RESPONSE TO CONSULTATION PAPER

Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like:

(i) their whole submission or part of it (but not their identity), or

(ii) their identity along with their whole submission,

to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

Consultation topic:	Second Consultation Paper and Response to Feedback on Proposed Revisions to Guidelines on Business Continuity Management
Name[1]/Organisation: [1]if responding in a personal capacity	Asia Securities Industry and Financial Markets Association (ASIFMA)[1]
Contact number for any clarifications:	+65 6622 5972
Email address for any clarifications:	lvanderloo@asifma.org Laurence Van der Loo, Executive Director, Technology and Operations
Confidentiality	
I wish to keep the following confidential:	Comments can be treated as public

[1] ASIFMA is an independent, regional trade association with over 150 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

Dear,

ASIFMA and its members appreciate the opportunity to respond to MAS' second consultation paper and Feedback Received on *Proposed Revisions to Guidelines on Business Continuity Management* ("Second BCM Consultation Paper"). ASIFMA had responded to the first consultation paper in 2019 and is pleased to see that many of our recommendations have been reflected in the Second Consultation Paper. Since the first consultation paper, the Basel Committee on Banking Supervision ("BCBS") has issued its Principles for Operational Resilience (May 2021). We note that the MAS Second BCM Consultation Paper is more closely aligned with the BCBS Principles in some areas and the international best practices that many FIs are already adopting (e.g. dependency mapping, introduction of severe and plausible scenarios).

As mentioned in our below response, we have however also noted some key differences with the BCBS approach and terminology which might be challenging for our members that operate globally and are implementing a global operational resilience approach.

We would recommend that in line with the developing body of international work on operational resilience, the MAS also introduces the concept and term into its framework (which is not used in the Second Consultation Paper). The BCBS principles embed business continuity into the larger domain of Operational Resilience and it would therefore be prudent for MAS to follow the BCBS lead. We suggest that for business functions a continued focus on BCM is essential, but for critical business services, the focus should be on the wider concept of operational resilience.

We hope the MAS will continue to participate in the international dialogue on operational resilience and BCM and base its domestic approach on the globally agreed BCBS Operational Resilience Principles. Cross-border consistency and alignment of regulatory requirements and further harmonisation of the taxonomy and lexicon with the BCBS Principles will enable global firms that operate in multiple jurisdictions to have consistent operational resilience programs. Such alignment and harmonisation will be critical to negate the risk of unnecessary complexity, regulatory divergence, increased cost and effort that ultimately affects progress and could hamper efforts to manage cross-jurisdictional disruptions.

We do support the flexible approach of MAS, which provides firms with the ability to implement the Guidelines commensurate with the nature, size, and complexity of their business operations.

Given the extent of the changes, we suggest a phased implementation approach, or an extended timeline of 24 months to give FIs sufficient time to comply with the Guidelines or alternatively to have a deadline for having an executable plan.

We are grateful for the MAS to issue a Second Consultation Paper on this important topic and in what follows, we have outlined on behalf of our members some additional suggestions which we hope can be reflected in the final Guidelines.

We would welcome the opportunity to discuss our feedback in more detail during a meeting and remain at your disposal for any follow up questions you might have,

Yours sincerely,

Laurence Van der Loo
Executive Director Technology and Operations
ASIFMA

Question 1: MAS seeks comments on the proposed identification and prioritisation of critical business services in addition to critical business functions.

