RESPONSE TO CONSULTATION REPORT

Consultation topic:	MAS Consultation Paper on Proposed Amendments to Notices on Technology Risk Management
Name/Organisation:	Investment Management Association of Singapore (IMAS)
Contact number for any clarifications:	6223 9353
Email address for any clarifications:	enquiries@imas.org.sg

Feedback:

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

Members generally welcome the greater clarity introduced by the revised Notice and Appendix A. This provides a useful baseline for establishing and maintaining IT asset inventories.

In view of the different business models and different system configurations deployed at each firm, IMAS suggests that MAS allows firms to adopt a risk-based approach to determine the appropriate scope of the information, which may not include the items listed in Appendix A, required for each IT asset. This particularly applies to IT assets such as Cryptographic assets.

A common concern raised across the membership relates to the expected scope of "direct and indirect dependencies" for open-source and third-party components. As currently drafted, the requirement may be read as obliging an FI to map the complete dependency tree of every such component. This information is often held by the software supplier or open-source community rather than the FI itself. A single component may involve hundreds of direct and transitive dependencies, and such information is not always publicly available or sufficiently detailed for proprietary third-party software.

IMAS requests that MAS clarify that the dependency information expected relates to the FI's own internal systems, applications or business processes that rely on a given open-source or third-party component, and not to the component's own internal dependency tree.

Members also seek clarification on the following points. Whether Software-as-a-Service solutions fall within the scope of the inventory. The appropriate level of granularity for itemising sub-components embedded within a broader IT asset, for example whether firmware or peripheral-level detail such as BIOS, UEFI or network interface cards is expected, or whether classification at the level of the asset itself would suffice. Whether standard automated inventory exports from common endpoint management tools would be accepted as satisfying the requirement for non-critical assets. Whether the inventory is expected to capture lifecycle milestones such as End-of-Support and End-of-Life dates, together with clear ownership and lifecycle checkpoints at onboarding, change and retirement. Members also note that "patch levels" is not a standardised or consistently trackable industry term, unlike software version numbers, and request that MAS adopt a more precise formulation.

2. MAS seeks comments on the proposed scope of the IT risk assessment, te 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.

Members are generally supportive of the proposed IT risk assessment, risk register and key risk indicator (KRI) requirements. These are broadly consistent with paragraph 4.1 of the existing MAS Technology Risk Management Guidelines.

Views are mixed on whether MAS should specify baseline KRIs within the Notice. Some members support a common set of baseline indicators, as this would enhance consistency and facilitate more effective industry-wide risk oversight. Other members prefer that MAS instead provide a high-level, non-exhaustive menu of suggested indicators. This would allow FIs to select KRIs appropriate to their operational scale, complexity and existing tooling.

Members request that the requirements be framed to support a risk-based and proportionate approach, rather than uniform application across all systems. The depth and frequency of risk assessments, and the granularity of risk registers and KRIs, should be commensurate with system criticality.

IMAS requests that MAS clarify the definition of "material risks", the expected level of granularity at the system level, for example per-system versus grouped or aggregated reporting, and how KRIs should demonstrate the effectiveness of mitigation measures in practice. Members also request that MAS publish supplementary implementation guidance or information papers, whether independently or with industry bodies such as IMAS, to support consistent interpretation of supervisory expectations.

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

Members support the objective of ensuring adequate capacity planning for critical systems, but raise concerns on the practical application of the proposed requirements.

Several members note that directly correlating commercial growth projections, such as projected customer numbers or transaction volumes, with specific technical capacity requirements is inherently uncertain and operationally complex, particularly for smaller or growing FIs. In practice, many institutions instead rely on existing enterprise budgeting and governance processes to determine appropriate capacity investment.

If a more prescriptive expectation is intended, members request that it be applied proportionately, having regard to the nature, size, complexity and criticality of the FI and its systems. For example, granular capacity planning would be more relevant for a fund manager operating retail-facing, daily-traded products than one managing privately placed restricted schemes subject to lock-up periods.

Some members observe that in modern distributed and cloud environments, system dependencies and demand patterns evolve dynamically. Continuous monitoring and resilience mechanisms may offer more meaningful, real-time visibility into emerging capacity constraints than static, formal dependency mapping.

On frequency, members prefer a risk-based approach over a fixed review cycle. Capacity plans should be reassessed following any material change in business or technological conditions. Several members suggest an annual review as a reasonable default, as this would align with existing IT budgeting cycles. IMAS also requests that MAS clarify the meaning of "systems that critical systems depend on" for the purposes of this requirement.

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.

Members are generally supportive of continuous system and security monitoring, but favour a principles-based rather than prescriptive formulation. Members caution against static, fixed definitions of indicators and thresholds. Effective monitoring is typically adaptive and evolves continuously in response to telemetry, threat intelligence and system behaviour. Response and remediation are usually operationalised through playbooks and real-time decisioning rather than rigid, predefined frameworks.

IMAS requests that the requirement focus on the effectiveness of detection and response capabilities, rather than the specific configuration of monitoring tools.

Members also seek guidance on how the requirement should apply where critical systems are operated by regulated third parties, or delivered via Software-as-a-Service arrangements, where FIs may have limited or no direct monitoring capability. IMAS requests that MAS confirm that monitoring obligations may be evidenced through vendor reporting and telemetry in such cases. Members also request a phased implementation approach that prioritises alerting on core production layers before extending to underlying infrastructure logs, given the deployment time and capital investment typically required to build continuous monitoring capability where it does not already exist.

