customer choice in how it designs for high availability and disaster recovery. The RTO/RPO is always down to the design of the application by the customer.</p> <p>With respect to SaaS, our service operates using an active configuration with immediate failovers built-in. Such a configuration allows the service to meet a high resilience design and cope with blackswan events such as total loss of datacenter(s).</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Hence, in this context, RTO/RPO is not considered a valid metric for evaluating active/active configurations or for services like Exchange Online, as this service is built to targets for near instant failover and zero data loss. In on-premise scenarios having clear RTO and RPO measures (at service) make sense as organizations need to understand how to manually bring the service back and/or failover to the DR site. The reason the metric makes sense in this context is that on-premise software is typically built in an active/passive configuration perhaps using offline tape backup for rollback/recovery.</p> <p>Accordingly we recommend that the requirement in 5.8 that the parties “set[] specific and measurable recovery expectations (e.g. RTOs) and “redundancies agreed upon” be deleted. Instead, MAS could require financial institutions understand the CSPs’ RTOs/redundancies, rather than requiring that they be negotiated or agreed on, or put into service level agreements.</p> <p>Second, it is neither universally necessary nor feasible for CSPs to contractually commit to joint testing of their BCPs. 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.</p> <p>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.</p> <p>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.”</p> <p>Likewise, CSPs should not be required to be involved in BCM exercises with financial institution customers. Financial institutions and CSPs have their own BCM practices in place, which they exercise independently. Given the volume of customers, CSPs would not be able to participate in the BCM exercises of all of their financial institution customers.</p> <p>In light of the above, we recommend for this proposed section 5.8 to be deleted in its entirety. The relevant principles are covered in 5.7 and 5.9.</p>
23.	MUFG Bank, Ltd.	<p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> With reference to the definition of the “Business Function refers to a service provided to customers of an FI” in clause 3.1. We made comparisons to the International Standards on Business Continuity Management (i.e. ISO 22301) and APRA Prudential Standard CPS 232 Business Continuity Management and we noted the difference in the meaning below. Though business functions are not defined specifically in the standards, the substance that draws from the definition in the international standards is different from the interpretation written in the MAS Consultation paper. We would like to clarify if MAS has any intention to align the following standards on the definition of a “business functions”. <p>APRA Standards: “Critical business operations are the business functions...”</p> <p>ISO 22301:</p>

S/N	Respondent	Feedback from respondent
		<p>“Organization – person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.”</p> <p>“Products and Services – Beneficial outcomes provided by an organization to its customers, recipients and interested parties.”</p> <ul style="list-style-type: none"> On clause 3.5, we noted examples of the Technology Risk Management resilience. We would like to suggest for MAS to provide more specific guidance on resilience from the BCM guidelines’ perspective. <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ul style="list-style-type: none"> There are “adequacy”, “relevant”, “appropriateness” elements throughout the guidance. We propose that all the considerations to be consistent throughout the guidelines to avoid confusion of what is expected of an FI. For example: clause 4.4 says “Senior management... should participate actively in the FI’s BCM tests”, clause 6.6 says “Senior management... should participate in all relevant tests”. We would also like to highlight that the reference to Para 3.5 for definition of business continuity objectives in Footnote 4 is incorrect. <p>Comments on the scope of a BCP:</p> <p>On clause 5.1, it says that “BCPs are typically established at the organizational unit level (e.g. by department or unit), but should also be established at the business function level.” “Business Functions” refers to Processes and Activities performed in the organization.</p> <p>We would like to clarify if MAS is expecting a Business Continuity Plan for every business function identified in the FI.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <p>On 5.11: Per Circular SRD BCM 01/2006 indicates: “Financial institutions are reminded to inform MAS’ supervisory officers immediately of the occurrence of an emergency where business operations are or will be severely disrupted, as well as once their contingency plans have been activated...” We interpret 5.11 to mean that a first notification should be made immediately upon discovery of occurrence; followed by subsequent updates of mitigations implemented.</p> <p>If this is the intention, we propose for 5.11 to read: “FIs should notify MAS immediately upon discovery of the disruption of a critical business function. FIs should subsequently provide information on the assessed impact on its customers and the actions that have been taken (alternative service channels, media engagement, etc.) to MAS in a prompt manner.”</p> <p>We further propose to include that: “FIs should abide by the reporting timelines set out in other relevant MAS notices. For example, Notice on Technology Risk Management [Notice No. CMG-N02], in the event of IT incidents.”</p>
24.	LIA member Old Mutual International	<p>General comments:</p> <p>Require clarity as to how MAS will apply these guidelines in respect of branch offices in Singapore with main offices outside of the country.</p> <p>Comments on the definition of business function:</p> <p>Agree with the concept and approach.</p>

S/N	Respondent	Feedback from respondent
		<p>Use of business function to mean service is likely to cause confusion, in addition, function is defined differently across industries and regulators again creating the potential for confusion.</p> <p>Comments on the roles and responsibilities of the Board and senior management: The level of oversight and requirements proposed will ensure visibility and accountability by both the Board and senior management, however consideration as the scale of the business should be made.</p> <p>Comments on the scope of a BCP: The proposal to move from process to service focused will provide a clearer and consolidated view, however, the potential for silos remains across services. Consideration should be given to the ability to present an overarching view of the business which will:</p> <ul style="list-style-type: none"> • reduce the likelihood of the same resource being used by more than one service (staff, hardware) • strengthen the ability to capture dependencies • identify IT systems used across services enabling financial institutions to more clearly prioritise key systems for impact and recovery <p>Thereby increasing the ability of a FI to respond to a incident.</p> <p>Comments on the type and frequency of BCM tests: The requirement to test the BCP for each critical function would be onerous if the requirement included OMI IOM services as it would require multiple tests to prove each BCP. Request consideration is given for FI's to be able to consolidated tests proving a number of business functions/services at the same time. The benefit of which would reduce testing fatigue from multiple tests as well as giving an FI a holistic view of a full response to an incident impacting multiple functions.</p> <p>Comments on the conduct of regular BCM audits: Agree</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: In respect of industry-wide exercises and the strong encouragement to participate, consideration of the scale of the business and the criticality of the services provided against the frequency and level of participation should be considered by MAS.</p>
25.	Oliver Wyman	<p>Comments on the definition of business function: Definition broadly in line with what other regulators are defining it. BOT calls it "Business Service", MAS calls it "Business function" but the definitions are broadly the same in that it's a service that FIs provides to its customers.</p> <p>Comments on the roles and responsibilities of the Board and senior management: No potential issues – in line with global practice and other regulators</p> <p>Comments on the scope of a BCP: Introduction of an "end-to-end BCP" in addition to BCP at unit-level; while theoretically a good idea – there are several challenges that we foresee that would be good for MAS to clarify:</p> <ul style="list-style-type: none"> • What are the possible duplication of effort for "end-to-end" BCP vs unit-level BCPs?

S/N	Respondent	Feedback from respondent
		<ul style="list-style-type: none"> Who is the ultimate owner of this “end-to-end” BCP? It would be difficult to conduct or create an end-to-end BCP as you would ideally require an end-to-end process owner who can coordinate the hand-offs across each step in the process / across units in the end-to-end process Is the new end-to-end BCP supposed to co-ordinate which units need to recover sequentially vs in parallel, in order to consider the whole service recovered? This concept makes more sense in the context of IT recovery plans / contingency plans where there are certain core systems (e.g. core banking system & related system services) that must be recovered before front-end applications can recover. The IT recovery plan / contingency plan needs to be end-to-end in this respect and identify all the pre-requisite services that must be recovered before the critical application (i.e. the one that drives the critical business function) can recover <p>Comments on the type and frequency of BCM tests: Some of the suggestions that MAS have provided as example types of BCM tests seem reasonable; but unclear if it’s realistic to expect the FI to do all of the more complex exercises. Also – the FI would need to be very careful if they run this to ensure that this doesn’t cause an actual BCM incident (e.g. planned test for switching to alternate data centres / operating from disaster recovery site leads to actual issues if switch doesn’t go smoothly)</p> <p>Comments on the conduct of regular BCM audits:</p> <ul style="list-style-type: none"> Need to clarify the scope of BCM audits to avoid duplication of work done by BCM team (e.g. would BCM audit conducted by Internal Audit also conduct BCP testing to verify BCM teams’ testing results?) Role of BCM audit only makes sense if its job is to ensure BCPs are in place for all business functions and that testing takes place regularly. If it also goes into verifying actual test results is where it will lead to duplication of work and unclear the benefit / value-add of a BCM audit conducted by internal audit. <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Other: Industry-wide exercises are becoming more common; and it would be useful if MAS or other industry bodies can help identify & communicate if there are any potential areas of systemic BCM risks due to</p>
26.	Oversea-Chinese Banking Corp Ltd	<p>Comments on the definition of business function:</p> <ol style="list-style-type: none"> As the definition of a business function (service) is rather vague, the Bank recommends using FSB guidance on identifying critical functions and critical shared services as a foundation to work from. Guidance Link http://www.fsb.org/wp-content/uploads/r_130716a.pdf In the example given under chapter3.1, "customers" seem to refers to retail or corporate customers. We would like to seek clarity on whether "customers" includes both internal and external customers (e.g. FMIs, other banks, critical shared services such as HR or IT functions). Otherwise, would there be a definition of "customers" provided? <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ol style="list-style-type: none"> The Bank seek clarification for chapter 4.4(c) on the expected role of senior management in the Bank's BCM tests. Does “BCM test” refer to crisis management exercise in this instance? <p>Comments on the scope of a BCP:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>1. The bank proposes that BCP for critical business functions should not duplicate downstream processes (which has its own BCP) but to capture pertinent information that is needed at the critical business functions.</p> <p>2. In addition, as most BC plans are part of enterprise governance, risk and compliance portal ample time should be given to capture the new requirements and its implementation. We propose to set out a transition period of 24-36 months to implement.</p>
27.	Prusik Investment Management Singapore Pte Ltd	No comments.
28.	Rabobank Singapore Branch	<p>Comments on the definition of business function: Recommend that the Guidelines provide guidance on the responsibility and criteria used to define the risk/continuity owner of the business functions since now it involves multiple business processes and multiple departments.</p> <p>Comments on the scope of a BCP: Paragraph 2.15 of the consultation paper states that “The proposed Guidelines will expect FIs to have in place end-to-end business continuity plans for each service that is delivered to their customers, thereby drawing out any internal or external dependencies”. We are of view that such services are too many and broad which may not be effective. Instead, it may be more effective for the FIs to focus on the “critical” services that are delivered to their customers according to the FI’s business continuity objectives.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Paragraph 5.11 of the proposed Guidelines states that “FIs should notify MAS promptly when a critical business function is disrupted”. Could We recommend for these Guidelines to be enhanced to include the following similar to those that have been included in MAS Notice 644: <ul style="list-style-type: none"> • Further dDetails of the reporting channels to be used (eg email, Portal, etc.) and format (report template) is required. • Provide measurable term to the definition of “promptly”. Paragraph 5.14 of the proposed Guidelines states that “Relevant portions of communication plans should be aligned with crisis communication protocols established by industry associations so that there is consistent messaging to the public in a wide-spread disruption”. We would like to seek clarification as to the “crisis communication protocols” that the Guidelines is referring to.</p>
29.	RBC Investor Services Trust Singapore Limited	<p>General comments: We agree on the approach and direction the regulator is suggesting and are currently focusing our efforts to move toward this model.</p> <p>As this is a significant departure from the previous regulation, management would seek to understand the proposed timeline for implementation.</p> <p>Comments on the definition of business function: Management agrees with the direction on "business function".</p> <p>2.6 It may be difficult to specify a single minimum performance level and it may change from time to time, depending on factors such as market condition, nature of the incident, the risk appetite of senior management and the prolonged extent of damage an incident to an FI.</p>