1. We welcome the change in taxonomy which is more aligned with international practices and the developing international body of work on operational resilience. This is particularly beneficial for our members that are global multi-national firms with global frameworks managing operational resilience which includes BCM. As mentioned in the introduction, it would be helpful if MAS could also introduce the term Operational Resilience and further align it with the BCBS Principles on Operational Resilience.
2. The identification and prioritisation of critical business services in addition to critical business functions is a logical next step as FIs seek to remain operationally resilient during disruptions. The proposal is in principle aligned with the BCBS Principles on Operational Resilience that define operational resilience as *"the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption."*
3. That being said, there are still a few differences in terminology between the MAS Second BCM Consultation Paper and the BCBS terminology. For example, whilst the MAS uses the term of *Critical Business Service,* the BCBS uses the term *Critical Operations* (paragraph 11 and 12 of the BCBS Principles). In its Operational Resilience Principles, the BCBS uses the term *Critical Operations* as based on the Joint Forum's 2006 high-level principles for business continuity. It encompasses *Critical Functions* as defined by the FSB which includes activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the bank or its role in the financial system.
4. We appreciate MAS' inclusion of 'Examples of Business Services' in the appendix (2.4) and would welcome further guidance on how wide or narrow is the definition of a Critical Business Service to help with more focused prioritization of Critical Business Services and setting more relevant/ accurate Service Recovery Time Objectives ("SRTO"). Example: For the provision of service 'Access to Savings', should 1) providing a view of available cash 2) dispensing cash, be considered as two distinct critical business services for which two different SRTOs must be set or not? We

recommend the former to help with more focused prioritization of Critical Business Services and setting more relevant/accurate SRTO.

Question 2: MAS seeks comments on the proposed establishment of Service Recovery Time Objectives (SRTO) for each critical business service, and the implementation of recovery strategies to meet the SRTO.

1. The SRTO concept appears to be broadly aligned with the concept of a 'tolerance for disruption' set out in the BCBS Principles defined as "…*the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios*." We welcome this conceptual alignment and our assumption is that SRTOs, like 'tolerances for disruption', are intended to be measures that should not be exceeded following an operational incident.
2. However, we note that the MAS nonetheless introduce a new term "SRTO" which does not feature in other operational resilience frameworks. In particular, the UK PRA framework for operational resilience used the term 'Impact Tolerance' which it defines as "*the maximum tolerable level of disruption to an important business service or an important group business service as measured by a length of time in addition to any other relevant metrics".* The MAS defines SRTO as a time-based metric, which provides clarity between FIs and their third parties on the recovery expectation of the critical business service.
3. As mentioned above, we would welcome further alignment with the BCBS Operational Resilience Principles and we would appreciate more clarity on the definition of SRTO. Differences in definition of key operational resilience concepts in local markets will not only increase organizational complexity but also increase the compliance divergence/ fragmentation. Adopting, or as a minimum aligning with existing terminology already in use in the industry would significantly reduce ambiguity and improve implementation of a relatively immature concept.
4. We also note that the Consultation Paper reads that "*FIs must ensure that the Recovery Time Objectives ("RTO"s) of the underlying business functions and their dependencies will meet its SRTOs*". Some global FIs have been implementing operational resilience programs to be aligned with the BCBS Principles and other regulatory requirements (e.g., the UK) and have discovered that a strategy to meet their tolerances for disruption (or other similar targets) that is dependent on the underlying function RTOs is not always achievable. Certain severe but plausible scenarios e.g., a sophisticated cyber-attack may prevent function RTOs being met, but that does not remove the need to remain within the stated tolerance for disruption (or recover a sufficient level of service within the SRTO). We would therefore assume that an SRTO should be set at the point at which intolerable harm is likely to be caused to customers, the financial ecosystem, and its participants (which the Consultation Paper states firms must take into account when setting SRTOs). We would welcome clarification from the MAS on this issue and we would ask for more detail on the link between RTOs and SRTOs and the MAS' expectations around SRTOs. The ways to ensure that an FI remains within its tolerance for disruption (and ensure that the SRTO is met) could be numerous and may require some out-of-the-box thinking, but it is this flexible thinking that allows FIs to remain within their tolerances for disruption (and therefore meet the SRTO) without attaining individual function RTOs in those severe but plausible scenarios. We therefore suggest that instead of providing the term RTO for business function, firms should ensure that all

functions have the ability to support the SRTO of the critical business service and recommend that the link between RTOs and SRTOs be reviewed ahead of the final publication of the updated Guidelines.

