asifma

Growing Asia's Markets

31 July 2026

To:
Monetary Authority of Singapore
Technology & Cyber Risk Supervision Department

Submitted via FormSG

ASIFMA Response to MAS Consultation Paper on Proposed Amendments to Notices on Technology Risk Management

Dear Sir/Madam,

On behalf of the Asia Securities Industry & Financial Association ("**ASIFMA**")[1] Financial Institution and Asset Management members (together, "**FI**")[2], we are pleased to respond to the Monetary Authority of Singapore ("**MAS**") Consultation Paper on Proposed Amendments to Notices on Technology Risk Management, with the support of Ernst & Young.

Across the consultation, members broadly support the intended regulatory outcomes and a consistent theme throughout the feedback is the importance of adopting a risk-based, proportionate and principles-based approach to implementation. Members emphasise that requirements should be calibrated according to the criticality of systems, materiality of risks, operational complexity and firms' risk profiles, rather than applying a one-size-fits-all approach.

Members also highlight the importance of maintaining flexibility in implementation, recognising the diversity of technology environments, operating models and organisational structures across the industry. There is broad support for outcome-focused requirements that establish clear risk management objectives while allowing firms to leverage existing governance, risk management and operational resilience frameworks.

Members emphasise the importance of maintaining clear and consistent definitions, materiality criteria, treatment of third-party dependencies and supervisory expectations to support consistent implementation. Members also note that implementation timelines should be proportionate to the scale and complexity of the proposed requirements.

Overall, the industry supports MAS' efforts to enhance the resilience and security of the financial sector and encourages MAS to continue applying a risk-based, proportionate and practical approach that focuses on risk management outcomes while preserving implementation flexibility for FIs.

---

[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, and competitive 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. More information about ASIFMA can be found at: www.asifma.org.

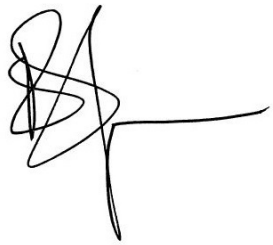
[2] ASIFMA Membership Composition: https://www.asifma.org/membership/members/

ASIFMA Headquarters
Unit 3603, Tower 2, Lippo Centre
89 Queensway
Admiralty, Hong Kong
Tel: +852 2531 6500

ASIFMA Singapore Office
12 Marina View, Asia Square Tower 2
Level 11, #11-01
Singapore 018961

We would be pleased to discuss our response in further detail. Should you wish to do so, please do not hesitate to contact me at rkapoor@asifma.org.

Sincerely,



Rishi Kapoor
Executive Director
Head of Technology and Operations
Asia Securities Industry & Financial Markets Association

ANNEX

Question 1: MAS seeks comments on the proposed scope of the IT asset inventory and the information to be recorded and maintained by FIs.

1.1 Adoption of a Risk-Based Approach

A. Members believe the proposed IT asset inventory requirements should be implemented using a risk-based and principles-based approach, focusing on critical systems, material dependencies and assets with significant operational or customer impact. Firms should have the flexibility to determine the scope and structure of their inventory management practices based on their risk profile, organisational size, technology landscape and adoption of emerging technologies.

B. Members generally support MAS establishing overarching principles and governance expectations for IT asset management, while emphasising the importance of allowing institutions flexibility in implementation. Several members express concerns that the proposed requirements in Appendix A may be overly prescriptive for inclusion within a Notice, noting that detailed operational expectations may be more appropriately addressed through supporting Guidelines rather than binding regulatory requirements.

C. Additionally, some members believe that the Notice should focus on the intended risk management outcomes, such as vulnerability management, patch management and technology obsolescence management, with IT asset inventories serving as supporting controls rather than standalone compliance objectives.

1.2 Practical Challenges of Maintaining a Single Comprehensive Asset Inventory

A. Some members propose that firms should be permitted to maintain separate inventories for different asset categories, provided that appropriate governance and oversight mechanisms are in place. A single consolidated inventory may not be practical for all asset classes.

B. Members note that hardware, software, cryptographic assets, auto components and third-party components often require different management processes, data attributes and tooling. As a result, maintaining separate inventories may be operationally more practical and effective. Additionally, a member suggests that Appendix A could instead be turned into a Guideline (see paragraph 1.1B above).

