Frequently Asked Questions: Notice on Technology Risk Management

Q1: Which categories of financial institutions ("FIs") are subject to the Notice on Technology Risk Management ("Notice")?

A1: The FIs to which the Notices apply are:

S/No.	FIs	Governing Act	Notice No.
1	All- (a) approved exchanges; (b) licensed trade repositories; (c) holders of a capital markets services licence; (d) recognised market operators which are incorporated in Singapore; and (e) persons who are approved under section 289 of the Securities and Futures Act to act as a trustee of a collective investment scheme which is authorised under section 286 of the Securities and Futures Act and constituted as a unit trust (f) approved clearing houses; (g) recognised clearing houses which are incorporated in Singapore; (h) authorised benchmark administrators; (i) authorised benchmark submitters; (j) designated benchmark submitters; and (k) the Depository	Securities and Futures Act	Notice CMG-N02
2	All licensed financial advisers	Financial Advisers Act	Notice FAA-N18
3	All licensed insurers, other than captive insurers and marine mutual insurers	Insurance Act	Notice MAS 127
4	All registered insurance brokers	Insurance Act	Notice MAS 506
5	All banks in Singapore	Banking Act	Notice MAS 644
6	All credit card or charge card licensees in Singapore	Banking Act	Notice MAS 644A
7	All finance companies	Finance Companies Act	Notice MAS 830
8	All money brokers approved under section 28 of the Monetary Authority of Singapore Act	Monetary Authority of Singapore Act	Notice MAS 912
9	All merchant banks in Singapore	Banking Act	Notice MAS 1114
10	All operators and settlement institutions of designated payment systems	Payment Services Act 2019	Notice PSN05
11	All trust companies licensed under the Trust Companies Act	Trust Companies Act	Notice TCA-N05
12	All licensed credit bureaus	Credit Bureau Act 2016	Notice CBN02

Q2: Do "customer" and "customer information" have the same meaning as defined in Section 40A of the Banking Act?

A2: For the purpose of the Notice, the definitions of "customer" and "customer information" do not follow those in section 40A of the Banking Act. "Customer information" in the Notice refers to information held by the FI that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the FI.

Q3: Are FIs expected to submit their framework for the identification of critical systems and the list of critical systems to MAS for review and approval?

A3: FIs should establish and document a framework for the identification of critical systems. FIs should also document and maintain a list of critical systems, if any. Although MAS does not require FIs to submit said documentation for review and approval, MAS may request for them during its ongoing supervision.

Q4: Is it necessary for FIs to identify critical systems? Will FIs breach the Notice if they do not consider any of their systems as "critical"?

A4: Although not all FIs operate critical systems as defined in the Notice, all FIs are required to establish a framework and process to identify critical systems as defined in the Notice. It is possible that after an assessment, none of the FIs' systems falls within the definition of "critical system" in the Notice.

Q5: Could MAS provide some examples of "critical systems"?

A5: Examples of critical systems include Automated Teller Machine (ATM) systems, online banking systems, and systems which support payment, clearing or settlement functions.

Q6: What type of incidents or outages should be reported? Should an FI report the isolated outage of an Automated Teller Machine ("ATM"), a common occurrence typically managed as a normal operational event?

A6: Any IT security incident or system malfunction with severe and widespread impact on an FI's operations, or materially impacts the FI's service to its customers, is a reportable event. Isolated ATM outages that do not have a widespread impact on an FI's operations or materially impact services to customers are unlikely to be considered as reportable events.

Q7: Do FIs need to report a breakdown of a critical system or its components if the backup system or components have taken over the functions of the faulty system or components and there is no service or operation disruption?

A7: FIs do not need to report a system or component failure which has been recovered through a "high availability" configuration and does not affect the proper functioning of the system.

Q8: Are FIs expected to maintain a record of unscheduled downtime of their critical systems?

A8: An FI should record the unscheduled downtime for each critical system that affects the FI's operations or service to its customers as part of its system availability monitoring. MAS may request for such records during its ongoing supervision.

Q9: If an outage of a critical system did not have a severe and widespread impact on the operations of an FI or material impact to its customers, for example during off-peak hours, does it need to report the incident to MAS?

A9: An FI must notify MAS within 1 hour upon the discovery of a system malfunction or IT security incident which has severe and widespread impact on its operations or materially impact the FI's customers regardless of when the malfunction or incident occurs.

Q10: How is the total unscheduled downtime for a system calculated?

A10: Under the Notice, FIs shall ensure that the maximum downtime for each critical system does not exceed 4 hours within any period of 12 months. For example:

- FI recorded outage A of 3 hours in 1 July 2013,
- FI recorded outage B of 0.5 hours in 20 December 2013,
- Assuming there are no other incidents between 21 December 2013 and 30 June 2014, the total system downtime for the 12-mth period from July 2013 to June 2014, is 3.5 hours,
- Starting 1 July 2014, the total system downtime becomes 0.5 hours as outage A can only be accrued for 12 months; and
- If the FI encounters an outage C between July and December 2014, the total system downtime would be calculated as, "0.5 hours + outage C" until outage B expires on 19 December 2014.

