FINANCIAL INSTITUTIONS | TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

MAS Proposes Amendments to Notices on Technology Risk Management to Enhance Technology Resilience

Introduction

In Singapore, financial institutions ("**FIs**") are subject to certain requirements on technology risk management, as contained in the Monetary Authority of Singapore ("**MAS**") Notices on Technology Risk Management ("**Notices**"). Against the backdrop of increasing digitalisation and an evolving risk landscape, MAS is proposing amendments to the Notices to reinforce the importance of the risk management measures and to strengthen FIs' technology resilience.

The proposed amendments will require the relevant FIs to implement measures across the following key areas:

1. IT asset management;
2. IT risk assessment and monitoring;
3. Capacity planning and management;
4. Change management controls;
5. Continuous system and security monitoring;
6. Immutable and offline data backup; and
7. Incident management.

MAS is conducting a public consultation of the proposed amendments, with stakeholders invited to submit their feedback by 31 July 2026.

This Update highlights the key amendments proposed and their implications for FIs in Singapore.

Current Framework

The current Notices on technology risk management and the FIs which they apply to include the following:

1. FSM-N03: licensed insurers
2. FSM-N05: banks
3. FSM-N07: credit card or charge card licensees
4. FSM-N09: finance companies

5. FSM-N11: merchant banks
6. FSM-N13: operators and settlement institutions of designated payment systems and holders of payment services licence (digital payment token service)
7. FSM-N17: licensed credit bureaus
8. FSM-N19: registered insurance brokers
9. FSM-N21: capital markets financial institutions
10. FSM-N23: licensed financial advisers
11. FSM-N25: licensed trust companies

Key Proposed Amendments

IT Asset Management

MAS proposes that FIs maintain a comprehensive and up-to-date inventory of all of their IT assets, including hardware, software, cryptographic assets, open-source and third-party components. This seeks to provide FIs with an accurate view of their IT operating environment and the ability to support other IT processes.

IT Risk Assessment and Monitoring

MAS proposes that FIs establish and maintain a framework and process to conduct regular IT risk assessments and implement risk mitigation measures that are commensurate with the identified risks.

MAS also proposes that FIs 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. Further, FIs must establish and maintain key risk indicators to monitor the material identified risks and the effectiveness of the measures to mitigate such risks.

This requirement seeks to enable effective risk management by ensuring that FIs consider the threats and vulnerabilities that their systems may be subject to, including those associated with their IT supply chains and the use of artificial intelligence.

Capacity Planning and Management

MAS proposes that FIs establish a framework to ensure that the capacity of all critical systems as well as the systems that the critical systems depend on, are sufficient to meet business needs, including projected business growth and potential surges in customer traffic.

This requirement seeks to ensure that FIs proactively plan and manage system capacity to meet their operational and business needs, and to cater for future growth.

Change Management Controls

MAS has noted that a number of IT incidents in FIs were attributed to poor change management. MAS thus proposes that FIs must implement effective controls to prevent unauthorised system changes in order to maintain system integrity and availability.

FIs are also required to put in place a framework to assess the risks arising from the proposed changes to their systems prior to implementation. These 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 then implement risk mitigation measures that are commensurate with the risks identified.

Further, FIs must carry out testing for all changes to critical systems before they are implemented. FIs must 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

To address the occurrence of major IT incidents caused by lack of monitoring, delayed detection and slow response to rectify the causes of the incidents, MAS proposes that FIs implement a framework to continuously monitor all critical systems for timely detection and response to issues affecting the system performance or security. At a minimum, this should include: (i) defined indicators and thresholds that trigger alerts; and (ii) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issue.

Immutable or Offline Data Backup

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

Incident Management

MAS proposes that FIs establish an incident management framework, with clearly defined roles and responsibilities for managing and responding to IT incidents. This should include: (i) procedures to collect and preserve evidence for incident investigation; (ii) stakeholder and customer communication; and (iii) prompt notification to FIs' senior management.

This requirement seeks to minimise the impact of the disruption and to maintain business and operational continuity in the event of any incident.

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

Effective Date

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

Consultation Questions

In this public consultation, MAS is seeking comments on the following:

1. The proposed scope of the IT asset inventory and the information to be recorded and maintained by FIs;
2. The proposed scope of the IT risk assessment, the information to be maintained in the IT risk register and whether specific key risk indicators should be specified;
3. The proposed capacity planning and management requirements;
4. The proposed requirements on continuous system and security monitoring;
5. Whether FIs should be required to maintain data backups that are both immutable and offline;
6. Whether there is a need to prescribe the backup frequency for immutable and offline data backup;
7. The proposed areas that are to be covered in the incident management framework;
8. Whether the phrase "partial or intermittent disruption" is sufficiently clear to enable consistent classification of disruption scenarios; and
9. Whether the implementation timeline for the requirements of the Notices is sufficient.