C. While members generally agree with the information fields set out in Appendix A, requiring firms to maintain all prescribed attributes in a specific manner may result in significant implementation effort without necessarily enhancing risk management outcomes. Members therefore recommend that MAS allows flexibility in the implementation of Appendix A, with firms retaining flexibility to determine how asset information is captured and maintained, provided they can demonstrate effective inventory management and governance.

1.3 Scope Inclusion for Open-Source Software, Cloud Assets, Third-Party Components and Dependency Mapping

A. **Open-Source Software and Dependency Management**: Members highlight the complexity of tracking all open-source software dependencies, particularly transitive dependencies embedded within commercial software where visibility is limited. They propose further guidance on the scope of tracking expectations (e.g., direct, transitive, or

material dependencies) and express a preference for inventory requirements to focus on material and critical dependencies. Some members suggest that direct and indirect dependencies should not form part of the prescribed minimum information set and would welcome clarification on the specific risks the requirement is intended to address, to support proportionate implementation and risk-based scoping.

B. **Third-Party Components and Dependency Mapping**: Members highlight challenges in maintaining inventories of vendor-managed assets and dependencies and propose that MAS allow firms to implement risk-based prioritisation while improving vendor transparency for dependency mapping.
C. **Shadow IT**: Consistent with a risk-based approach, members suggest focusing on the identification and management of unmanaged assets that are material to critical systems or customer services, rather than requiring the exhaustive inclusion of all shadow IT assets within formal asset inventories.
D. **Cryptographic Assets**: Members recommend a risk-based inventory approach focused on critical systems and customer data and propose that MAS recognise platform-based continuous assurance from managed certificate authorities (CAs), key management service providers (KMSs), hardware security modules (HSMs) and certificate lifecycle management platforms as equivalent evidence to a static inventory or register.
E. **End-of-Life and End-of-Support Assets**: Some members see merit in capturing end-of-life (EOL) and end-of-support (EOS) information to strengthen asset lifecycle management and support risk identification. However, members suggest these attributes be implemented as good business practice rather than being prescribed as mandatory Appendix A fields, consistent with a principles-based and proportionate approach.
F. **Asset Coverage**: Members support a risk-based approach to asset coverage, with inventories focused on assets that support critical systems and the delivery of customer services. Members propose that non-production environments should not be included in the scope of an asset inventory, while other assets such as end-user devices, cloud native assets, cryptographic assets, shadow IT, IoT/OT assets, and development and test environments should be included based on their risk profile, materiality and relevance to operational resilience objectives. Members also note that based on their experience, for items such as cryptographic assets, the process of identification and inclusion in an inventory is likely to be a multi-year process.
G. **Alignment to Global Regulations**: Convergence with international standards supports consistent implementation for globally active institutions. As such, members suggest that MAS consider providing implementation guidance or transitional arrangements that recognise the maturity curve for different asset categories, similar to the phased approach being adopted in some EU jurisdictions. This would acknowledge that while hardware and software inventories are generally mature, cryptographic asset inventories and comprehensive open-source dependency mapping may require significant investment in specialised tooling and processes.

1.4 <u>"Up-to-Date" Asset Inventory Maintenance Expectations</u>

A. Members suggest that MAS further consider its expectations regarding the timeliness and maintenance of asset inventories, including what constitutes an "up-to-date" inventory and whether minimum refresh expectations apply. Members recommend that MAS allow FIs to determine the appropriate frequency for maintaining and updating asset inventories based on their operating environment, asset criticality and change management

processes. Prescribing a minimum refresh cycle may not be appropriate given the differing characteristics and update frequencies across asset classes.

B. Members express concern that expectations for continuously updated inventories may effectively necessitate the deployment of automated discovery and reconciliation tools, resulting in substantial implementation effort, ongoing maintenance requirements and additional costs for firms. Such tools are also not readily available in the market at scale in areas such as cryptography.

1.5 Protection of Sensitive Information within Asset Inventories

A. Members are concerned regarding the sensitivity of information contained within IT asset inventories and the potential cybersecurity risks associated with regulatory requests for detailed inventory information, which should be avoided. Highly detailed IT asset inventories contain information that could expose firms to heightened security risks if accessed or distributed inappropriately.

B. They support a risk-based data minimisation approach that balances supervisory needs with cybersecurity and data protection considerations. It is best practice for this information not to leave the firm's network perimeter and any supervisory interaction with this information should be done in a "reading room" like construct.

