**Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines for Financial Institutions (FI’s) (including Banks) – Jan 2021 edition**

**7.7 Incident Management**

7.7.1 An IT incident occurs when there is an unexpected disruption to the delivery of IT services or a security breach of an IT system, which compromises the confidentiality, integrity and availability of data or the IT system. The FI should establish an incident management framework with the objective of restoring an affected IT service or system to a secure and stable state, as quickly as possible, so as to minimise impact to the FI’s business and customers.

7.7.2 The FI should ensure sufficient resources are available to facilitate and support incident response and recovery. The FI may engage external assistance to augment its resources to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber attack investigation, and provide 24 by 7 incident response capability.

* + 1. The incident management framework should minimally cover:

1. the process and procedure for handling IT incidents, including cyber related incidents;

Examples of cyber incidents include malware infection, social engineering, man-in-the-middle attack, denial of service attack, etc.

1. maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and

(c) the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents.

7.7.4 The FI should configure system events or alerts to provide an early indication of issues that may affect its IT systems’ performance and security. System events or alerts should be actively monitored so that prompt measures can be taken to address the issues early.

7.7.5 In some situations, a major incident may develop unfavorably into a crisis. The FI should regularly apprise its senior management of the status of major incidents so that decisions to mitigate the impact of the crisis can be made in a timely manner, such as activation of IT disaster recovery.

7.7.6 A communications plan that covers the process and procedures to apprise customers of impact on services, and to handle media or public queries should be maintained. The plan should also include identifying the spokespersons and subject matter experts to address the media or public queries as well as the communication channels to disseminate information.

7.7.7 It would be useful for the FI to provide timely updates to its customers on the progress of its incident management and the measures the FI is implementing to protect its customers and continue delivery of financial services. Where appropriate, the FI should advise its customers on actions that they should take to protect themselves.

**7.8 Problem Management**

7.8.1 The FI should establish problem management process and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.

7.8.2 The FI should maintain a record of past incidents which include lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.

7.8.3 A trend analysis of past incidents should be performed by the FI to identify commonalities and patterns in the incidents, and verify if the root causes to the problems had been properly identified and resolved. The FI should also use the analysis to determine if further corrective or preventive measures are necessary.

**8 IT Resilience**

**8.1 System Availability**

8.1.1 Maintaining system availability is crucial in achieving confidence and trust in the FI’s operational capabilities. IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs.

8.1.2 Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. The review should include a mapping of internal and external dependencies of the FI’s IT systems to determine any single point of failure. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.

8.1.3 The FI should continuously monitor the utilisation of its system resources against a set of pre-defined thresholds.13 Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs.

The monitoring of system resources could cover the utilisation of the computing processor, memory and data storage. For network resources, the monitoring indicators could cover network throughput, latency and packet loss.

8.1.4 Procedures should be established to respond to situations when pre-defined thresholds for system resources and system performance have been breached.

**The Association of Banks in Singapore, with support from the Monetary Authority of Singapore, has developed a set of cybersecurity guidelines to strengthen the cyber resilience of the sector**

Known as the Adversarial Attack Simulation Exercises (AASE) Guidelines or «Red Teaming» Guidelines, they provide financial institutions (FIs) with best practices and guidance on planning and conducting exercises to enhance their security testing.

AASE is a form of cybersecurity assessment designed to test the robustness of FIs’ cyber defences through a simulated cyber-attack using tactics, techniques and procedures that are commonly employed by threat actors, the [**Association of Banks in Singapore**](https://www.abs.org.sg/industry-guidelines/cyber-security) (ABS) said in a statement on Wednesday 14 November 2018.

**Simulating Realistic Attacks**

«We hope that the AASE guidelines will complement the FIs’ existing cybersecurity testing programmes and further strengthen their ability to assess the effectiveness of their cybersecurity measures to detect and respond to very sophisticated incidents,» **Ong-Ang Ai Boon**, Director of ABS, said.

By simulating realistic attacks during the exercise and taking into consideration the relevant threat landscape and potential adversaries, the following benefits can be achieved:

* An assessment of an FI’s cyber resilience against adversarial attack techniques, tactics and procedures
* Identification of weaknesses in security controls and associated risks not detected by standard vulnerability and security testing methodologies
* An assessment of the FI’s security incident management and/or crisis management response and processes
* A safe, controlled opportunity to identify and enhance the security posture of a FI whilst reducing risk of cyber breach or compromise
* An opportunity for the defensive teams, such as the security monitoring or incident response team to gain experience and be more proficient in detecting and responding to incidents.
* Improved confidence in formalising an informed post-activity short, medium and long-term security strategy.

**Modus Operandi**

«The AASE closely mimic the modus operandi of cyber criminals in targeting the actual operating environments of financial institutions. This makes it an effective way of assessing the cyber resilience of financial institutions,» **Tan Yeow Seng**, Chief Cyber Security Officer, MAS, said.

##