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.

Members are aligned that FIs should be permitted to maintain either an immutable or an offline backup, rather than being required to maintain both. Requiring both would impose a duplication of infrastructure, operational processes and cost without a commensurate improvement in resilience. Immutable backups are increasingly delivered natively through cloud platforms, for example through immutability policies on cloud object storage. Offline backups typically require separate infrastructure and recovery procedures that may breach specified recovery time objectives.

IMAS requests that MAS adopt a technology-neutral, risk-based formulation, under which the FI's IT risk assessment determines the appropriate backup strategy for a given system. More resilient controls, potentially including both immutable and offline backups, or other technically equivalent controls, would be expected where the risk assessment identifies elevated exposure to data corruption, tampering or ransomware, for example for critical systems supporting systemically important business services.

Members also request that MAS treat immutability as a control outcome rather than a prescribed technology. This would allow smaller FIs to rely on alternative compensating controls, such as logical data segregation, air-gapping or role-based access restrictions, where dedicated immutable infrastructure is not warranted by their data profile.

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

Members are near-unanimous against a single prescribed backup frequency. They support a risk-based approach whereby backup frequency is determined by the criticality of the underlying data and systems, the applicable Recovery Point Objective (RPO) and Recovery Time Objective (RTO), and the results of the FI's IT

risk assessment. Periodic review and testing should validate that data can be restored within the required timeframe.

Different categories of data warrant different backup strategies. Transaction data supporting critical business services may require continuous or near real-time replication. Reference or archival data may reasonably be backed up at longer intervals. A single prescribed frequency risks being insufficient for rapidly changing critical data, and unnecessarily onerous for more static data.

IMAS requests that MAS not prescribe a fixed backup frequency, and instead confirm that a risk-based approach aligned to RPO is acceptable.

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.

Members are broadly supportive of the proposed areas covered under the incident management framework, including clearly defined roles and responsibilities, evidence collection and preservation, senior management notification, and stakeholder and customer communication.

Members request that the framework remain principles-based and proportionate, allowing FIs to align it with their existing incident management and operational resilience arrangements, rather than prescribing a single uniform structure. The depth of investigation and notification timing should be calibrated to incident severity and impact.

IMAS requests that MAS clarify the following. How the incident management framework interacts with the existing one-hour notification and 14-day root-cause and impact report obligations. The materiality threshold applicable to stakeholder and customer notification. Whether prompt senior management notification applies to all IT incidents or only to critical incidents. How the framework should apply where FIs rely on Software-as-a-Service providers for incident detection, investigation and reporting. The expected retention period for preserved forensic evidence, to assist IT teams in sizing logging and storage infrastructure.

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.

Member views on the clarity of the phrase "partial or intermittent disruption" are mixed. Some members consider the phrase to be a helpful and appropriately clear enhancement, ensuring the four-hour unscheduled downtime limit reflects customers' actual experience.

Other members note an inconsistency between the treatment of disruption under the Business Continuity Management (BCM) Guidelines and the revised Notice. The BCM Guidelines treat intermittent disruption as a sub-set of partial disruption, and adopt a materiality-based trigger for business continuity plan activation. The revised Notice distinguishes between the two concepts. As currently drafted, it could be read as requiring every instance of partial or intermittent disruption to be monitored and recorded irrespective of materiality.

IMAS requests that MAS align the terminology used across the BCM Guidelines and the revised Notice, and introduce a materiality threshold. This could reference the duration of the disruption, the proportion of customers, transactions or business services affected, or the impact on critical business services.

Members propose the following illustrative definitions. Partial disruption means a critical system that remains available but operates with degraded performance, causing delays to business-critical workflows beyond agreed service levels. Intermittent disruption means recurring or sporadic interruptions whose cumulative impact within a defined window exceeds agreed service levels, excluding scheduled maintenance. IMAS also requests that MAS clarify how intermittent disruptions should be aggregated for the purpose of computing total unscheduled downtime.

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

Member views on the sufficiency of the proposed 12-month implementation timeline are divided. A number of members favour an extended or phased approach.

Members who consider 12 months insufficient point to the sequential and interdependent nature of implementation. This comprises internal gap assessment and policy updates, vendor identification and engagement, due diligence, contractual review and negotiation, and technical implementation and validation. FIs also depend on external vendors, subcontractors and group-managed technology services to deliver the required changes, particularly smaller FIs without dedicated internal transformation capabilities.

IMAS recommends that MAS adopt a phased implementation timeline. A 12-month period would be workable for foundational governance requirements, such as core asset inventory management and critical-system-facing controls. A longer period of approximately 18 to 24 months would be more appropriate for requirements involving significant architectural or operational uplift, such as comprehensive dependency mapping across open-source and third-party components, enhancements to continuous monitoring capability, and immutable or offline backup infrastructure, as well as for emerging technology areas such as artificial intelligence and arrangements contingent on group or third-party co-ordination across jurisdictions.

10. Any other comments / remarks.

Members request that MAS provide continued supervisory and implementation guidance following finalisation of the Notice. This could be through Information Papers, updates to the Technology Risk Management Guidelines, FAQs, or continued industry engagement, including via IMAS, to support consistent interpretation of the revised requirements across the industry.

IMAS also suggests to MAS to consider and ensure alignment in terms and base requirements between this Notice and other Notices and Guidelines on overlapping topics such as Business Continuity Management (BCM), Third Party Risk Management, Operational Risk Management etc. This is to avoid confusion and duplication of efforts across related risk management regulatory requirements.