WONG PARTNERSHIP

MAS Consultation | Notices on Technology Risk Management

MAS Consultation on Proposed Amendments to Notices on Technology Risk Management

On 10 June 2026, the Monetary Authority of Singapore (**MAS**) launched a consultation seeking comments on proposed amendments to 11 MAS Notices on Technology Risk Management (collectively, **Notices**)[1] to strengthen the technology resilience of the financial services sector. The consultation closes on 31 July 2026.

The proposed amendments require the relevant financial institutions (**FIs**) to which the Notices pertain to implement measures across seven key areas: (a) IT asset management; (b) IT risk assessment and monitoring; (c) capacity planning and management; (d) change management controls; (e) continuous system and security monitoring; (f) immutable and offline data backup; and (g) incident management. The revised Notices also clarify the computation of unscheduled downtime for critical systems.

We summarise below the key proposals under the consultation paper and the questions on which MAS is seeking comments.

IT Asset Management

IT asset management entails the planning, tracking, handling and monitoring of an organisation's IT assets to maintain effective control and oversight across their entire lifecycle, from acquisition and deployment, to decommissioning and disposal. A key requirement is the maintenance of a proper inventory of IT assets, providing FIs with an accurate view of their IT operating environment and supporting other IT processes, including vulnerability and patch management, technology obsolescence management, cryptographic key management and digital certificate management. The inventory also facilitates the identification and management of risks relating to specific third-party components and supply chain issues.

MAS proposes that FIs maintain a comprehensive and up-to-date inventory of all their IT assets, which includes hardware, software, cryptographic assets, open-source and third-party components.

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] The 11 Notices are: (a) FSM-N03, Notice on Technology Risk Management to licensed insurers other than captive insurers and marine mutual insurers; (b) FSM-N05, Notice on Technology Risk Management to banks in Singapore; (c) FSM-N07, Notice on Technology Risk Management to credit card or charge card licensees in Singapore; (d) FSM-N09, Notice on Technology Risk Management to finance companies; (e) FSM-N11, Notice on Technology Risk Management to merchant banks in Singapore; (f) FSM-N13, Notice on Technology Risk Management to operators and settlement institutions of designated payment systems and holders of payment services licence (digital payment token service); (g) FSM-N17, Notice on Technology Risk Management to licensed credit bureaus; (h) FSM-N19, Notice on Technology Risk Management to registered insurance brokers; (i) FSM-N21, Notice on Technology Risk Management to capital markets financial institutions; (j) FSM-N23, Notice on Technology Risk Management to licensed financial advisers; and (k) FSM-N25, Notice on Technology Risk Management to licensed trust companies.

IT Risk Assessment and Monitoring

IT risk assessment and monitoring are essential to enable effective risk management in FIs. In conducting IT risk assessments, FIs must consider threats and vulnerabilities to which their systems may be subject, including those associated with their IT supply chains and the use of artificial intelligence (**AI**). They must then assess, in accordance with their established risk assessment criteria, the resulting risks, including the potential likelihood and impact of those risks affecting their operations or the services provided to customers (**identified risks**).

MAS proposes that FIs:

(a) **IT risk assessments**: Establish and maintain a framework and process to conduct regular IT risk assessments that cover these areas and implement risk mitigation measures that are commensurate with the identified risks (**risk mitigation measures**).

(b) **IT risk register**: Maintain an IT risk register that records: (i) the material identified risks; (ii) the risk owners who will be accountable for managing the material identified risks; and (iii) the measures to mitigate the material identified risks.

(c) **Key risk indicators (KRIs)**: Establish and maintain KRIs to effectively monitor the material identified risks and the effectiveness of the measures to mitigate the material identified risks.

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 Notices for the monitoring of material identified risks.

Capacity Planning and Management

Inadequate system capacity planning and management can lead to service degradation or disruption. MAS proposes that FIs establish a framework and process to ensure that the capacity of all critical systems, and the systems that the critical systems depend on, are sufficient to meet business needs, including projected business growth and potential surges in customer traffic.