Concluding Words

The proposed amendments to the Notices represent a focused effort at enhancing the technology resilience of FIs in the context of a rapidly changing digital economy. The amendments, should they be adopted, will impose a wide set of requirements on FIs relating to their technology risk management.

FIs should thus assess their frameworks and processes to determine if they are in compliance with the enhanced measures, and if not, the remedial action that needs to be taken. Stakeholders may also wish to provide their feedback in this public consultation to address and concerns or uncertainties.

The full public consultation is available here.

If you have any queries on the above, or if you wish to seek advice on providing feedback on the proposed amendments, please reach out to our team set out on this page.

For regional financial services matters, please see Rajah & Tann Asia's Regional Financial Services Regulatory Practice for more information.

Contacts

FINANCIAL INSTITUTIONS

Regina Liew

HEAD

D +65 6232 0465
regina.liew@rajahtann.com

Larry Lim

DEPUTY HEAD

D +65 6232 0482
regina.liew@rajahtann.com

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Rajesh Sreenivasan

HEAD

D +65 6232 0751
rajesh@rajahtann.com

Steve Tan

DEPUTY HEAD

D +65 6232 0786
steve.tan@rajahtann.com

Benjamin Cheong 张汶权

DEPUTY HEAD

D +65 6232 0738
benjamin.cheong@rajahtann.com

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia
Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 | +855 23 963 113
kh.rajahtannasia.com

China
Rajah & Tann Singapore LLP
Representative Offices

Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820

Shenzhen Representative Office
T +86 755 8898 0230
cn.rajahtannasia.com

Indonesia
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR
Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
la.rajahtannasia.com

Malaysia
Christopher & Lee Ong

T +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar
Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

T +632 8248 5250
www.cagatlaw.com

Singapore
Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand
Rajah & Tann (Thailand) Limited

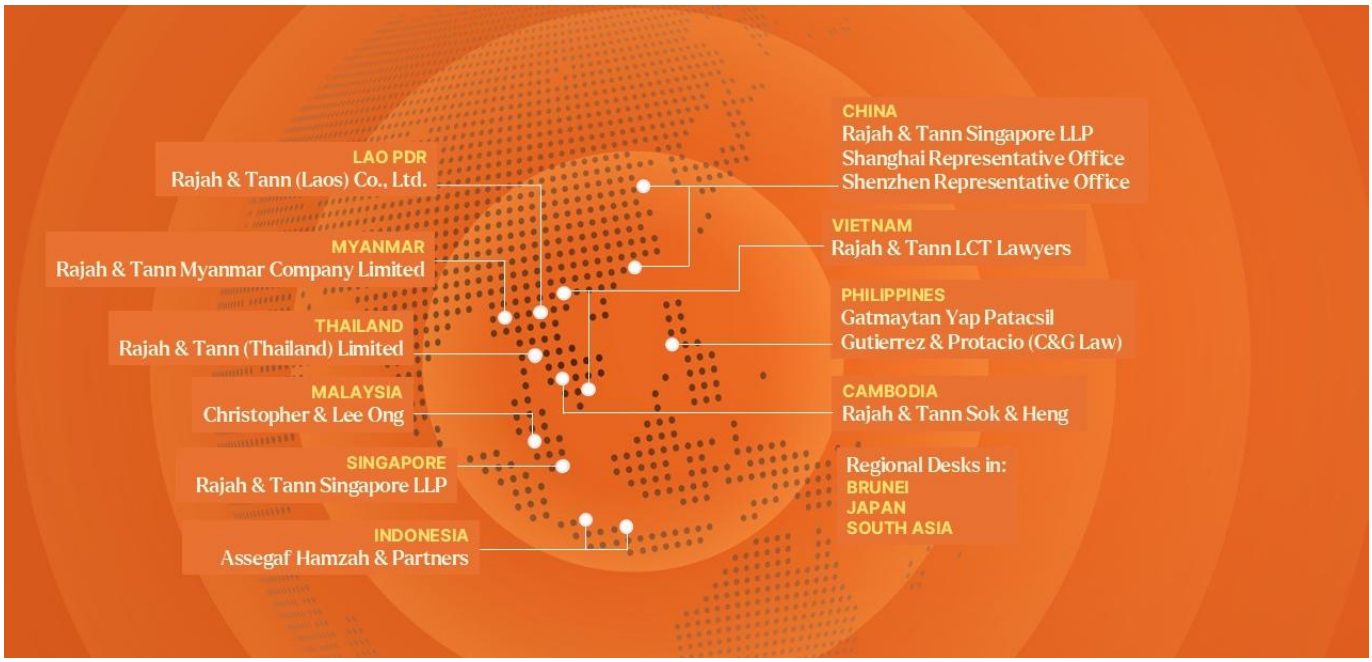
T +66 2656 1991
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2673 | +84 28 3521 2832

Hanoi Office
T +84 24 3267 6127 | +84 24 3267 6128
vn.rajahtannasia.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.