1.6 Implementation Considerations

A. Members recommend considering a phased implementation approach, recognising that inventories for hardware and software are generally more mature than those for cryptographic assets and open-source dependency mapping, which may require integration with key management systems, certificate management tools, software composition analysis (SCA) tools and other specialised technologies. For example, comprehensive tracking of open-source components, including transitive dependencies, may require the deployment or enhancement of automated tooling and associated governance processes.

1.7 Alignment with Other MAS Technology Inventories and Registers

A. Members note the potential overlap between the proposed IT asset inventory requirements and other MAS initiatives, including the proposed Third-Party Risk Management Guidelines (particularly the Register of Third-Party Arrangements) and the Guidelines on AI Risk Management.

B. Members encourage MAS to harmonise requirements relating to system criticality, service dependency mapping, third-party dependency tracking and technology inventories across regulatory frameworks to reduce duplication, minimise implementation complexity and promote consistency.

C. Members also suggest that, rather than mandating the recording of the "criticality of supported system" for every IT asset in Appendix A, MAS consider requiring firms to maintain linkages between IT assets and the critical systems or business services they support.

Question 2: MAS seeks comments on the proposed scope of the IT risk assessment, the information to be maintained in the IT risk register and whether specific KRIs should be specified in the Notice for the monitoring of material identified risks.

2.1 Definition of "Material Identified Risks"

A. Members recommend that FIs retain flexibility to determine what constitutes a material identified risk based on their risk profile, business activities and risk management framework. Firms should be able to establish and document their own materiality criteria, supported by appropriate governance and oversight.

2.2 KRI Guidance and Implementation Flexibility

A. Some members observe that the proposed KRI requirements are more prescriptive than comparable international frameworks, such as the UK PRA Operational Resilience Framework, APRA CPS 230 and the Basel Committee's Principles for Operational Resilience. These frameworks focus on achieving resilience outcomes and do not prescribe specific KRIs or metrics.

B. As such, members caution against prescribing specific KRIs and recommend that firms should be allowed to retain flexibility to define KRIs based on their risk profiles, operating models and risk appetites. A principles-based approach would be more consistent with international standards, while enabling firms to implement risk management practices that are tailored to their operational resilience objectives and business environments.

2.3 Requirement to "Effectively Monitor" Material Risks

A. Members suggest that the assessment of whether KRIs are being monitored effectively should be determined by individual firms within their established risk appetite and governance frameworks, rather than through prescriptive regulatory criteria.

2.4 Frequency of IT Risk Assessments and Risk Register Reviews

A. Members generally support a risk-based approach and propose that firms retain flexibility on review frequency, based on their risk management frameworks and risk appetites. Several members suggest that the Notice should focus on outcomes and governance frameworks, while more detailed guidance could be provided through the TRM Guidelines.

B. Members suggest that firms should have flexibility to maintain risk registers within their existing risk management frameworks. An enterprise-level risk register aligned with existing governance processes, tooling and risk taxonomies should generally be sufficient, provided material technology risks are appropriately identified, monitored and managed.

C. Members believe it is appropriate to leverage existing risk management artefacts, assessment processes and governance frameworks to satisfy the proposed requirements, where they already achieve the intended risk management outcomes. They suggest MAS acknowledge this in the final Notices to provide greater clarity to the industry.

2.5 Scoping of IT Supply Chain Risk Assessments

A. Members suggest that a risk-based approach can be adopted, whereby enhanced monitoring is focused on material or higher-risk suppliers rather than applying uniform requirements across all suppliers.

B. Some members suggest that the minimum scope of the IT risk assessment and risk register requirements under the Notice should focus on critical systems. Broader risk assessment coverage beyond critical systems should be implemented on a risk-based basis, with more

detailed expectations provided through the TRM Guidelines rather than prescribed within the Notice.

C. Members suggest that MAS clarify whether the reference in clause 2.5 to threats and vulnerabilities associated with "IT supply chains and the use of artificial intelligence" is intended to address AI-related risks within IT supply chains, or whether MAS is referring to IT supply chain risks and AI-related risks as two separate areas.