5. We also note that the definition of SRTO within the glossary does not specify that they should be applied to critical business services only and would welcome clarification on this point. Without this clarification, there is a risk that FIs will be expected to apply SRTOs to a much broader range of services and functions than is required. This would impose a disproportionate burden on FIs and would not achieve MAS' aims. We suggest that the definition of SRTO in the glossary on page 13 of the Consultation Paper is aligned with the definition of SRTO in section 5.9, page 34 of the Consultation Paper, which defines SRTO as "*SRTO refers to the target time to recover a critical business service to a level sufficient to meet its business obligations, or the acceptable duration before the disruption of a critical business service would result in severe business impact and losses to the FI and any of its customers".*
6. Given that SRTO is a time-based metric, we would also appreciate clarification as to when the SRTO time period starts and stops, with reference to the availability of service. For example, is it appropriate for the objective to be set at the point in time that the service is only up and running, or would it be appropriate to set it at where the clearing of backlogs following recovery of the service (be that transactions, reconciliation, client queries, compensation claims) has been completed. Is the interpretation of SRTO to resume full BAU or to a pre-determined (lesser) capacity?
7. Most firms would have an existing service level agreement ("SLA") with their third-party providers and the SLA timelines are pre-defined as part of the agreement. It would be helpful if the MAS can clarify how such SLA differs from the proposed SRTO.
8. We are pleased to see that the guideline acknowledges that 'in the event of disruption it might not be practical nor possible to recover all business services and functions at the earliest opportunity (2.3) therefore FIs should prioritize the recovery of its business services and functions based on criticality' i.e. critical business services and critical business functions'. It also states that an FI can adopt the business impact analysis (BIA) methodology to assist in identification of critical business services and functions. Does it follow that a BIA and other similar methodologies can be used by FIs to articulate their thought process to ascertain criticality? Could FIs also cluster together critical business services that have similar business impact?
9. We are grateful to MAS for allowing FIs in adopting aglobal frameworks, policies and procedures that have been instituted at Group level 'as long as it enables FI's Singapore operations to comply with the Guidelines'. We would like to confirm that firms are to adopt existing accountability framework to evidence local compliance to Guidelines for firms' global critical business services.
10. Further clarification is appreciated on what 'recovery' criteria (3.1) are? There are instances whereby a lesser capacity is sufficient and resumption of BAU operation is not a good use of limited resources. For example - Due to COVID-19, it was acceptable that branches operate at degraded level due to the local ministry directive. Or if capacity is constrained following a disruption because of backlog.

Question 3: MAS seeks comments on the proposed development of an end-to-end dependency mapping on people, processes, and technology, including those involving third parties, for each critical business service.

1. Point 2.13 – "*The FI should perform its due diligence to obtain assurance that the SRTOs of the critical business service can be met by the third parties. This assurance can be obtained through measures, such as the following ,where possible:* (*a) Establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations; (b) Request for dedicated manpower from their third party service providers for specialist functions that cannot be performed in-house; or (c) Conduct audits, regular tests, or joint tests with their third parties to ensure that the third parties have the ability to support FIs even in the scenario that these third parties experience disruptions."*
    - We note and support that end-to-end dependency mapping for critical business services aligns with the BCBS Principles on Operational Resilience.
    - Our members take third party management very seriously, certainly in light of their BCM and ASIFMA and GFMA are very engaged in the global regulatory efforts on this front. However, we point out that the negotiation power that FIs have over their critical third parties depends on many factors, including the service package FIs are buying. Many third parties are moving from STOs to SLAs and there is an increasing reluctance among third parties to participate in bilateral tests. We also understand that many FMIs/FMUs do not conduct live failover testing. Adopting the requirements listed in 2.13 will thus be on a best-effort basis, and subject to contractual challenges. We also point out that there is no harmonized guidance to FIs on what is required to gain operational resilience assurance. Further, there is no guidance for the artifacts that a third-party must collect to provide these assurances to FIs. In combination, this may result in disparate requests from different institutions to the same service providers and FMIs/FMUs which may limit these entities from providing FIs the support required to demonstrate compliance.
    - Our members see the value of the requirement for end-to-end mapping of Business Services to enable them to enhance their investment decisions, to understand residual risks, and to ensure appropriate decision-making during disruption. We would however request more guidance from the MAS around what level of detail the MAS expect from FIs. For example, in the mapping of people resources, would a percentage of recovery staff suffice or does the MAS expect each recovery staff to be mapped to a process/ task? Given that staff attrition rate, evolving technologies and enhanced focus on client delivery, these processes will undergo continuous change. We foresee challenges to taking an overly granular approach and ask for more time for FIs to develop a level of mapping sophistication.
    - Mapping People, Process, and Technology to Business Services would benefit resilience, provided that the effort would require sufficient time for FIs to develop. We also note that the text of the consultation already provides a caveat "where possible".