S/N	Respondent	Feedback from respondent
		<p>Comments on the roles and responsibilities of the Board and senior management: Management agrees that the board and senior management should have oversight to the BCM program.</p> <p>Comments on the scope of a BCP: Management agrees with the end-to-end BCPs for business function and is channeling resources to move toward this model.</p> <p>Comments on the type and frequency of BCM tests: Management agrees with the proposed approach.</p> <p>Comments on the conduct of regular BCM audits: 2.20 Management agrees with the proposed approach; this aligns with the three lines of defense.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Management agrees with this approach.</p>
30.	RGA International Reinsurance Company	<p>General comments: One of the biggest changes is the way the MAS want to cover business functions. It can be challenging to actually specify minimum operating levels across multiple departments required to fulfil what they call critical business functions especially if there is a reliance on departments outside of Singapore. The requirement for end-to-end business continuity plans for each service delivered to customers to include internal and external dependencies could be quite challenging and will need significant time and resources to implement.</p> <p>Comments on the definition of business function: A business function should be considered as the collection of activities, regardless of departmental structure, required to complete a critical business process.</p> <p>Comments on the roles and responsibilities of the Board and senior management: The roles and responsibilities for the Board and senior management are quite reasonable.</p> <p>Comments on the scope of a BCP: The proposed end to end business continuity plan requirement is logical but could be exceedingly difficult to implement. Many popular BCM software solutions do not provide this functionality out of the box and these types of plans would require either system configuration or the undesirable idea of building end to end BCPs outside of the FI's mainstream BCM toolkit</p> <p>Comments on the type and frequency of BCM tests: The proposed type and frequency of BCM tests is reasonable</p> <p>Comments on the conduct of regular BCM audits: BCM audits are often performed as part of broader business process audits rather than as a standalone effort. It may not be reasonable to think that an FI will totally reorient its customary audit plan to accommodate this idea. It could be possible to synthesize the BCM audit component from process audits into one report which would be available for senior management or MAS review.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <p>It would be good to hear more of MAS expectations for FI's oversight of the continuity of key third parties.</p>
31.	RHT Compliance Solutions Pte. Ltd	<p>General comments:</p> <p>RHT Compliance Solutions conducted a roundtable discussion with industry members/financial institutions around the substantive issues raised in the Consultation Paper. The roundtable was attended by 125 attendees from 89 companies on 1 April 2019. Participants comprised representatives ranging from Insurers, Reinsurers, banking and capital market industries, including locally incorporated banks and Singapore branch of foreign banks.</p> <p>While we are broadly supportive of the proposal to revamp and refine the current Business Continuity Management Guideline (the "Guidelines"), we urge MAS to further consider the implications of some suggestions raised in the Guidelines.</p> <p>Our comments on the questions posed in the Guidelines are set out below and incorporate, where appropriate, inputs received from the roundtable participants.</p> <p>Comments on the definition of business function:</p> <p>MAS proposes to revise the definition of a "business function" to a service that a Financial Institution ("FI") ultimately provides to its "customer". Participants would like to clarify if the term "customer" includes internal-facing customers of a financial institution as well. Their main concern lies with the possibility of identifying multiple business functions that require further breaking down of processes and the supporting departments. The inclusion of internal customer may also risk over-complicating the Business Continuity Management ("BCM") process.</p> <p>We also seek clarity on the applicability of guidelines to external vendors who have been contracted by the financial institution to support a business function. For example, the diagram on Business Function shows departments and processes supporting it, but does not include external vendors.</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>We agree with MAS that an annual attestation to the Board would help to ensure both the BCM readiness and programme comply with all the requirements from the Guidelines. As the Guidelines apply to financial institutions and would not be applicable to most outsourced providers, we would like to seek clarification whether it would be sufficient to provide the Service Level Agreement ("SLA") as part of the attestation. We think that as the requirements in para 5.8 of the Outsourcing Guidelines already encompass a rigorous risk management approach with explicit requirements can therefore be considered a satisfactory attestation. Examples of such requirements include establishing outsourcing management control groups to monitor and control the outsourced service on an ongoing basis which meets the objective of the annual attestation.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>While triggers in relation to activation of the Crisis Management Team (“CMT”) may vary according to the nature of the company business, participants would nonetheless prefer MAS to issue a guide or examples of general triggers and incidents in a company that could call for the activation of the CMT.</p> <p>In relation to the need to review the adequacy of training for CMT members at least annually and ensure that they are competently prepared, there are few such courses for senior management to attend every year and we would like MAS to clarify whether conducting tests for CMT, with lessons learnt, would suffice.</p> <p>Comments on the scope of a BCP: We understand that FIs generally already have department-level BCP and can achieve end-to-end BCP by coming together to identify dependencies. The requirement for an FI to develop a Business Function BCP is onerous and unnecessary, as it means going through the whole process of risk assessment to develop the BCP at the Business Function level. A Business Function BCP is in fact just a collection of departmental BCPs with dependencies already identified and accounted for.</p> <p>Comments on the type and frequency of BCM tests: We note that the Guidelines set out in Para 6.4 state that a crisis management exercise and tests relating to the Business Continuity Plan for each critical business function should be done annually.</p> <p>However, it was also mentioned in the same paragraph that the test and frequency of exercises should commensurate with the scale and complexity of the FI. While we agree that it is essential for a FI to conduct periodic tests to establish a concrete BCM, coordinating a joint test between the FI and all critical external vendors can be onerous and requires a lot of resources and time to plan especially for more complex operations involving multiple parties. To this end, we would like to propose to MAS to revise the annual frequency to one that is biennial or a frequency to be decided by the FIs.</p> <p>Further, we note that the guidelines require all CMT members and their alternates be involved in the annual crisis and communications exercise. We are of the view that it is unrealistic to expect that all CMT members, or all alternates to be present. In fact, in an actual crisis, a crisis management meeting should be able to convene even without all members or their alternates being present. While we understand that it is essential for all CMT members to be familiar with the crisis management exercise, we urge MAS to consider other means of ensuring this e.g. through the imposition of a quorum or requiring that all members must go through at least one CMT exercise within a defined period (e.g. two years).</p> <p>Comments on the conduct of regular BCM audits: We are supportive of MAS’ intention to have an audit process in place in assuring the BCM is effective. We also understand that the frequency of the BCM audit should commensurate with the criticality of the business function.</p> <p>MAS did not determine the commencement of audit in the Guidelines. Participants were concerned about the implementation timeline for the audit as there may not be enough auditors with strong BCM knowledge and it may require time to train. It would therefore be challenging to comply within a year.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>To this end, we would like MAS to stipulate when the first audit is to be expected from FIs upon the official issuance of the Guidelines.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: We have no comments for this question.</p>
32.	Schroder Investment Management (Singapore) Ltd	<p>General comments: FIs will be expected to adopt the Guidelines within a year following its publication. We would like MAS to consider extending the period from 1 year to 2 years to ensure sufficient time for FIs to adopt the Guidelines.</p> <p>Comments on the definition of business function: We would like to obtain more guidance on the definition of “business function” in relation to the fund management industry. Some examples of related processes will be useful.</p> <p>Comments on the scope of a BCP: We would like to obtain more guidance on the expected risk assessment process covered under para 5.3. Is the expectation to perform scenario based BCP?</p>
33.	Securities Association of Singapore (CGS-CIMB Securities (Singapore) Pte Ltd, Charles Schwab Singapore Pte Ltd, DBS Vickers Securities (Singapore) Pte Ltd, Gain Capital Singapore Pte Ltd, IG Asia Pte Ltd, KGI Securities (Singapore) Pte Ltd, Lim & Tan Securities Pte Ltd, Maybank Kim Eng Securities Pte Ltd, OCBC Securities Pte Ltd, Phillip Securities Pte Ltd, Saxo Capital Markets Pte Ltd, UOB Kay Hian Pte Ltd)	<p>Comments on the definition of business function: We noted that the definition of business functions will be revised to refer to a service that an FI ultimately provides to its customers. We would suggest that MAS considers expanding it for FIs to refer to a specific product / instrument that is being provided to customers. By defining a business function as a service that an FI ultimately provides to its customers may force the FI to omit business critical processes such as regulatory reporting, cash management, employee compensation, that are not included in the customer value chain but essential to business operations. Scoping the business function so wide as to cover a regulated activity such as securities trading will also raise questions on how to document the business function flow when the transactions cut across to external parties such as SGX (trade section) and CDP (trade settlement) whose recovery processes, RTO, RPO etc are not disclosed. Determining the RTO for a business function defined so widely may also prove to be problematic as the solution is not so simple as to consolidate the RTO times of all processes within the function. Consolidating the RTO times of all processes within the function would be the assumption that all processes have encountered difficulty and require recovery which is not realistic. Are we supposed to plan on a single process failing or multiple processes failing?</p> <p>Comments on the roles and responsibilities of the Board and senior management: Will entities that are complying to their Group BCM policies (BCM plan approved at Group Level) with Group oversight (aka Group CMT) be able to continue to rely on the support provided by the Group if members are able to demonstrate that adequate controls are in place at Group level to meet the MAS requirements, and these controls are subject to Group oversight?</p> <p>Comments on the scope of a BCP: Development of overarching BCPs for each service that is delivered to customers in addition to BCPs at Unit or Department level would add an unwelcomed complexity to recovery plans that are already complicated due to the number of individual processes that need to be covered.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Such complexity does not translate well into training especially if the audience is of varying experiences, ranks and ages. Members find that when a crisis occurs, the solutions that work are the simplest because they are understandable. In a crisis it is counterproductive to pull out a 100-page BCP that cross referenced to each and every Unit's BCP.</p> <p>Comments on the type and frequency of BCM tests: Requirement for a test relating to each critical business function would functionally mean an entity with 6 regulated activities (securities trading, leverage forex trading, futures trading, share margin financing, shares borrowing and lending and custodian) would be required to conduct 6 separate BCP tests in a calendar year. This is akin to continuously BCP testing over the calendar year, involving the same units (eg Retail Dealing), in addition to the Industry Wide BCP and DRE exercises with SGX. Would it not be possible to conduct a single BCP to cover all 6 regulated activities at the same time?</p> <p>Comments on the conduct of regular BCM audits: Conducting annual BCM Audits may be deemed too frequent. Some FIs are mandated by their internal policies or Group Audit policies BCM function for their Internal Audit to perform Observation on DRs and Crisis Management Simulation. DRs are conducted annually for critical systems and Crisis Simulation Exercise is also done yearly for Critical Business functions. Therefore, a full scope of BCM Audit could be done once every 2-3 years which may cover the adequacy of the institution's BCM Framework and how the framework is being implemented.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: If the above suggestion in Q1 is tenable, members would like to propose for MAS to consider to define "critical business functions", so that our recovery strategies, as well as the RTO can be tailored accordingly. The criteria for any specific service / product to be deemed as "critical business functions" could be spelt out for clarity (for eg. revenue contribution, or impact to customers). The suggestion to have such distinction for "critical business functions" is such that FIs can highlight and focus on the relative priorities in a crisis situation where recovery of all business functions may not be practical.</p>
34.	Singapore Exchange Limited	<p>Comments on the definition of business function: Agree with the proposed requirements.</p> <p>However, the new definition of "business function" will cut across various functions and units within each FI. Significant work will be necessary to review and refresh the existing BCM work flow, governance and documentation. We request that MAS provide at least 18 months for FIs to comply with the new guidelines.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Agree with the proposed requirements.</p> <p>Comments on the scope of a BCP: Agree with the proposed requirements.</p> <p>Comments on the type and frequency of BCM tests:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>MAS expects that an FI, at minimum, conduct annually, “a test relating to the BCP for each critical business function”. From previous clarifications with MAS, we understand that MAS’s intention is that such tests need not be conducted for every element of each critical business function’s BCP every year. We strongly recommend that the BCM guidelines specifically clarify that FIs can take a modular, risk-based approach to such testing, based on the FI’s own risk assessment and BCM programme.</p> <p>Comments on the conduct of regular BCM audits: Agree with the proposed requirements.</p>
35.	SingCash Pte Ltd/Telecom Equipment Pte Ltd	<p>General comments:</p> <p>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.</p> <p>2. There are areas that we feel the MAS may wish to consider and factor into the Guidelines:</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p>