2.6 <u>AI-Related Risks</u>

A. Members support MAS' recognition that IT risk assessments should consider AI-related risks and AI-enabled threats. Members recommend that AI-related requirements remain technology-neutral, risk-based and principles-based, leveraging existing risk management, governance and monitoring frameworks (e.g., MAS Guidance on recent Safeguards for Agentic Finance at Runtime) rather than introducing prescriptive AI-specific controls.

B. Members support a risk-based approach to AI supply chain risks focused on material third parties and critical AI-enabled services, where there is a distinction made between external AI-enabled threats and risks arising from a firm's own use of AI. Given the rapid evolution of AI technologies and threat vectors, firms should be required to identify, assess and mitigate AI-related risks in a manner proportionate to their use cases and risk profiles.

Question 3: MAS seeks comments on the proposed capacity planning and management requirements, including whether a specific frequency should be prescribed for capacity planning.

3.1 <u>Capacity Planning, Recovery Considerations and Dependency Analysis</u>

A. Members observe that the proposed requirements extend beyond monitoring current system utilisation and require firms to consider future capacity demands. In addition to current workloads, firms are required to consider projected business growth, future workload increases, traffic surges and peak demand scenarios, and potential changes in technology environments when assessing capacity requirements. In this regard, firms should be permitted to determine the appropriate methodologies, assumptions and planning horizons for capacity assessments. Members suggest that regulatory requirements should focus on ensuring capacity is sufficient to support operational resilience and risk management objectives, rather than requiring firms to provision capacity for anticipated business growth. In that regard, paragraph 11 should be amended to remove the requirement for projected business growth as this should be part of different planning activities within the FI.

B. Members generally do not support prescribing a single fixed frequency for capacity planning, as an appropriate frequency may vary depending on the size of the FI, the nature and criticality of business services, the complexity of technology environments and the rate of organisational change. A risk-based approach would provide firms with the flexibility to determine an appropriate review cycle while ensuring that capacity remains sufficient to support business needs.

C. Some members suggest that the requirements should be aligned with the Business Continuity Management (BCM) Guidelines, particularly the concept of Service Recovery Time Objectives (SRTOs) for critical business services. Members note that while technology recovery metrics may support capacity planning, they do not always provide a

complete measure of end-to-end business service recovery timelines, which may depend on multiple systems, infrastructure, data and operational processes. Additionally, given the overlap with existing BCM and operational resilience requirements, some members suggest that detailed capacity planning requirements may be more appropriately addressed through the TRM Guidelines rather than the Notices.

D. Members believe the frequency and depth of load and stress testing should be determined by the FI based on the criticality of the system, its risk profile, and the potential impact of capacity constraints on business services.
E. Members support a proportionate and risk-based approach to dependency analysis as part of capacity planning and resilience assessments. Firms should have the flexibility to determine the appropriate depth of dependency mapping based on materiality and risk, with enhanced analysis applied where warranted. Dependency assessments should focus on material dependencies across supporting systems, infrastructure and third-party services, rather than requiring comprehensive mapping of the entire dependency chain in all circumstances.
F. Members suggest that the requirements recognise cloud operating environments that scale automatically with demand, with automated scaling accepted as a valid capacity management approach. This would allow firms to achieve the intended outcome of maintaining sufficient capacity in a manner proportionate to their technology environment.

3.2 Materiality Threshold for Capacity Degradation

A. Some members note that the requirement to prevent system degradation may be overly broad. Minor performance fluctuations may occur in normal operations and that it would be impractical to escalate and report any level of degradation as a regulatory concern. Members highlight that requirements should focus on capacity constraints or degradation that materially affect service delivery, operational resilience or customer outcomes.
B. Therefore, we also recommend applying materiality to escalation and reporting, where the definition of capacity is linked to the prevention of *material* performance degradation, rather than any level of performance degradation, which could occur for any number of reasons and be within the FI's risk appetite.
C. Consistent with a principles-based approach, members suggest firms determine degradation indicators and thresholds proportionate to each system's criticality - supported by principles and examples rather than prescribed quantitative thresholds.

3.3 Third-Party Dependencies in Capacity Planning

A. Members note that capacity planning should take into account relevant dependencies, including outsourced and third-party services where these support critical systems or business services. Firms should retain the flexibility to determine how such dependencies are incorporated into their capacity planning processes, taking into account the nature of the dependency, contractual arrangements and the criticality of the underlying service.

Question 4: MAS seeks comments on the proposed requirements on continuous system and security monitoring, including the scope of monitoring, indicators and thresholds, response and remedial action frameworks, and key implementation considerations.