2. We note that footnote 3 in Section 2.12 includes intra-group service providers in the definition of third-parties. We suggest that the final BCM Guidelines are aligned with the MAS Outsourcing Guidelines in terms of dealing with intra-group service providers, on a risk-based approach.
3. Point 2.15 – "*Some interdependency risks (e.g. unavailability of telecommunications networks, power utilities, etc.) may be beyond an FI's direct control to mitigate completely. Hence, it is important that FIs put in place risk mitigating measures, such as implementing redundancy or back-up arrangements, to address the interdependency risks posed by the disruption of these services."* As some of these utilities are critical national infrastructure (power utilities, telco service provider, internet service provider), we would like to seek clarification on whether MAS through other relevant government agencies require these utilities to maintain redundancy and high availability to service FIs in Singapore.

Question 4: MAS seeks comments on the expectation to conduct BCM audits that are commensurate with the criticality of the business services and functions.

1. We welcome that the MAS has taken our response to the first consultation paper on board and clarified in 2.17 that the scope and frequency of BCM audits should be commensurate with the criticality of business services and business functions and that any qualified independent party (whether internal or external) can perform the audit.
2. Audits are an essential tool in any FIs risk management approach. In order to remain aligned with the BCBS principles we recommend that the phrase "BCM audits" is amended to simply "audits". The BCBS principles identify BCM as one principle (Principle 3 Business Continuity & Planning) within Operational Resilience and, as such, to audit Operational Resilience an effective audit should not be limited to just BCM aspects.

Question 5: MAS seeks comments on any other aspects of BCM that warrant further guidance from MAS.

1. **Timeline:** For FIs that adopt a global operating model, some aspects of the business functions that support a critical business service may be performed outside Singapore. The work to incorporate and align the concepts of critical business services, SRTO, end-to-end business service mapping for interdependencies etc. may require significant amount of time and effort. We would therefore suggest a phased implementation approach (e.g. a period of time to determine an FI's critical business services and the establishment of SRTOs (or similar measure); a further period to conduct mapping and testing; and then a date by which any identified gaps (to SRTO or similar measure) are addressed), or an extended timeline of 24 months to give FIs sufficient time to comply with the Guidelines, or even have different deadline depending on the complexity of the change/requirement. For example, the UK PRA recognized that certain aspects of what they are asking for were complex and could be particularly onerous therefore allowed up to 3 years to come into compliance with the Impact Tolerance requirements.

<u>Comments Annex B – Revised Guidelines on BCM</u>

Section 3: Service Recovery Time Objective

1. Intermittent Service Availability, in addition to perhaps SRTO, is an area which may require additional consideration to properly assess, and time to implement, particularly as it may require additional tooling, monitoring and alerting (to assess cumulative delays against SLAs/deadlines for example) in order to properly comply.

Section 4: Mapping of interdependencies

1. Is there an expectation from MAS for FIs to review the exit clause for all its third-party SLAs (4.5)? and perform infrastructure or utility risk assessment for all its critical third-party suppliers (4.6) (including suppliers out of Singapore)?