S/N	Respondent	Feedback from respondent
		<p>(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.</p> <p>(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.</p>
36.	Sompo Insurance Singapore Pte. Ltd.	<p>Comments on the definition of business function: The definition of business function to a service that ultimately provides to customers may include support activities. The inter-dependency of “business function” in operational process in the value chain will need to be explored in depth.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Board may not have detailed knowledge of operational processes to review and endorse processes/procedures. Hence, may not be the best party to evaluate intrinsic operational processes. Board of Management: Annual attestation to Board of Directors may increase the BCP cost and not necessarily achieve the objectives subsequently turning it into a “checkbox” exercise.</p> <p>Comments on the scope of a BCP: Whilst proposed scope of a BCP is a good initiative, external dependencies with third party vendors may be susceptible to changes and may face challenges if vendor is not familiar with BCP regimes of FIs.</p> <p>Comments on the type and frequency of BCM tests: It may be helpful if MAS could propose some samples of type of BCP tests that are relevant to different industries.</p> <p>Comments on the conduct of regular BCM audits: BCM audits should commensurate the risks posed/adopt risk based approach.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Consider establishing a platform in sharing of information that affects multiple industries eg in the event of cyber attacks, is helpful as it is difficult to validate incomplete/unsubstantial information/news.</p>
37.	Sumitomo Mitsui Banking Corporation	<p>General comments: Pursuant to paragraph 5.11 of the proposed BCM Guidelines, financial institutions are to notify MAS promptly in the event that a critical business function is disrupted. As there are reporting requirements under MAS Notice 644 as well, the bank would like to seek clarification on the notification requirements in the event an incident is reportable under both MAS Notice 644 and the proposed BCM Guidelines. Similar to MAS Notice 644, the bank would also be grateful if MAS could provide financial institutions with the relevant reporting templates to facilitate ease of reporting.</p>