4.1 Flexibility in Monitoring Framework Design and Implementation

A. Members believe firms should retain flexibility in their design and implementation of system and security monitoring frameworks, provided that monitoring arrangements remain commensurate with the firm's operational risks and technology environment.

B. We emphasise that firms operate diverse technology environments and they may implement monitoring capabilities differently, depending on their technology architecture, operating model, risk profile and available tooling.

C. As such, members suggest that firms should be accorded flexibility in determining the specific monitoring tools utilised, monitoring methodologies and approaches, indicators and thresholds, escalation and response arrangements, and implementation models across different environments.

4.2 Recognition of Practical Limitations of Continuous Monitoring

A. Members note that new threats, vulnerabilities and incident scenarios emerge constantly, meaning firms often adapt and enhance monitoring capabilities as they learn from incidents and industry developments. While members recognise the importance of continuous improvement considering the evolving threat landscape, there is concern that the proposed requirements may create unrealistic expectations regarding the completeness or effectiveness of monitoring controls.

B. The requirements should therefore focus on establishing robust monitoring processes and continuous improvement mechanisms, rather than creating an expectation that monitoring controls can address every conceivable scenario. Members suggest that MAS allow FIs to define an implementation plan for full deployment, with prioritisation of most critical systems first.

C. Some members note that international frameworks recognise the practical limitations of monitoring controls in an evolving threat landscape. For example, certain threats may evade detection despite robust controls, including zero-day vulnerabilities, advanced persistent threats and supply chain compromises. As such, members recommend that the requirements focus on having robust monitoring processes, threat intelligence integration, incident response capabilities and continuous improvement mechanisms. This would align with international frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001 and the UK Cyber Assessment Framework, which recognise cybersecurity as a continuous journey of resilience and maturity enhancement, rather than a static state of complete protection.

4.3 Applicability to Vendor-Managed Systems and Third-Party Services

A. Members support the objective of strengthening monitoring capabilities but emphasise the importance of maintaining a principles-based approach that provides firms with flexibility in how their monitoring frameworks are designed and implemented.

B. Consideration should be given to situations where firms have limited control or visibility over monitoring activities performed by third-party service providers. As a result, firms may not always be able to implement the same level of monitoring that can be achieved within internally managed environments. In the event where direct monitoring is not possible,

firms should be allowed to leverage compensating controls, oversight and contractual assurance mechanisms in order to manage risk within their risk appetite.

4.4 Change Management Controls and Testing Requirement

A. Members support pre-implementation testing of critical system changes, but note that certain administrative activities (e.g., user account deletions, gateway removals and infrastructure restarts) may not be practical to test in advance.

B. Members therefore suggest that MAS clarify the requirement for testing of changes to critical systems. In particular, members propose that the requirement be framed as "testing for all changes to critical systems, except where testing is not applicable", rather than requiring testing for all changes in every circumstance. Additionally, members propose that firms be allowed to take a risk-based assessment and apply exemptions where applicable.

Question 5: MAS seeks comments on whether FIs should be required to maintain data backups that are both immutable and offline, or whether maintaining either form of backup would suffice to enable the timely and reliable resumption of the FIs' relevant business services. MAS also welcomes suggestions on alternative approaches or strategies to achieve the same objective.

5.1 Focus on Recovery Outcomes Rather than Prescriptive Backup Methods

A. Several members question whether mandating both immutable and offline backups is the most effective way to achieve the underlying objective of timely and reliable service recovery. Members note that many other international frameworks (e.g., US CISA Guidance on Ransomware Protection, NIST SP 800-34 and the UK Operational Resilience Framework) adopt outcome-focused requirements where backup strategies are assessed against recovery outcomes such as Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), business service resilience and cyber resilience requirements.

B. Therefore, members believe that the Notices should also focus on demonstrating the ability to recover systems and data within established recovery objectives, rather than prescribing specific backup methodologies. Firms should have the flexibility to adopt backup strategies that best support timely and reliable service restoration.

C. Members believe that they should retain the flexibility to determine the appropriate testing approach for their backup and recovery arrangements, taking into account their operating environment, recovery architecture and recovery objectives. The effectiveness of recovery arrangements should be assessed based on the firm's ability to meet established recovery outcomes, rather than through prescribed testing methodologies.