Section 5: Concentration Risk

1. It is noted that MAS acknowledges the fact that due to a number of factors such as the differing size and complexity of business operations across FIs in Singapore, it would not be appropriate nor practical, to standardize on a criteria that defines a zone that could be applied equally across the financial sector. For smaller organizations or larger organizations with smaller teams that are performing specialized functions, it would be a challenge to adopt the suggested approaches to mitigate concentration risk. We hope that MAS can provide clarity on this point, as well as guidance for smaller firms.
2. In relation to section 5.2 (e) (cross-border support), we are grateful for MAS supporting this approach but we wanted to flag that regulators in other jurisdictions might not be as supportive of this approach. Any assistance that the MAS can provide in engaging with other regulators on the benefits of allowing cross-border support would be welcome. An area that may require further discussion is cross-border support for regulated/licensed activities. In these instances, we may need specific allowance for non-licensed or previously licensed personnel in another jurisdiction to provide support during a BCP event.
3. Also in relation to 5.2 (e) (cross-border support): as cross border support can help FIs establish a way to mitigate concentration risk, will MAS accept a risk-based approach for onshore only services in the event of a Singapore wide catastrophic event?
4. In relation to section 5.2 (f), whilst we appreciate that appointing an alternative service provider is one of the many options for FIs to consider to mitigate concentration risk, some members have some concerns about pre-designated alternative service providers. This is because there are existing guardrails such as checking/testing that the service provider has satisfactory business continuity plans, notification requirements should there be any adverse developments which could impact the services. In addition, there could be other viable alternative approaches in the event that the primary service provider is unavailable to provide service. For example, for thir- party service such as cloud, FIs may choose internal hosting as a primary contingency plan rather than alternative service provider. MAS may encourage FIs to focus on contingency plans for critical third-party service providers and allow FIs to assess whether to bring the service back in-house or transfer to a replacement service provider or leverage other means. Pre-designating an alternate service provider would increase operational cost without necessarily enhancing business continuity.

Section 6: Continuous Review and Improvement

1. Point 6.5 – "*An FI should regularly assess the need for additional tools and automation to enable it to manage an incident or disruption more effectively. These could include implementing tools that enhance the FI's BCM implementation or crisis management to better facilitate decision-making during a disruption."* - Implementing some of these requirements would mean upon a careful review, additional enhancements to the existing automated tools to extract the relevant information. As mentioned above, compliance within a 12-month time frame may be a challenge for the FIs. As mentioned further above, we suggest the MAS considers a 24 month implementation deadline.

Section 7: Testing

1. Component failover of specific application: we submit that this is not directly related to resilience but rather linked to availability which is covered in the MAS Technology Risk Management (TRM) Guidelines. Applications with high availability architecture will have many component failure mode for testing.
2. Restoring data from back-up media: We submit that this too focuses on operational backup for short-term recovery which is not related to resilience. The MAS TRM Guidelines already cover recovery for application testing.
3. In demonstrating End-to-End testing of dependencies, what is the expectation from FIs to evidence that each service component has been incorporated/aggregated into the SRTO? We would appreciate guidance about how to set (and distinguish between) SRTO of 'degraded and BAU service' and how they might be calculated. Clarification on how to ascertain 'trigger point' of the event of disruption is also appreciated.

Section 9: Crisis Management and Communications

1. Point 9.5 – "FIs *should ensure that MAS is notified immediately of incidents where business operations are, or will, be severely disrupted, or when the BCP is activated, or going to be activated in response to an incident. In the notification, the FI should provide information, such as the assessed impact to its customers and the actions that have been taken (e.g. activation of alternative service channels, alternate sites or manual procedures, public communications, etc.)"* – We would like to seek clarity from the MAS on the time limits to notify as the organization would require some time to activate the incident response, understand the issue and initiate appropriate resolution measures. For example, Notice 644 Technology Risk Management states that "a bank shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident". We hope the MAS will agree that the impacted organization will need to assess the impact of an event, initiate failover and recovery strategies etc. and then provide an effective understanding of the situation and action being taken, within a reasonable timeframe (e.g. perhaps within 1 hour of a BCP event being confirmed).

Section 10. Responsibilities of Board and Senior Management

1. Item 10.6 which requires "*an annual attestation to the Board on the state of the FI's BCM preparedness, the extent of its alignment with the Guidelines, and key issues requiring Board's attention such as significant residual risk and assessment of BCM readiness"* seems overly prescriptive.
1. For many of our members, the Singapore operations rely largely on global systems and functions together with their regional and global approach for governance and oversight of BCP (including management/monitoring of testing, escalation of resiliency issues and their mitigation/remediation, etc.).
2. Understanding that some form of reporting to the Board may be required, but wonder whether global multi-national organizations with established global frameworks for BCM can leverage/outsource those frameworks and governance/oversight without requiring what seems to be a very a detailed attestation to the Board?