S/N	Respondent	Feedback from respondent
		<p>Comments on the conduct of regular BCM audits:</p> <p>With reference to paragraphs 2.20 and 2.21 of the CP, we seek clarification on the following:</p> <ol style="list-style-type: none"> 1. As the proposed BCM Guidelines are silent on the topic of the frequency of the BCM audits, we would appreciate if MAS could clarify its expectation in relation to the frequency of the BCM audits. 2. Paragraph 2.21 of the CP requires an FI to develop a BCM audit plan, comprising auditable areas for the coming year, should be developed by the FI. The bank's understanding is that the process of determining the audit plan for BCM and the approval of such plans to be no different from other audits as all audits would go through the same process in Internal audit. We would appreciate MAS clarification in this regard.
38.	Swiss Re Asia Pte. Ltd.	<p>General comments:</p> <p>Swiss Re Asia Pte. Ltd. (SRAL) is generally agreeable to the proposed revisions to the BCM guidelines with additional clarification needed on definition of customers and recommend flexibility to define frequency, scope and governing body of BCM.</p> <p>Comments on the definition of business function:</p> <p>The definition set out is largely agreeable, although the term 'customers' should be defined for a reinsurance company. Particularly for a reinsurance company which is B2B, as opposed to B2C for an insurance company, the regulation should be commensurate with the reinsurance business model and not be specifically tailored to the needs of retail customers.</p> <p>Additionally, we would recommend BIA to be conducted every three years in line with other regulators.</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>Roles and responsibilities are agreeable with the exceptions as below:</p> <ul style="list-style-type: none"> • Annually endorsing the overall BC programme – Swiss Re has a Group endorsement for the BC programme rather than instead of at the specific legal entity level. Would this fulfil suffice the requirement? • Annually endorsing the critical business functions – Given the relatively static nature of our business, we do not feel the need for this recommendation. • Annually review over adequacy of training – We recommend the training to be limited to the BCM network (e.g. IMT), rather than the whole company. • Annual attestation over BCM preparedness – We propose for the governing body of BCM to be defined by the company. For SRAL, the committee overseeing BCM according to existing practice is 1st line of defence with focus on the BCM preparedness of the Singapore location. <p>Comments on the scope of a BCP:</p> <p>The scope of BCPs is largely agreeable, with two main exceptions. End-to-end planning should be for key / material services to customers rather than all services to customers. Secondly, planning for specific disruptive scenarios seems less efficient and effective. Preference would be to plan for the four main effects of disruption, i.e. loss of physical infrastructure (offices), employees, IT / communications, and third party service providers.</p> <p>Comments on the type and frequency of BCM tests:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Largely agreeable, although FIs should be permitted to decide on the nature and frequency of tests which are most relevant to their organisation, rather than a prescribed list and schedule.</p> <p>Comments on the conduct of regular BCM audits: Agree that an independent party should periodically conduct audits, but this is better placed with the BCM function so long as it is independent since their knowledge in the field would be superior.</p> <p>Additionally, we would recommend the frequency of the audit should be defined by the audit committee with discretion to decide the focus and the frequency of the audits.</p>
39.	Swiss Re International SE	<p>Comments on the definition of business function: The definition set out is largely agreeable, although the term 'customers' should be clearly defined for an insurance company. Additionally, we would recommend BIA to be conducted every three years in line with other regulators such as FINMA.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Our observations are as following:</p> <ul style="list-style-type: none"> • We would request clarity over which Board the paper refers to (Group vs the Singapore Legal Entity?) • Annually endorsing the overall BC programme – Swiss Re has a group endorsement for the BC programme rather than specific legal entity. Would this suffice the requirement? • Annually endorsing the critical business functions – Given the relatively static nature of our (insurance) business, we do not feel the need for this recommendation. • Satisfy itself that adequate resources are in place – It is part of the governance requirement and need not need to be explicitly mentioned. • Annually review of testing & implementation of lessons learned – Recommend this to be at the discretion of the FI depending on the nature and complexity of business model. • Annually review over adequacy of training – We recommend the training to be limited to the BCM network (e.g. IMT), rather than the whole company. • Annual attestation over BCM preparedness – Attestation of any sort cannot be performed at legal entity level due to limited resources. • Overall responsibility with CRO – recommend overall responsibility to be with branch head/manager and CRO to be an integral part of discussions and consultations. <p>Comments on the scope of a BCP: The scope of BCP seems to be largely catered towards banking institutions with headquarters in Singapore. In general we have two main exceptions. End-to-end planning should be for key / material services to customers rather than all services to customers. Secondly, planning for specific disruptive scenarios seems less efficient and effective. Preference would be to plan for the four main effects of disruption, i.e. loss of physical infrastructure (offices), employees, IT / communications, and third party service providers.</p> <p>Comments on the type and frequency of BCM tests: Largely agreeable, although FIs should be permitted to decide on the nature and frequency of tests which are most relevant to their organisation, rather than a prescribed list and schedule.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Comments on the conduct of regular BCM audits: Agree that an independent party should periodically conduct audits, but this is better placed with the BCM function so long as it is independent since their knowledge in the field would be superior.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: The guidelines in general appear to be more targeted towards banking industry. We would request more clarity in terms of expectations from insurance/reinsurance companies esp. those with Headquarters based outside Singapore and a relatively static business portfolio.</p>
40.	The Association of Banks in Singapore (ABS)	<p>General comments: The ABS welcomes the opportunity to provide its comments on the proposed Guidelines on Business Continuity Management (for convenience, we refer to this as "BCMG" in this submission).</p> <p>The ABS supports the MAS's efforts to provide guidance on establishing plans to ensure that business functions can be promptly resumed following a disruption. ABS members are of the view that these proposed Guidelines will help financial institutions to strengthen their resilience to disruptions.</p> <p>The ABS has received a number of comments from its members and has discussed the issues raised in the consultation paper. The key points are highlighted in Annex-A. A collation of all members' comments is set out in Annex-B to this submission.</p> <p>The comments listed in Annex-A are intended to provide an overview of some of the key matters discussed and is not intended to be exhaustive. The ABS will be conducting an industry briefing for its members and should any additional issues emerge from the briefing, we will update the MAS by way of an addendum to this submission.</p> <p>In conclusion, the ABS would suggest that these proposed Guidelines be implemented on an institution by institution basis, having regard to its size, risk, structure and in consultation with its respective MAS supervisors. Given the new BCMG requirements introduced, while the design and planning could be achieved in 12 months, the implementation and testing would need more than 12 months to operationalize.</p> <p>Comments on the definition of business function: Section 3, Paragraph 3.1</p> <p>Comments: The BCMG concept of business function (BF) defined as a service to customer is understood. However, the granularity and determination of what constitutes a BF may vary between FIs within the same banking license group.</p> <p>FIs could determine their BFs at group level (e.g. investment banking or retail banking) or by business lines (e.g. FX, securities, wealth management, loans, deposit taking) or by product lines (e.g. derivatives, collateral management, cash management, loan origination).</p> <p>Depending on the nature, scale and complexity of each FI's organizational construct, the FI will determine the level of BF that is most appropriate for itself. Only thereafter will all business process, supporting systems and</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>infrastructures (hereinafter referred as Unit) be mapped to each BF and the end-to-end BF process view be established. ABS will offer this interpretation and will educate the banking industry along these lines.</p> <p>Section 3, Paragraph 3.2 Comments: Assuming the proposal of BF recovery intentions (BFRI) (item 8 below) is accepted, it will state the recovery and risk appetite and residual risk tolerance of the BF. It is from this deliberation that the FI decides whether a BF will be considered critical business function (CBF).</p> <p>It is important to note that that once a CBF is determined, FI should identify the key unit level processes and systems supporting the CBF. ABS will offer this interpretation and will educate the banking industry along these lines.</p> <p>Section 3, Paragraph 3.5 Comments: As technology related performance is already covered in the technology risk management guidelines, the performance monitoring and thresholds should refer to the business processes required to carry out the critical business functions at the acceptable levels.</p> <p>Recommendations: To give business process examples instead of technology examples</p> <p>Comments on the roles and responsibilities of the Board and senior management: Section 4, Paragraph 4.3, Footnote 3 Comments: For overseas incorporated institutions in Singapore, it is suggested that the Board be able to delegate the responsibility (excluding accountability) to a local or regional committee in order to ensure a proper oversight and discharge of the Board's duties.</p> <p>Recommendation: 3 The Board may delegate the authority to make decisions to a Board committee but bears the ultimate responsibility. Please refer to MAS Guidelines on Risk Management Practices – Board and Senior management. For overseas incorporated institutions in Singapore, the roles and responsibilities specified for the Board can be performed by the relevant function responsible for BCM at Group/Global or Regional and/or Local committee while ensuring no conflict of interest.</p> <p>Section 4, Paragraph 4.3(c) Comments: By requiring the Board to satisfy itself that adequate resources including budget, technology, and staff are allocated, this suggests that the Board has to understand the operational details relating to the budget, technology and staff allocation. It is suggested that the paragraph be less prescriptive on the components (e.g. budget, technology, staff) to be considered and suffice that the Board just needs to be satisfied that adequate resources have to be allocated to the BCM programme.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Instead, MAS may wish to consider placing the components in the Senior Management section.</p> <p>Recommendation: (c) Satisfy itself that adequate resources <Propose to delete ">, including budget, technology, and staff"> are allocated to facilitate the implementation of an effective BCM</p> <p>Section 4, Paragraph 4.4(c) Comments: The phrase "participate actively" suggests that senior management must always be directly involved in BCM tests. Senior management will be involved in BCM tests and their reviews, but often will be present on-site as an observer (as opposed to direct participation in a BCM test).</p> <p>Recommendations: It is suggested to amend the statement to "Participate <propose to delete "actively"> in all relevant BCM and Crisis Management tests"</p> <p>Section 4, Paragraph 4.7(e) Comments: The specific details of the work routine required may vary significantly as it depends on the circumstances and severity of the crisis. It is more appropriate to require FI's to define the approach and have a list of consideration items prepared in advance and have it included in the crisis management plan. Upon the occurrence of a crisis, the approach and list should be considered when determining the required work routine to address the crisis.</p> <p>Recommendation: (e) Set out <Propose to delete "a potential work routine"> the approach and items to consider when determining the required work routine in the event <propose to delete "that the duration of the crisis is prolonged"> of a prolonged crisis.</p> <p>Comments on the scope of a BCP: Section 5, Paragraphs 5.1 and 5.6 Comments: In Singapore, FIs generally implement BCP at a unit level. This includes business and product line owners. The current proposed development of a procedural business continuity plan (BCP) at the Business Function (BF) level may give rise to duplication of efforts given that recovery procedures are already captured at the unit-level BCP. This also increases the risk of misalignment, which may cause conflicting instructions.</p> <p>It may be more relevant to document the BF's recovery intention. To ensure end-to-end focus, it is paramount that all processes and systems that support the BF understand the recovery expectations of the BF and to develop their respective unit-level BCP to meet the BF's recovery intentions.</p> <p>Components of Recovery Intentions could include the following; strategy owner, the BF's Recovery or Risk appetite and corresponding BCO statements (e.g. MPL, RTO, RPO), dependencies expectations (including intra-group dependency and third parties) and residual risk tolerances.</p> <p>Recommendations:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>It is recommended to rename Business Function BCP to “Business Function Recovery Intentions” (BFRI) to better reflect the BF business priorities and intentions in the recovery process. We should avoid using “Recovery Strategies” as this has been used in other components of BCP. Components of the recovery intentions should be made clear as suggested above.</p> <p>Section 5, Paragraphs 5.2, 5.5 and 5.6 – References to “pandemics”</p> <p>Comments:</p> <p>The word “pandemic” suggests a worldwide spread of a disease. BCPs may be activated in cases of infectious disease outbreaks even on a smaller scale e.g. the country-level. Hence the “infectious disease” may be a better reference to consider.</p> <p>Recommendations:</p> <p>5.2 Disruptions could be caused by malicious acts (e.g. cyber-attack, terrorism), natural occurrences (e.g. floods, infectious disease outbreaks, including pandemics) or accidents (e.g. electricity outages, failure of individual system components). Disruptions typically arise due to the diminished availability or functionality of one or more of the following factors that the business function depends on: personnel, physical infrastructure and/or IT components⁷. A disruption could also occur due to the failure of a key third-party service provider.⁸</p> <p>5.5 In this regard, an FI should develop BCPs that can address a broad range of plausible scenarios from wide-area disruptions to infectious disease outbreaks, (including pandemics). For example, the primary and secondary sites of critical business functions should not rely on the same substation for electricity. FIs with sufficient scale could also operate from multiple locations such that staff and equipment located at a secondary site will be sufficient to allow an FI to continue performing a business function even when the primary site is completely unavailable.</p> <p>5.6 FIs should establish a process to monitor news or developments on incidents that could have a downstream impact on their business functions. Lessons learned from its own near-misses, as well as incidents at other FIs or industries, can be used to enhance the institution’s understanding of plausible causes of disruptions. In addition to institution-specific disruptions, an FI should also have the plans to deal with a general <propose to delete “pandemic”> infectious disease outbreak in a manner consistent with the guidance issued by the Ministry of Health.</p> <p>Section 5, Paragraph 5.3</p> <p>Comments:</p> <p>It is noted that risk assessment is mentioned under the section on BCP. Clarification is sought on whether the expectation is for a risk assessment at the BCP level or at a higher level (e.g. country-level).</p> <p>It is suggested that this is preferably done at the country-level given that most business functions and organization units will share the same possible causes of disruptions. Adopting it at the BCP level may not be feasible and will be especially challenging if it is required for a prompt replacement or process changes for an end-to-end BCP.</p> <p>Recommendation:</p> <p>To include a footnote that risk assessment can be done at country and not just BCP level.</p>