5.2 Clarification of "Offline Backup" Definition

A. Members note that the term "offline backup" could be interpreted narrowly as requiring physically disconnected backups. While such approaches may provide strong protection against cyber threats, they may not always be practical or compatible with rapid recovery objectives. Due to their separation from production environments, offline backups may be updated less frequently, potentially increasing the gap between backup and live data during a disruption and affecting a firm's ability to meet its RPOs.

B. Members therefore recommend that firms retain the flexibility to implement the most appropriate combination of backup controls for their operating environments, provided they can demonstrate that recovery objectives can be achieved. In particular, MAS could consider recognising immutable storage and logically segregated backup environments where these solutions provide effective protection against unauthorised modification or deletion, while supporting more timely recovery and more frequent data capture.

5.3 Flexibility in Implementing Backup Controls

A. Members believe firms should retain flexibility in the implementation of backup controls, including immutability and segregation mechanisms, provided they can demonstrate that backup arrangements effectively support their cyber resilience and service recovery objectives.
B. Given the diversity of technology environments, business models and recovery architectures, a single implementation model may not be appropriate across all institutions. Members also suggest that the requirements recognise cloud and SaaS environments, where firms may rely on third-party providers' backup and recovery capabilities, provided they can demonstrate that the relevant recovery and resilience objectives are met.
C. Members recommend allowing firms to implement either immutable or offline backups based on risk assessments and recovery requirements, rather than mandating both controls concurrently. Members note that immutable and offline backups independently address the primary risks of unauthorised modification, corruption, encryption or deletion of backup data. Members suggest that firms may implement other compensating controls such as strong encryption, access controls, segregation of duties, monitoring and other security measures that prevent unauthorised access or alteration of backup data.

5.4 Scope of Data Subject to Backup Requirements

A. Members suggest that MAS clarify that backup requirements should be proportionate to the objective of supporting the recovery of relevant business services. Firms should be permitted to focus on critical data, systems and supporting information necessary to achieve established recovery objectives, rather than applying the same backup requirements across all data assets.
B. There is concern that the current wording may unintentionally broaden the requirement beyond the assets and information necessary for operational resilience, which can ultimately make good backup and restoration of the necessary data harder to achieve.

5.5 Clarification of Applicability to SaaS and Third-Party Services

A. As firms rely on SaaS solutions, cloud service providers and outsourced service arrangements to support systems and services, firms should be permitted to determine the most appropriate governance, contractual arrangements and technical controls to ensure that backup and recovery arrangements support established recovery objectives.

5.6 Clarification of "Relevant Business Services"

A. Members recommend that MAS avoid introducing a separate concept of "Relevant Business Services" where the intended scope substantially overlaps with the existing concept of Critical Business Services (CBSs) under the BCM Guidelines. They note that the introduction of new terminology for similar concepts may create unnecessary complexity, ambiguity and implementation challenges, particularly where firms already manage their

business continuity and operational resilience obligations through established frameworks.

B. To support consistent implementation, members suggest that MAS either align the definition of "Relevant Business Services" with existing regulatory concepts or provide clear guidance on how it differs from CBSs and how both concepts should be applied within firms' operational resilience frameworks.

Question 6: MAS seeks comments on whether there is a need to prescribe the backup frequency for immutable and offline data backup respectively.

6.1 Backup Frequency Should Align with RTO and RPO Requirements

A. Members do not support a prescriptive backup frequency requirement within the Notices and believe that regulatory expectations should instead focus on whether backup arrangements support the achievement of the firm's RTOs, RPOs and service recovery objectives. As recovery requirements vary across systems and services, members believe that aligning backup tools, processes and recovery capabilities with the recovery objectives they are intended to support is a more effective, outcome-focused approach than prescribing specific backup frequencies that might result in requirements that are either excessive for some systems or insufficient for others.

6.2 Focus on Critical Data Rather Than All Data

A. Members note that the requirement should focus on data that is necessary to support the recovery of relevant business services. Consideration should be given to focusing backup requirements on data that is critical to supporting service recovery and resilience objectives, rather than applying uniformly to all data associated with those services.

B. Any definitions which create a requirement to capture an unnecessarily large quantity of data bring significant opportunity costs to firms. Not only is it more expensive to store that quantity of data, leading to the allocation of resources away from other risk management activities, but it also means recovery of the most vital data during a restoration event could be slower or harder to achieve.