Question 3

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

Change Management Controls

MAS notes that a significant number of IT incidents in FIs were attributed to poor change management. The lapses observed include insufficient risk and impact assessment of changes, poor understanding of system dependencies, inadequate testing of changes, and the absence of effective change recovery plans.

MAS proposes that FIs:

(a) **Prevention of unauthorised system changes**: Implement effective controls to prevent unauthorised system changes to maintain system integrity and availability.

(b) **Risk assessment of proposed changes**: Establish and maintain a framework and process to assess risks arising from proposed changes to their systems prior to implementation. Such assessments must evaluate the potential impact arising from the failure or incorrect implementation of the proposed changes, including the impact on upstream and downstream systems. FIs must implement risk mitigation measures commensurate with the risks identified.

(c) **Pre-implementation testing**: Carry out testing for all changes to critical systems before they are implemented in the production environment.

(d) **Change recovery measures**: Have in place effective change recovery measures to recover any critical system affected by any issue arising during or after change implementation.

Continuous System and Security Monitoring

MAS has observed that a number of major IT incidents have been attributed to lack of monitoring, delayed detection and/or slow response to rectify the causes of the incidents, such as those related to capacity, performance or cybersecurity.

MAS proposes that FIs establish and maintain a framework and process to continuously monitor all critical systems for timely detection and response to issues affecting system performance or security. The framework and process must include, at a minimum:

(a) Defined indicators and thresholds that trigger alerts; and

(b) Response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issue.

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.

Immutable or Offline Data Backup

System bugs, cyber-attacks (e.g., ransomware), and human errors can lead to loss and corruption of data that is essential to the delivery of FIs' business services. Implementing immutable and/or offline data backup forms an important part of a resilient data protection strategy to enable data recovery if that production data is corrupted, tampered with, or made inaccessible.

MAS proposes that FIs must maintain an immutable or offline backup of data that is crucial for supporting the FIs' relevant business services, to enable timely and reliable resumption of those services in the event the production data is corrupted, tampered with, or made inaccessible.

Questions 5 and 6

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.

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

Incident Management

In the event of an incident, FIs need a well-defined process and procedure to recover their systems and the affected services, so as to minimise the impact of the disruption and to maintain business and operational continuity.

MAS proposes that FIs establish an incident management framework and process, with clearly defined roles and responsibilities for managing and responding to IT incidents, including procedures to collect and preserve evidence for incident investigation, stakeholder and customer communication, and prompt notification to FIs' senior management upon identification of the IT incident to enable informed decision-making.

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 Notices.

Monitoring of Unscheduled Downtime

The current Notices require FIs to ensure that the total unscheduled downtime for each critical system does not exceed four hours within any 12-month period. FIs are presently required to monitor and document any such downtime that affects their operations or services to customers. MAS has observed that some FIs have not accounted for partial and intermittent disruptions that have affected their operations or services to customers, which undermines the intent of the original requirement.

MAS proposes to make it clear and explicit that any partial or intermittent disruption must be included in the computation of unscheduled downtime for critical systems.

Question 8

MAS seeks comments on whether the phrase "partial or intermittent disruption", as set out in the revised Notices, 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.

Effective Date

MAS proposes that the requirements set out in the revised Notices take effect **12 months** after the date that the finalised Notices are published.

Question 9

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

Submission of Comments

MAS seeks feedback on Questions 1 to 9, as well as other comments on the proposed amendments to the Notices, taking into account emerging risk developments, including AI-enabled threats.

Comments should be submitted by **11.30 pm on 31 July 2026** *via* FormSG.

If you would like information and/or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

Elaine CHAN
Co-Head – Financial Services Regulatory

LAM Chung Nian
Head – Intellectual Property, Technology & Data

TIAN Sion Yoong
Partner – Financial Services Regulatory

Kylie PEH
Partner – Intellectual Property, Technology & Data

CHAN Jia Hui
Partner – Financial Services Regulatory

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Cheang & Ariff
Advocates & Solicitors
Loke Mansion
273A, Jalan Medan Tuanku
50300 Kuala Lumpur
t +60 3 2691 0803
f +60 3 2693 4475
w cheangariff.com
-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com
-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com