S/N	Respondent	Feedback from respondent
		<p>Section 5, Paragraph 5.5</p> <p>Comments:</p> <p>The statement “broad range of plausible scenarios” could be mis-interpreted to require FI to have BCP that addressed all causes of disruptions – large or small, simple or complex. The causation list of disruptions will be exhaustive. BCM is about consequence management and having in place control measures to address outage scenarios that may materially impact the operations of the FI. Typically, the plausible outage scenarios are developed following a risk assessment process that considers the threat landscape, the risk and impact to the FI and thereafter the required outage scenarios that the FI should plan against.</p> <p>The plausible scenarios provided are wide-area disruptions and pandemics. It is noted that “disruptions” is an impact instead of a scenario.</p> <p>Recommendations:</p> <p>It is suggested to amend the statement as follows:</p> <p>5.5 In this regard, an FI should develop BCPs that can address a broad range of plausible impact-based scenarios from wide-area disruptions to infectious disease outbreaks, (including pandemics). For example, the primary and secondary sites of critical business functions should not rely on the same substation for electricity. FIs with sufficient scale could also operate from multiple locations such that staff and equipment located at a secondary site will be sufficient to allow an FI to continue performing a business function even when the primary site is completely unavailable.</p> <p>Section 5, Paragraph 5.8</p> <p>Comments:</p> <p>Not every service may be governed by a formal service level agreement (SLA) and FIs may not sign agreements with all intra-group. It is suggested that the word “agreements”, as opposed to SLAs, be used.</p> <p>It is also noted that the reference to RTOs for intra-group service providers and third-party vendors may not be necessary given that such is covered under the Guidelines on Outsourcing, revised 5 October 2018. As such, the second sentence of this paragraph can be removed.</p> <p>Recommendations:</p> <p>5.8 Where recovery arrangements rely on other stakeholders, such as intra-group partners and third party vendors, formal service level agreements (SLAs) and documented agreement should be established for third party vendors and intra-group partners respectively, and the appropriate redundancies agreed upon. <Propose to delete "This would include setting specific and measurable recovery expectations (e.g. RTOs), mutual participation in testing and review of SLAs on a regular basis."> FIs are encouraged to share their business continuity objectives with key stakeholders to mitigate the risk of mismatched expectations. An FI should proactively assess the resilience of these stakeholders and involve them in its BCM exercises, where appropriate.</p> <p>Section 5, Paragraph 5.16</p> <p>Comments:</p> <p>In respect of the list of non-exhaustive components mentioned, not all components are necessarily applicable for every BCP. For instance:</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<ul style="list-style-type: none"> • Procedures to retrieve vital records may not be applicable to all functions and business impacts, and may leverage data recovery measures by IT; • Information on the recovery site may not be applicable if recovery strategies utilised include remotely working from home or handing over to teams in other locations are utilised recovery strategies in case of a loss of premises scenario; • Coordination with external dependencies and parties may not be applicable to all functions; and • 'Call Tree' procedures may be separately managed, such as through HR automated notification systems and in such event, the details will not be reflected in the BCP. <p>Further, the references to "detailed procedures" and "according to a timeframe" in point 4 of the paragraph suggests a focus on specific timeframes or the day to day routines, which should not be the case as the BCP should be focused on the broader recovery procedures.</p> <p>Recommendation:</p> <p>5.16 The following (non-exhaustive) components are expected to be included in the BCP, where applicable:</p> <ul style="list-style-type: none"> • Planning assumptions; • Business continuity objectives • Identified recovery staff and alternates; • Detailed recovery procedures<Propose to delete", according to a timeframe,"> performed by staff; • Procedures to retrieve vital records¹¹; • Notification procedures, e.g. call trees procedures; • Information on the recovery site; • Coordination with external dependencies and parties (including authorities, etc.); and • Related information or references on IT recovery, such as critical applications and databases and their RTOs/RPOs. <p>Comments on the type and frequency of BCM tests:</p> <p>Section 6, Paragraph 6.2</p> <p>Comments:</p> <p>"All aspects" is already encompassed in the phrase "regularly and meaningfully" and should be removed.</p> <p>Recommendation:</p> <p>6.2 An FI should have a formal testing programme to systemically validate their ability to achieve their business continuity objectives in the event of a disruption. The testing programme should comprise a process to regularly and meaningfully test¹² <Propose to delete "all aspects of"> a business function's BCP, as well as an FI's overall crisis management plan.</p> <p>Section 6, Paragraph 6.4</p> <p>Comments:</p> <p>The need for crisis management exercises to be conducted annually is acknowledged. However, it may be difficult to have every CMT member and their alternates participates in exercises on the same day.</p> <p>Recommendation:</p> <p>6.4 The type and frequency of exercises should be commensurate with the scale and complexity of the FI, with particular attention being paid to critical business functions. The FI should have a programme to ensure all CMT</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>members and their alternates are meaningfully involved in crisis management and communications exercises. At the minimum, an FI should conduct the following annually:</p> <ul style="list-style-type: none"> • A crisis management and communications exercise <Propose to delete" involving all CMT members and their alternates;"> and • A <Propose to delete "test relating to the BCP of each"> validation of Business Function Recovery Intention of critical business function. <p>MAS to provide further comment on test relating to unit-level BCPs.</p> <p>Section 6, Paragraph 6.5 Comment: As there is no industry standard on how to define or measure RPOs, there is a challenge for an FI to design the appropriate metrics for measuring quantitative and qualitative RPOs.</p> <p>Recommendation: MAS to provide a common understanding on how to measure RPOs as this will help FIs to design the appropriate metrics for quantitative measurement of RPOs.</p> <p>Comments on the conduct of regular BCM audits: Comments: Paragraphs 6.10 and 6.11 refer to the need for an audit process, audit plan and approval of the audit plan by the FI's Audit Committee but allow the audit activity to be conducted by an independent unit.</p> <p>It is not clear if the independent unit is only meant to be the Group Audit function or includes units (internal or external) that are not Group Audit but are independent to the BCM programme of the FI. It would also be useful to clarify the definition of "independent". It would be reasonable to assume that such units do not own the FI's BCM framework, programme, policy, and control standards nor do they own the actual controls.</p> <p>Recommendation: To clarify the meaning of "independent unit" and the definition of "independent".</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: 1) Resilience vs Continuity Comments: We understand that the proposed BCMG only covers BCM from a consequence management perspective. Increasingly, regulators are focused on how the provision of key products and services can be maintained during disruptions and the operational resilience of an FI is just as important as its financial resilience. Operational resilience is often referred to the ability of FIs to detect/prevent, respond to, recover and learn from operational disruptions.</p> <p>While some aspects of operational resilience are not as easily implemented in BCM than in technology (e.g. preventative controls), the increasing threat and risk landscape, in particular that in relation to cyberspace, necessitate organisations to operate their business with resilience and not just recovery.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Today, a number of banks have already embarked on pro-active and pre-emptive mind-set of resilience programmes and will need time to achieve a high state of resilience against disruptions. MAS clarification is required as to the extent that BCMG should cover resilience instead of just business continuity (consequence management).</p> <p>2) Business Continuity in the aspect of Information Technology Comments: The proposed revisions to the BCM guidelines adopt the concepts of “business functions” and “critical business functions” and introduce the concepts of “business continuity objectives” and “minimum performance levels”. Given that the Technology Risk Management Guidelines make references to information technology, guidance is sought regarding business continuity in the context of information technology (IT) recovery.</p> <p>Recommendations: It is suggested that provisions be made to connect the requirements of BCMG in TRMG. One example is the role of Business Function in the area of IT recovery and how BCO and MPL requirements configure in the context of IT. Clarification is sought on what does RPO mean in the context of data corruption.</p> <p>3) Differentiations for small and medium FIs Comments: Section 4, Paragraph 1.4 Small and Medium FIs may struggle to calibrate their BCM programme. They would want to avoid misinterpretation of the BCMG and maximize use of their scarce financial resources.</p> <p>Recommendation: Clarification is sought on how small and medium FI should calibrate their BCM programme to adhere to the BCMG given their relatively smaller scale, nature and complexity of business operations.</p> <p>4) Risk Acceptance Comments: Considering “Residual Risk” was included in the Definitions, it would be useful to include the definition of “Risk Acceptance” as this is also referred in BCMG.</p>
41.	The Northern Trust Company	<p>General comments:</p> <p>The one year period to adopt the Guidelines may not be sufficient as there will be a need to reconcile the standards with our overseas head office to ensure alignment. We are also looking to evaluate and use a new risk management tool to streamline documentation requirements that can group different business processes that support a business function, and map dependencies with other entities and IT systems which may reside outside our Singapore branch. As this may take more than one year to meet the requirements, we suggest a flexible implementation timeframe that commensurate with the risks posed to the FI.</p> <p>Comments on the scope of a BCP:</p> <ul style="list-style-type: none"> Paragraphs 2.16 of the Consultation paper and 5.3 of the proposed BCM Guidelines stipulate that the risk assessment process identifies possible causes of disruptions and their potential impact. On the other hand, the Business