Question 7: MAS seeks comments on the proposed areas that are to be covered in the incident management framework, and whether there are other key areas that should be included in the Notice.

7.1 Clarification of Incident Scope and Definitions

A. Members propose that MAS provides a definition for an "IT incident" as it is not defined in the proposed notices.

B. Members note that the reporting thresholds are generally and appropriately linked to incidents that have materially affected the FI or customer interests or involve validated unauthorised access resulting in actual data loss or other material impacts.

C. Members also suggest that the proposed requirements should leverage and align with existing regulatory definitions where possible, rather than introducing new or overlapping concepts. For example, there is support for using the existing definition of "IT security incident" as the foundation for the requirements, namely, an event that involves a security breach, such as hacking of, intrusion into, or denial-of-service attack on a critical system,

or a system which compromises the security, integrity or confidentiality of customer information.

7.2 Incident Management Requirements

A. Some members note that incidents vary significantly in severity and impact and that the proposed requirements may be interpreted as applying equally to all incidents regardless of significance. This is largely owing to the ambiguity of the definition of "IT incident" which is not defined in the proposed Notices.

B. Members suggest that MAS consider amending the incident management requirements to allow for greater proportionality to distinguish between routine operational incidents and incidents that warrant enhanced investigation, escalation and governance oversight. This would allow institutions to prioritise resources and escalation efforts towards incidents that have meaningful operational, customer, security or resilience impacts. In particular, paragraphs 17(b) and 17(c) of the Notices could be amended to require that the procedures allow the firm to determine when it is necessary to collect and preserve evidence or to notify senior management.

C. Members suggest that MAS adopt a risk-based approach to stakeholder and customer notifications, allowing firms the flexibility to determine notification requirements in accordance with their internal risk management frameworks.

7.3 Applicability to Third-Party and Supplier Incidents

A. Consideration should be given to situations where firms have limited visibility, control or access to information relating to supplier-managed incidents. Reporting requirements should be focused on information that communicates the impact to the firm and not information on the third party, which the firm is unlikely to have access to in the early stages of an incident.

7.4 Evidence Preservation Requirements

A. Evidence preservation requirements are typically associated with cybersecurity incidents, security investigations, forensic investigations and regulatory investigations, and applying these requirements to all incidents may impose a regulatory burden that is disproportionate to the risks.

7.5 Senior Management Notification Requirements

A. Members highlight the need for clear management escalation expectations and a defined interpretation of "senior management" for incident management and reporting purposes. Members also support a materiality-based approach to senior management escalation, whereby notification obligations are limited to incidents affecting critical systems or incidents that materially impact operations or customer services.

B. Additionally, members do not support a prescriptive requirement to notify MAS within one hour of incident discovery, given that a fixed one-hour timeline may result in premature or inaccurate reporting before sufficient information is available. Those members cite examples from the EU DORA and the new UK IT and Operational Incident Reporting guidelines both of which require reporting within 24hrs. Members suggest that reporting obligations should be triggered after an incident has been assessed and determined to meet the applicable materiality threshold, rather than from the point of initial discovery. Some members also suggest alignment with international standards and global regulations such as those of the HKMA, UK PRA/FCA and APRA.

Question 8: MAS seeks comments on whether the phrase "partial or intermittent disruption", as set out in the revised Notice, is sufficiently clear to enable consistent classification of disruption scenarios in practice for the purposes of computing unscheduled downtime of critical systems. Respondents are invited to suggest terms and definitions that will enhance the clarity of the requirement.

8.1 Materiality Determination for Criticality of a System and a Business Service

A. The definition of a critical system or a critical business service should align with existing MAS guidelines for operational resilience and business continuity, to ensure consistent interpretation and implementation. Firms should be able to determine what constitutes a critical system based on their materiality assessments.

B. Members recommend that MAS explicitly align the definition of a critical system with the concept of Critical Business Services (CBSs) under the BCM Guidelines. Specifically, a critical system should refer to a system whose failure would materially impair the delivery of a CBS, including the ability to meet the CBS's Service Recovery Time Objective (SRTO). Firms already maintain technology dependency mapping for CBSs, therefore, alignment would promote consistency, interoperability and more efficient implementation.