Q11: How should FIs go about notifying MAS of an IT incident and via what channel?

A11: FIs should establish an internal reporting and escalation process to ensure that they report to MAS in a timely manner. FIs should contact their respective MAS Supervisory Officers (RO) during MAS office hours (Monday to Friday: 8.30am – 6.00pm). If the RO is not contactable, or the IT incident occurs outside MAS office hours, FIs may contact the MAS duty officer via the 24-hour MAS BCM hotlines (Tel: 97174201). Please refer to the Instructions on IT Incident Notification to MAS for further information.

Q12: FIs are required to notify MAS upon discovery of a Relevant Incident. What is MAS definition of "upon discovery"?

A12: FIs are required to notify MAS promptly after they have ascertained that the nature and magnitude of an IT incident meets the criteria set out in the Notice. FIs are expected to establish clear internal procedures for the swift detection and identification of Relevant Incidents.

Q13: We have performed a business impact analysis and determined that recovery time objective ("RTO") of 24 hours is sufficient for our critical systems. Would this be considered as a breach of the Notice?

A13: All systems that are identified as critical during the FI's risk assessment process should establish an RTO of not more than 4 hours. "Critical system" means a system, the failure of which will cause significant disruption to the operations of the FI or materially impact the customers of the FI, such as a system which processes transactions that are time critical; or provides essential services to customers. FIs are advised to identify systems as "critical systems" only if they meet the criteria in the Notice.

Q14: What does MAS mean when an incident needs to be reported within 1 hour upon discovery of a system malfunction? How is this different from the RTO of 4 hours?

A14: The RTO is defined as the duration of time from the point of disruption to the point of recovery. An FI is required to notify MAS not more than 1 hour from the point it discovered the system malfunction. For example, if an incident occurs at T, but FI only discovered it at T+1, then FI must report to MAS by T+2. However, the RTO starts counting from T and system must be recovered by T+4.

Q15: Do FIs need to send the RTO validation documentation to MAS after conducting a verification of the time taken to recover the critical system?

A15: MAS expects FIs to implement measures to ensure the reliability, availability and recoverability of their critical systems. FIs are required to test and validate the effectiveness of the recovery process once every 12 months. There is no requirement for FIs to send the documents to MAS after the test. FIs should document the test results including the time taken to recover critical systems against established RTOs. MAS may request for the relevant reports during its ongoing supervision.

Q16: Is a Distributed Denial of Service ("DDoS") attack where customer information was not compromised a reportable event to MAS?

A16: An FI must report the incident to MAS if the DDoS has severe and widespread impact on its operations or materially impacts the FI's service to its customers, even if no customer information was compromised.

Q17: FIs' networks are often subject to potential intrusions such as attempted hacking, DDoS, port and vulnerability scans. Should FIs report attempted but unsuccessful intrusions to MAS?

A17: There is no requirement for FIs to notify MAS of attempted intrusions as they do not fall within the scope of Relevant Incident under the Notice.

Q18: An FI experienced a virus or malware desktop infection on 50 of 1000 employee personal computers. Must the FI notify MAS of the incident?

A18: To determine if the IT security incident is a reportable event under the Notice, the FI must assess whether the security breach has a severe and widespread impact on its operations or materially impacts the FI's service to its customers.

Q19: An FI's employee was found to have performed an unauthorised access to its computer system but no major damage was done and customer information was not compromised. Must the FI notify MAS of the incident?

A19: An FI is not required to notify MAS of an IT security incident if it did not have a severe and widespread impact on the FI's operations or materially impact the FI's service to its customers.

Q20: Will MAS prescribe a template for root-cause and impact analysis report?

A20: The root-cause and impact analysis report should include an executive summary of the incident, detailed analysis and explanation on the cause of the incident, impact of the incident on the FI's compliance with regulations, operations and customers as well as remedial measures taken to address the incident consequences. A template is provided for root-cause and impact analysis report. Please refer to the Instructions on IT Incident Notification and Reporting to MAS for further information.

Q21: Would MAS extend the period for submitting a root-cause and impact analysis report if the FI cannot complete the incident report within 14 days?

A21: FIs have an interest to promptly investigate, identify and address the root cause of any Relevant Incident. Hence, based on past experience, the 14-day period should suffice for FIs to submit their reports on most types of incidents. However, the Notice allows FIs to request for an extension of the submission deadline. MAS will review, and may grant an extension of the submission deadline, based on the merit of each request.

Q22: Do FIs need to submit a separate incident report as part of business continuity management?

A22: FIs are only required to submit one report as per the template provided for incident reporting to MAS. Please refer to the Instructions on IT Incident Notification and Reporting to MAS for further information.