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Continuity Plan (BCP) document focuses on the restoration a business function in the event of a disruption.</p> <p>Does MAS recommend this risk management document to be part of the BCP, or can this form separate processes and documents?</p> <ul style="list-style-type: none"> Paragraph 5.5 of the proposed BCM Guidelines mention that 'FI should develop BCPs that can address a broad range of plausible scenarios from wide area disruptions to pandemics.' <p>We would like to have more clarity and examples on the "broad range of plausible scenarios" as it may not be possible or practical to include an exhaustive list of event-based scenarios in BCPs. This would result in the BCP to be excessively long, impractical and lose its objectivity as each scenario may result in various outcomes which may be challenging for an FI to anticipate, particularly if the scenario occurs over a prolonged period of time.</p> <p>Based on best practices, we are of the view that BCPs should focus on recovery processes and resources using outcome based events that can cater to a broad range of scenarios. For example, the loss of facility, people, technology, service providers and inter-dependencies.</p> <ul style="list-style-type: none"> Paragraph 5.8 of the proposed BCM Guidelines mentions that 'formal Service Level Agreements (SLAs) should be established and the appropriate redundancies agreed upon.' <p>We would like to confirm if this corresponds, and does not supersede requirements from paragraph 5.7 of the MAS Outsourcing Guidelines, on Business Continuity Management.</p>
42.	Transamerica Life Bermuda Ltd	<p>Comments on the scope of a BCP:</p> <p>With respect to interdependency risks beyond FI direct control, e.g. unavailability of telecommunications network (per section 5.9, page 19 of the Consultation Paper), a general assumption in local BCM framework is that core public infrastructure such as utilities (water, electricity) and those of monopoly in nature, would remain available in event of a crisis impacting FI. It may inefficient for individual FI to approach those service providers to assess BCM standard and their disaster recovery service level. It would be helpful if MAS could provide further guidance in terms of the extent of assurance FIs are expected to obtain from those service providers of this nature.</p> <p>Suggest further guidance on relevant protocols described in section 5.14 on page 21 of the Consultation Paper.</p> <p>Comments on the conduct of regular BCM audits:</p> <p>We would like to confirm our interpretation that the expected regularity of BCM audit can be aligned with FI's risk profile and internal audit roadmap based on risk priorities / maturity of the company, i.e. not necessarily on an annual basis.</p>
43.	Validus Reinsurance Ltd	<p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> There is good rationale for defining a business function as the set of processes (which may span multiple departments) that result in the delivery of a service to a customers. This is in contrast to the current definition which makes business function synonymous with department. The new definition of business function, when performing business impact analysis, would provide for easier identification of the complete set of processes involved with end to end

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>service delivery and easier identification of any process gaps. This is in contrast to focusing on departmental-based processes, whereby a key component of a complex processes for delivering a service could be overlooked.</p> <ul style="list-style-type: none"> • Organization of a business continuity plan (BCP) along functional as opposed to departmental lines, however, should be optional instead of mandatory, given the fact that if a thorough business impact analysis (BIA) has been performed, both approaches should lead to the same result. • For institutions that are going concerns, restructuring an existing BCP may not be a compelling value proposition and therefore something that should be considered as optional. However, for new entities the MAS may wish to make this approach mandatory using the proposed definition of business function. <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ul style="list-style-type: none"> • No issues with proposed roles and responsibilities. <p>Comments on the scope of a BCP:</p> <ul style="list-style-type: none"> • Same response as Question 1 • If the proposal is to become mandatory there should be a transition period based on the scale of the financial institution's operations, with the more complex institutions having a longer period to adapt. <p>Comments on the type and frequency of BCM tests:</p> <ul style="list-style-type: none"> • A crisis management and communications exercise should be performed once every 2 to 3 years, as opposed to annually, if there are no actual incidents during this period that test the crisis management response. <p>Comments on the conduct of regular BCM audits:</p> <ul style="list-style-type: none"> • No issues with the expectations.
44.	Wells Fargo Bank	<p>General comments:</p> <ul style="list-style-type: none"> • Where BCM audit is conducted by a specialized team as part of the Head Office audit function, what are the MAS' expectations on scope and frequency of local audits at branches that are not considered material from a group perspective? • Where BCM audits are conducted by local teams who are not specialists in the subject, what frequency and level of testing would the MAS expect the local teams (who are very small in size) to be able to perform? <p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> • Question 1a: The proposed definition of business function is rather broad. Could MAS provide clearer definition of business function? • Question 1b: The proposed definition of "business function" may not aligned to industrial definitions such as Disaster Recovery Institute International (DRI). How would MAS propose to align this definition of "business function" in line with industry practices? Particularly for global FIs where there are more than one regulators, FIs may have it challenging to align corporate definition with MAS' definition. • #2.6 What is MAS definition of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)? • #2.2 Would services provided by the Branch to other WF entities such as risk management, HR etc defined as customers, • #2.6 What information is MAS expecting to be constituted within the "minimal performance level" for each business function?

S/N	Respondent	Feedback from respondent
		<p>• On #2.7 the requirements that “a particular business function should be supported by all systems and processes that the function depends on” is there any expectations that these “systems and processes” can rely on their recovery plans?</p> <p>Comments on the roles and responsibilities of the Board and senior management: The roles and responsibilities are clearly set out in the revised guidelines. However, these roles and responsibilities may not take into consideration the local team set up for small- to mid-sized FIs where there could be dual hatting. Would MAS consider a more principles-based approach for segregation of roles and responsibilities?</p> <p>• #2.9a What contents would MAS expect to be included in the material for the Board to endorse?</p> <p>• #2.9c In situation where services and functions are supported by corporate or offshore backoffice locations that reside outside Singapore, to what degree is the Board expected to obtain satisfaction that “adequate resources, including budget, technology, and staff are allocated”</p> <p>• #2.11 Is there expectations that the “committee to oversee its BCM” and “the committee should thus be led by a senior management” be part of the branch as due to</p> <p>Comments on the scope of a BCP: While we agree, in principle, that the requirements for BCPs are moving in the right direction, FIs may not be set up at the moment to move within a short timeframe to end-to-end BCPs. Could MAS consider including an implementation/transition timeline for this requirement?</p> <p>#2.15 To what depth and detail does MAS expect the end to end BCP to contain? Is the expectations for end to end BCP is only specifically for services to customers?</p> <p>Comments on the type and frequency of BCM tests: We would like to propose that the type of BCM tests should be developed based on a risk-based approach. Where an FI is small- to mid-size, and where there are minimum critical client-facing activities, or where staff turnover is low, the type and frequency of BCM tests should reflect this nature.</p> <p>Comments on the conduct of regular BCM audits: We would like to propose for BCM audits to be inter-changed with self-attestation exercises. Where FIs are small or mid sized, or where the risks are relatively low, self-attestation exercises could take place instead of regular, full-fledged audits.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: We would like to propose for MAS to adopt a principles-based approach towards the revision of the guidelines. Where FIs are smaller in nature, these should be considered in the BCM guidelines particularly for the BCP, CMP.</p> <p>• #2.21 Where a FI is a global company are there alternatives to the audit committee approving the BCP audit plan?</p>
45.	An entity *	<p>Comments on the definition of business function: Q1. Para. 3.1 “A business function refers to a service provided to customers of an FI.” Would customers refer to external customers only?</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Q2. Para. 5.1 "While the focus here is on business functions, FIs should also conduct BIA and establish business continuity objectives at the unit-level." Are you able to clarify what it means by "unit-level" and provide some examples?</p> <p>Q3. Under the new definition of "business function", who will be the driving lead and how should accountability and responsibility be divided if the business process involves a few functional departments across?</p> <p>Q4. Are you able to provide some examples of "minimum performance level" and how it should be quantified?</p> <p>Q5. Some of the paragraphs and examples in Section 3 of the proposed BCM guidelines appear to be geared more towards "IT systems", "intermittent network connectivity", "faulty hardware" and also have similar references to IT incident management and problem management (example Para. 3.5) which is part of the MAS TRM Guidelines. Is there an overlap? Would it be better dealt with in the TRM Guidelines?</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>In relation to Para 4.6, where in a small company of less than 10, other than the Managing Director, how should the Crisis Management Team (CMT) comprising of senior management representatives be formed if the rest of the individuals are employees and not senior management? In such a case, the organization is very flat and it is not possible to have so many hierarchical layers with different roles and responsibilities for different groups relating to Senior Management, CMT, Audit Committee, and those who carry out the actual BCM recovery function. Is the MAS able to provide some guidelines on what is essential for a smaller FI setup of less than 10?</p> <p>Comments on the scope of a BCP:</p> <p>` In relation to Para. 5.9, where "key service providers" are mentioned, would this also relate to telco and internet service providers e.g. SingTel, Starhub, Singnet?</p> <p>I think it is quite onerous and hard for FIs to take reasonable steps to ensure that their key service providers will not falter during disruption time. In any business continuity planning, though scenarios can be thought of and plan for recovery, there is still that very small percentage of risk that would be impossible to plan for. At that point of the disruptions, it is possible that key service providers could also fail due to a coincidence.</p> <p>Comments on the conduct of regular BCM audits:</p> <p>In relation to Para. 6.10 and 6.11, for a small FI setup of less than 10, we do not have enough senior management representatives to form an Audit Committee. Also because of the small operations, we do not have an internal audit headcount or a staff who is not involved in the planning and execution of the BCM itself (Compliance Officer is involved in the BCM planning) that is independent and is able to produce a BCM audit report. While we can understand that the 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 to fulfill the audit requirements within the proposed BCM Guidelines?</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <p>The new Guidelines have evolved to be so onerous requiring different groups of people for oversight, and check and balance (audit), these is possible in a large organisation. However, in a very small setup, this is not feasible practically as</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		for example, we only have 7 headcount (including management, compliance, accounts/admin, and broking staff). I can understand that the BCM is geared to all financial institutions and it is a very important aspect. For many of the requirements it makes sense in a large organisation and it is practically possible to carry it out. However, the Guidelines have become quite "textbook-based" for our current small setup but in reality, some of the aspects are not possible to have as we have a very flat structure. The MAS could perhaps provide some guidance for smaller setups.
46.	An entity *	<p>Comments on the definition of business function: AXA supports the revised definition of business function as a service that the FI will provide to its customers. However, it takes time to map out these end-to-end business flows and the ability to do this will also depends on the maturity levels of the BCM within the FI as well.</p> <p>For the implementation of this requirement, it would good if MAS can -</p> <ol style="list-style-type: none"> 1. articulate clearly on requirements for minimum compliance preferably with reference to the maturity levels of the FIs 2. adopt the approach of progressive/phased compliance rather than a immediate full compliance upon the implementation of this requirement <p>With regards to Clause 2.7 - can MAS provide further guidance / reference / best practice on the monitoring capabilities?</p> <p>Comments on the conduct of regular BCM audits: Proposed frequency of BCM audits to be once every 3 years</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: In Annex B on the revised guidelines on BCM -</p> <ol style="list-style-type: none"> 1. Refer to section 5.11, on the requirement to "notify MAS promptly" – <ol style="list-style-type: none"> a. define the criteria to notify MAS b. Any stipulated template to use for notification? c. How soon must MAS be notified? 2. Refer to section 6.4, can MAS provide advice on what are the acceptable forms of BCP testing? Is desktop exercise acceptable?
47.	An entity *	<p>General comments: Question on the definition of Recovery Time Objective (RTO) for BCM, this definition is mentioned in different guidelines of MAS, can we suggest to have a distinct definition for RTO for BCM purposes.</p> <p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> • We agree that recovery of a business function should be cohesive and focused on delivery to the customer, and that a business function will likely require the performance of one or more business processes (in addition to supporting IT systems and physical infrastructure). We seek clarity and further guidance on what level of granularity is appropriate and how business functions can be categorised, such as by business type (consumer banking, business / wholesale banking), by product type (leveraged product, asset product), etc. We would like to request further examples of business functions be provided for this purpose. • We hope to see the definition and guidance of this term be further enhanced or expanded. In cases where business processes or activities that do not directly support any service to customers can be classified as critical, we would