8.2 Materiality and Significance Should Drive Downtime Assessment

A. Members propose that MAS clarify whether the computation of unscheduled downtime for critical systems takes into account the impact on the business service or customers. Members believe unscheduled downtime calculations should be driven by the materiality and significance of operational or customer impacts, rather than the occurrence of any technical issue affecting a critical system without customer impact.

B. For example, members note that a technical failure within a component of a critical system may not necessarily affect service delivery, operations or customers. Likewise, security patching activities should not be regarded as unplanned/unscheduled activities. Requiring firms to count all such incidents as unscheduled downtime can create a disproportionate reporting burden and may not accurately reflect operational risk.

C. Members are concerned that a compounded unscheduled downtime cap may result in technical non-compliance, even where disruptions have no material impact on customers, service delivery or financial stability. Members therefore recommend that downtime assessments focus on the materiality and significance of service impacts and support an outcome-focused objective of maintaining high availability and resilience, rather than prescribing a fixed downtime threshold across all critical systems.

8.3 Materiality Based Incident Reporting

A. Members express concern that the revised "partial or intermittent disruption" wording can result in firms having to record and potentially report a large number of low-impact incidents. Members suggest focusing reporting requirements on disruptions that materially affect business operations or customer services to ensure proportionality.

B. Members also suggest that time requirements in incident reporting obligations should be linked to the determination of materiality or impact, rather than the initial occurrence of an incident, recognising that firms often require time to assess the significance of a disruption.

C. Members note that it is possible that an incident can occur for some time at a lower level that is not material and then escalate depending on various circumstances. The result can often be that a firm is de-facto non-compliant with the time requirements. For example, a database could experience an error that is trivial and would normally be resolved in routine restart processes at start of day. However, those processes could then fail, escalating the incident. The time difference between when the database experienced an error and when it became an impactful incident due to the failure of the normal resolution mechanisms could place the firm in non-compliance with the reporting timelines.

8.4 <u>"Partial or Intermittent Disruption"</u>

A. Members note that the introduction of the terms "partial" and "intermittent" disruption has created uncertainty within the industry regarding how downtime should be assessed and reported. Members suggest that "partial or intermittent disruption" should be assessed by reference to whether the disruption materially affects a firm's ability to meet its obligations to customers or support its operations. There is concern that overly detailed or prescriptive thresholds may not be practical given differences in operating models, customer bases and technology environments.
B. Members recommend that MAS provide practical examples illustrating reportable versus non-reportable disruption scenarios. Such examples would enhance consistency in industry interpretation and support more uniform implementation of the downtime reporting requirements.

8.5 <u>Clarification on Whether Critical System Failure Alone Constitutes Downtime</u>

A. Members note that consistent interpretation of unscheduled downtime depends on MAS clearly defining whether it is determined solely by the availability of a critical system or also by impacts on business operations and customer services.
B. There is concern that the wording of the revised Notice may imply a broader interpretation than previous guidance and discussions with MAS. This can result in firms counting outages affecting underlying components even where no service disruption occurs.
C. Members recommend aligning to the MAS TRM Notice FAQs which take into account impact on operations or customers. Moreover, if there are alternatives that customers may rely on to fulfil their requests, it demonstrates that resilience is already built into the system and it is not necessary to account for such situation in the downtime calculation.

8.6 <u>Guidance on Critical System Identification and Review</u>

A. Members believe that the frequency of reviews and reassessments of critical system classifications should be determined by the FI, taking into account the nature and criticality of the system, changes in business activities, technology architecture and risk profile.

Question 9: MAS seeks comments on whether the implementation timeline for the requirements of the Notice is sufficient.

9.1 <u>Considerations for a Longer Implementation Timeline</u>

A. Members suggest a phased implementation approach, noting that timelines should reflect the finalised requirements, the scale and complexity of compliance efforts, varying institutional capabilities, and the additional maturity and implementation challenges associated with evolving areas such as AI, IT supply chain risk management, dependency mapping, and third-party ecosystem oversight. For example, Phase 1 (12 months): Hardware, software, and critical system inventories; Phase 2 (24 months): Cryptographic assets, open-source components, and comprehensive third-party component mapping.

B. Some members suggest an implementation period of up to 24 months following publication of the final Notice, noting that significant investment and operational budget may be required to establish the necessary processes, governance arrangements and technology solutions. Moreover, firms that are operating in a larger scale or are part of international operations would require more time to embed these changes into their operations.