S/N	Respondent	Feedback from respondent
		<p>like to have clarity on whether such functions should fall within the ambit of the proposed Guidelines.</p> <ul style="list-style-type: none"> • We found the diagram after Para 2.7 of the Consultation Paper (page 5), illustrating the relationship between “business function” and “business process”, to be clear and relevant, and suggest that it be retained in the proposed Guidelines’ table of definitions under the definition of “Business Function”. • We agree with the inclusion of minimum performance levels into business continuity objectives. For clarity, please include references to processing capacity (as opposed to “level of output”, which may not be applicable or meaningful in some cases). • We expect financial utility providers to take the lead in the disclosure of their minimum performance levels not only for the benefit of FIs who have critical interdependencies with them but also to set the bar for stating minimum performance levels that are “suitably defined, clear and measurable”. We would like to seek further clarity on the definition and where possible, examples provided, of defined, clear and measurable performance levels. • The capabilities to monitor reduced or intermittent service availabilities are part of business-as-usual (BAU) and day-to-day business monitoring and should not be confined to only the proposed BCM Guidelines or an FI’s BCM framework. BAU responses for reduced or intermittent service levels are usually activated to mitigate the impact for a short period of time (and longer if the impact were less). This area of response or recovery may not necessitate the activation of BCP or contingency plans nor necessarily be within the ambit of the proposed Guidelines. <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ul style="list-style-type: none"> • We note the detailed requirements for the Board and senior management. We understand the emphasis and the elaboration to emphasise the roles and responsibilities of the Board and senior management in the success and effectiveness of business continuity in the organization as well as senior management’s role in overseeing crisis management in the event of a severe disrupting event. <p>Comments on the scope of a BCP:</p> <ul style="list-style-type: none"> • To ensure that an FI’s BCP is fit-for-purpose, its BCP should take reference from the results of its risk assessment. Only then can the BCP be relevant for the risk environment in which the FI is operating. Risk assessment processes, however, should not necessarily be within the ambit of the proposed BCM Guidelines. • MAS may wish to consider making a distinction in the proposed Guidelines to convey an understanding that BCP measures are activated only when day-to-day measures are no longer appropriate to manage the disruption. • The process to monitor reduced or intermittent service availabilities should be part of business-as-usual (BAU) activity and not be confined only to the proposed BCM Guidelines or an FI’s BCM framework. BAU responses for reduced or intermittent service levels are usually activated to mitigate the impact for a short period of time (and longer if the impact were less). This area

S/N	Respondent	Feedback from respondent
		<p>of response or recovery may not necessitate the activation of BCP or contingency plans nor necessarily be within the ambit of the proposed Guidelines.</p> <ul style="list-style-type: none"> • We note that the setting of RTOs in formal SLAs with third-party vendors is consistent with BCM requirements stipulated in Section 5.7 Business Continuity Management of the MAS Guidelines on Outsourcing. • We agree and practise understanding and partnering key stakeholders and vendors in business continuity planning. We would like to request flexibility for FIs to demonstrate their engagement with such stakeholders including aligning business continuity objectives and having the appropriate level of involvement in BCM exercises, based on the criticality of business functions or processes that the outsourced services are supporting. • We seek confirmation that the Incident Reporting Template, issued by MAS via circular, continues to be applicable when submitting written incident updates to MAS. MAS may wish to consolidate the Template into the proposed Guidelines for completeness. <p>Comments on the type and frequency of BCM tests:</p> <ul style="list-style-type: none"> • We agree with the broad principles of testing documented in the proposed Guidelines which are in line with BCM best practices and support the opportunity to participate in industry-wide exercises. • We recognise the need to involve senior management and staff in BCM exercises and regular testing of crisis management and communication plans. Holding crisis management and communication exercises for all members of both the CMT as well as their alternates on an annual basis could involve a challenging degree of coordination, in particular where some members travel frequently due to their regional work coverage. Depending on the roles covered by the CMT members/alternates, their involvement in exercises could be more or less crucial. It may be adequate for either the primary member or their alternate to participate, and for both parties to have been involved within a few years or exercise cycles. <p>Comments on any other aspects of BCM that warrant further guidance from MAS:</p> <ul style="list-style-type: none"> • We note that MAS Guidelines on Outsourcing make reference to the MAS BCM Guidelines. With reference to BCM requirements for outsourcing, we will endeavour to promote adoption of industry best practices in BCM by our outsourced service providers (OSPs) but are mindful that OSPs have their own constraints and market practices (some of which are based on overseas practice) that limit the implementation of these practices. • Definitions of RTO are slightly different between BCM Guidelines and TRM Guidelines. MAS may wish to elaborate on the difference between business function/process RTO and IT system RTO to minimise confusion and misinterpretation by FIs.
48.	An entity *	<p>Comments on the definition of business function:</p> <p>Para 2.5</p> <p>The Bank suggests for the definition to only include financial services, and exclude value-added non-financial services. Business functions that do not result in a service that is ultimately provided to customers (e.g. Human Resources, Project Management) would thus not fall within the scope of BCM planning.</p>

S/N	Respondent	Feedback from respondent
		<p>Para 2.6 We would like to highlight that there may be instances where the sub-processes within a business function may not run sequentially and may have RTOs that are greater than the minimum RTO/RPO at the business function level (e.g. exception handling process). In which case, it may be challenging for the business continuity objectives for that business function to be aligned to the dependant sub-processes. Would such exceptions be permissible under the new Guidelines?</p> <p>Para 2.7 It may be operationally challenging to monitor/track/detect reduced or intermittent service availabilities and tie it with the minimum performance level at business function level. We request for MAS to provide more detailed guidance on this.</p> <p>Comments on the roles and responsibilities of the Board and senior management: Para 2.9 (a) The Bank agrees with MAS that the Board and senior management ought to be ultimately responsible for the business continuity of their FI. However, we would like to suggest for FIs to be given the flexibility to decide on the review frequency of the BCM framework, policies, processes and procedures, in line with the FI's internal policy approval standards.</p> <p>Comments on the type and frequency of BCM tests: Para 2.19 We agree with MAS that testing is crucial in validating an FI's BCM preparedness as it ensures an FI's response and recovery arrangements are effective and developed based on sound understanding of existing systems and processes. However, we would like to suggest for MAS to give FIs the flexibility to assess and review the necessity and frequency of such testing exercises.</p> <p>Comments on any other aspects of BCM that warrant further guidance from MAS: Para 1.3 In view of the complexity and coordination required to fully adopt the Guidelines, we would like to suggest an extended 18 to 24-month transition period instead of 12 months in order to ensure enough time to implement the required processes and controls holistically.</p>
49.	An entity *	<p>Comments on the type and frequency of BCM tests: To perform testing for each critical business function annually may be challenging, especially if the exercise complexity increases. Would the MAS consider the the testing frequency for critical functions be scheduled and spread across a period of 3 years? This will enable banks to have more meaningful and comprehensive exercise planning and execution through trainings and post-mortem exercise findings/recommendations.</p>
50.	An entity *	<p>General comments: There is currently no industry-wide methodology to measure the success of an RPO for business functions that involve Financial Market Infrastructure. Therefore, we would recommend that further guidance be issued on this in consultation with FIs.</p> <p>Regarding minimum performance levels (MPL), incident management processes are targeted at any component of a process that is degraded rather than across</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>an end-to-end business function. This ensures that an end-to-end business function is not unduly degraded due to existing incident escalation criteria, i.e. within any MPL that would be separately defined, so we would recommend to leverage the traditional incident management frameworks when considering MPLs.</p> <p>Comments on the definition of business function: We would suggest that the MAS sets out clear definition of what constitutes a “customer”. We would like clarification if a business function is expected to include OSPs, third parties or Financial Market Infrastructure (FMIs) that are part of the processes performed.</p> <p>We request that the scope be limited to critical business functions provided by the FI. If the MAS intends to extend this requirement to all business functions (including those that are non-critical) we would request an extended transition period.</p> <p>Comments on the scope of a BCP: For the business function recovery plan, we would suggest the FI be able to leverage the business entity process level recovery strategies currently in place as we expect the need to maintain plans at both a business entity process and business function level.</p> <p>We would like clarification, if a business function is expected to include third parties or FMIs that are part of the processes performed.</p> <p>Comments on the type and frequency of BCM tests: We request that the FI should have the flexibility to decide on the type of testing and the frequency depending on the risk assessment of the critical functions.</p> <p>To the extent that industry wide testing is required, we would need MAS to help with coordinating across FMIs.</p>
51.	An entity *	<p>Comments on the definition of business function:</p> <ul style="list-style-type: none"> o This is a major change in the way we conduct our BCP, and will require a big overhaul. We want to make sure this change is well thought-out and the objectives of this change can be implemented by FIs. o For a global organization, many functions are supported and performed by other locations outside of Singapore. We will need guidance how planning across these functions/locations can be integrated into a new plan based on this new definition. <p>Comments on the roles and responsibilities of the Board and senior management:</p> <ul style="list-style-type: none"> o For a global organization, managing the Business Continuity Management may be a global function supported by locations outside of Singapore. As such, oversight of the BCM is also done outside of Singapore. Does MAS consider these roles and responsibilities from a local office perspective or globally as an organization? <p>Comments on the type and frequency of BCM tests:</p> <ul style="list-style-type: none"> o With the proposed definition of business function, testing such business function which is end-to-end and crosses multiple functions and multiple locations can be very problematic. An end-to-end test could involve not only resources internally to an organization, but externally with third party vendors,

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>counter parties (such as trust bank, etc.), and even our clients. From a Technology perspective, testing end-to-end will involve multiple systems and data sources, and it will require posting data from one system to another, and each of these systems may have their own restrictions for posting test data. An error could cause major data integrity issue and could cause service disruptions. Can MAS provide guidance on testing.</p> <p>Comments on the conduct of regular BCM audits:</p> <ul style="list-style-type: none"> o For a global organization, auditing BCP maybe performed in different locations each time. Can MAS please clarify on the scope of BCP audit?
52.	An entity *	<p>General comments:</p> <p>This new guideline provides useful additions to the existing BCM guidelines which will significantly improve the alignment of business continuity plans with business services as well as facilitating the agility and lean initiatives currently going on the FSI industry to remain competitive in the digital age.</p> <p>However, while the organisational and human aspects of Business Continuity are generally appropriately documented and prepared, issues often arise in the technical aspects of business continuity: with their legacy systems' architecture designs inadequate for the expected SLAs or improperly tested dependencies. Considering the increasing interdependencies of FSIs through the use of open APIs and cloud providers, systemic financial reliability requires each service provider and FSI to perform at the highest levels of resilience and embrace resilience by design for their most critical business functions.</p> <p>With the rise of Agile and DevOps, organisations' technology and systems evolve at an unprecedented pace while the business functions and organisational structure are seldom modified themselves. To that extent, annual testing of crisis management and people-only scenarios of Business Continuity is appropriate, while it has become too infrequent to maintain an adapted grasp of technology changes.</p> <p>Leading organisations have embraced an approach of continuous testing of their systems' resilience through the practice of Site Reliability Engineering and Chaos Engineering. Modern BCP should adopt the core components of these practices to strengthen the resilience and risk management of their most critical functions. Such organisations drive resilience by design, by embracing an approach of continuous improvement with these practices, and the use of immutable architectures and microservices.</p> <p>To ensure a comprehensive view of the risks and adequate technical implementations, Business Continuity practitioners should be expected to understand the architecture design aspects of resiliency and consider each application's resilience factor as part of the overall application transformation strategy.</p> <p>Comments on the definition of business function:</p> <p>The change of business functions from organisational lines to services rendered to FI's customers is a great way to reduce the current corporate silos and facilitate the adoption of agile and lean principles.</p> <p>However, RTO and RPO are often too macroscopic and may be problematic as an objective transversal to several departments and teams. Owners of each system supporting the business function may aim for this RTO/RPO objective themselves, resulting in actual recovery times being higher than expected.</p>

S/N	Respondent	Feedback from respondent
		<p>Organisations should consider defining finer-grained active indicators for each component and process supporting the business function.</p> <p>Comments on the roles and responsibilities of the Board and senior management:</p> <p>1/ Third-party risk While SLAs provide a contractual agreement for services provided, they offer no guarantee of delivery. Senior Management should acknowledge the impact if the service provider were to fail to deliver these SLAs. Where the impact for a failed SLA would be significant (e.g. long term failure or contractual challenge), the organisation should have established exit plans in place allowing to resume acceptable levels of service promptly.</p> <p>2/ Creating a culture of resilience by design Whether Business Continuity and resilience is taken into account "by design" or retrofitted on existing processes, is often driven by the company's risk culture and staff performance objectives. Senior Management should promote a culture of continuous improvement of process and systems' resilience by introducing frequent and active failure testing, and incentivising incremental improvements.</p> <p>As such, Senior Management and Board should allocate a budget for the testing of resiliency and incentive programs.</p> <p>Comments on the scope of a BCP: System automation, Continuous Delivery pipelines and virtualisation/containerization technologies have made readily available native capabilities to backup and restore systems to their last known working state. Leading practitioners are rebuilding some of their critical systems regularly to increase the confidence that restoration of services will be effective in case of real issue.</p> <p>During the business continuity risk assessment, organisations should assess 1/ their capacity to regularly rebuild their critical systems to their last known working state or to another location, and 2/ their systems' capacity for zero-downtime operations (i.e. patching, updating, rebuilding).</p> <p>Comments on the type and frequency of BCM tests: With the increased complexity, interdependency and pace of change in technology, the risk of unplanned consequences of changes and minor failures keeps rising.</p> <p>Leading organisations are embracing continuous testing practices and key measurement metrics to ensure their systems and operations processes remain adequate at all times.</p> <p>Continuous testing practices such as Chaos Engineering help improve the overall resilience of technology ecosystems by continuously introducing failures in the system to ensure and strengthen its capacity to withstand issues. It also helps operations teams to build experience in recovery practices which are just not possible to achieve during annual exercises.</p> <p>As FIs become dependent on each other as well as on an increasing number of third-party providers, organisations should consider introducing Chaos Engineering functions to continuously test their critical functions' resilience and</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>mature their staff's expertise and confidence. FIs should also consider requiring similar practices from their critical service providers.</p> <p>FIs are also becoming increasingly software-driven organisations where change is continuous. FIs should consider tracking key resilience metrics such as MTTR (Mean Time To Recovery) and change failure rates, for each component a critical function is depending on, in order to establish a heat map of potential weaknesses.</p> <p>Learning is not only achieved through failures but from successes as well. It is particularly true for resilience by design. FIs should practice consistent "Retros" feedback to review the effects of events, even when no material impact was observed, to promote the learning of good practices.</p>
53.	An entity *	<p>Comments on the definition of business function: The proposed definition of "Business Function" could introduce ambiguity in interpretation, as it mis-aligns with an ordinary understanding of the term Business Function – which is commonly understood to be an organizational unit (e.g. by department or unit).</p> <p>The bank would like to seek MAS' consideration on the following:</p> <p>(i) Definition of "business function" to include Unit level – we understand this is a widely used term that most FIs currently refers to as Business functions</p> <p>(ii) In Section 5, rather than requiring BCPs to be for Business Functions – to consider to specify that BCPs (within the Unit) supporting the Business Functions (Service) should be established and provide aggregation and transparency to the front to back Business Function (Service) for resumption of output to minimum performance levels and the subsequent restoration to BAU levels.</p> <p>Comments on the roles and responsibilities of the Board and senior management: The bank would like to seek MAS consideration on the following:</p> <p>(i) For overseas incorporated institutions, Board may delegate to relevant function responsible for BCM at Group/Global/Regional level.</p> <p>(ii) Specify also that Senior Management responsibilities may be delegated to relevant locational governance committees.</p> <p>This is to provide flexibility and accountability and appropriate levels and committees, commensurate with business model that typifies a large global organisation.</p> <p>Comments on the scope of a BCP: The bank already has in place unit level BCP which highlights various internal and external interdependencies between teams (front-to-back processes) in each BCP. In this regard, we would like to clarify if this would dispense the need for a "business function" (i.e. business activity per MAS' proposed definition) level BCP.</p> <p>Relating to para 5.11, the bank would like to clarify if the meaning of "prompt notification" when a critical business function is disrupted, is aligned with the current requirements set out in "instructions on incident notification and reporting to the MAS", for bringing relevant incidents to the attention of the Authority.</p>

FEEDBACK RECEIVED ON PROPOSED REVISIONS TO GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

October 2021

S/N	Respondent	Feedback from respondent
		<p>Comments on the type and frequency of BCM tests: Relating to para 6.3, the bank would like to clarify if the examples provided by the MAS are baseline expectations of complex exercises to be included in a formalized BCM testing programme.</p> <p>If this is the intent, the bank would respectfully request the MAS to re-consider prescribing such baseline expectations within the guidelines, as FIs should be able to adopt a risk-based approach in designing its formal testing programme to systemically validate their ability to achieve their business continuity objectives in the event of a disruption.</p> <p>Comments on the conduct of regular BCM audits: The bank is generally supportive of the guideline requirement for banks to conduct regular BCM audits. However, we would appreciate further clarity on MAS' expectations on the frequency of audit.</p>