evvolabs™

ai • blockchain • cloud • cybersecurity • iot • media • mobility

INFORMATION SECURITY GUIDE FOR MAS TECHNOLOGY RISK MANAGEMENT

Authored by:

Jessica Tan – Technology Consultant

Kelly Chok – Marketing Lead

30.06.2022

evvolabs™

ai • blockchain • cloud • cybersecurity • iot • media • mobility

Table of Contents

Monetary Authority of Singapore (MAS) 4

The TRM Guidelines 4

Management of Third-Party Services 9

The TRM Notices 10

Why You Should Adopt TRM Guidelines and Notices 11

TRM Guidelines Checklist 11

Summary 12

How EVVO Labs Can Help You 13

evvolabs™

ai • blockchain • cloud • cybersecurity • iot • media • mobility

Monetary Authority of Singapore (MAS)

The Monetary Authority of Singapore (MAS) is the central bank of Singapore. It was established by the Monetary Authority of Singapore Act and gives it the authority to regulate the financial services sector in Singapore (Monetary Authority of Singapore Acts, 1999), which provides for the MAS to oversight and exercise control of all the financial operations performed by Singapore's financial institutions (FIs) and their related entities. The MAS also exercises powers under specific legislation directed at types of financial institutions and financial services providers, including the Banking Act, the Securities and Futures Act, the Financial Advisers Act, and the Insurance Act.

The TRM Guidelines

The Technology Risk Management (TRM) Guidelines are explanations of best practices that can be adopted by the Singapore FIs. The guidelines are meant to protect customer financial data, transactional data, and systems; as well as to strengthen system security and establish a robust technology risk management framework.

MAS initially issued the TRM Guidelines in June 2013 and published the updated version on the 18th of January 2021. MAS updated the guidelines to align with the digital transformation process within financial institutions and FinTech organisations. It aims to improve the cyber resilience of all FIs, especially with their capabilities to identify, protect, detect, respond, and recover from any cyberattacks. The updated guidelines represent significant changes including:

Below are the brief explanations of each clause in the TRM Guidelines:

1 The Role of Board of Directors and Senior Management in Oversight Technology Risks

Building a strong risk management framework that includes roles and responsibilities, information security rules, standards, and procedures is advised to the FI's Board of Directors and Senior Management. A plan for the People Selection Process is also included, with an emphasis on IT Security Awareness among the contractors, vendors, and employees of the FI.

2 Technology Risk Management Framework

The TRM standards place a strong emphasis on risk management as a key idea. MAS advises FIs to evaluate their compliance with the criteria using a risk-based approach. This section outlines the requirements for safeguarding the information system assets, risk identification, risk assessment, risk management, and risk monitoring and reporting.

3 Management of Third-Party Services

Advice on how to do background checks and due diligence on vendors and service providers. The guidelines place a strong emphasis on the operational risks that should be managed while outsourcing. It advises that FIs make sure service providers follow security procedures, rules, and controls that are at least as stringent as their own. In order to make sure their service providers uphold a high quality of diligence and care in protecting the confidentiality, integrity, and availability of their data and systems, the FIs must also perform routine reviews or assessments with them.

Below are the brief explanations of each clause in the TRM Guidelines:

4 Information System Acquisition and Development

This clause outlines all the best security practices that should be followed for system and application development. It emphasizes DevSecOps, Security by Design, and code standards. The list includes specific guidelines for end-user development, security requirements and testing, source code review, and IT project management.

5 IT Service Management

Explains the many service management frameworks that FIs can choose from and put into use. The framework's goal is to guarantee that the FIs have the necessary tools and resources to support IT services and operations. Some of the subjects covered are change management, program migration, problem management, capacity management, and incident management.

6 System Availability, Recoverability, and Reliability

For high system availability, the suggestions for backup procedures are provided in this section. The MAS examines flaws in the current design and recommends all FIs to evaluate the architecture of their IT systems and networks on a regular basis. Guidelines to follow include system availability, disaster recovery planning, disaster recovery testing, and data backup management.

Below are the brief explanations of each clause in the TRM Guidelines:

7 Operational Infrastructure Security Management

This section contains information on how to safeguard systems and data in detail. In this section, various rules are underlined, including:

- Data Loss Prevention (DLP)
- Technology Refresh Management
- Networks and Security Configuration Management
- Vulnerability Assessment (VA) and Penetration Testing (PT)
- Patch Management
- Security Monitoring.

8 Data Centres Protection and Controls

This section includes a list of advice on data center security. FIs should set up precautions to protect their Data Center from physical and environmental hazards, according to MAS. They are Physical Security, Threat and Vulnerability Risk Assessment (TVRA), and Data Center Resiliency.

9 Access Control

User access management and privileged access management are part of the access management policies. To update, modify, and revoke access permissions to information assets, the FIs should create a user management process. Access permissions should be authorized and approved by the appropriate parties, such as the owner of the information asset.

Below are the brief explanations of each clause in the TRM Guidelines:

10 Online Financial Services

The requirements for offering online financial services, including those provided by banks, insurance companies, and trading platforms. To maintain the security of data and online services, MAS advises this category of FIs to put in place suitable security and control measures. This section includes information on the security of online systems, mobile online services, and payments.

11 Payment Card Security (ATMs, Credit, and Debit Cards)

Security recommendations are provided in this section for payment card fraud, ATMs, and payment kiosks. According to MAS, financial institutions should inform their clients on security best practices, recent cyber threat warnings, how to spot illegal transactions, and how to report any suspicious frauds.

12 IT Audit

The planning and tracking guidelines for audits are provided in this section. In order to give the FI's Board of Directors and Senior Management an unbiased and impartial evaluation of the FI's governance, risk management, and controls' sufficiency and effectiveness.

Management of Third-Party Services

Under clause 3.4 on Management of Third-Party Services, MAS has specified the following conditions when FIs wish to engage any service providers for outsourcing purposes:

1. Before entering into a contractual partnership or outsourcing agreement, FIs are required to carry out due diligence or background checks to assess the service providers. This evaluation must take into account the service provider's physical and IT security controls, financial stability, business reputation, and capacity to fulfill the agreement's service obligations. In the Management of Third-Party Services, additional controls are also specified, such as hiring procedures and liability insurance.

2. FIs have the right to write all Terms and Conditions about engaging their service providers. Internal or external auditors, representatives designated by the institution, or the FIs themselves may carry out routine audits and compliance inspections.

The TRM Notices

MAS published TRM Notices, which provide further specific instructions in addition to the TRM Guidelines, as below:

- FIs to develop and define a framework for identifying critical systems.
- FIs to implement IT controls to protect customer information from unauthorized access or disclosure.
- FIs must take steps to ensure that their critical systems are reliable, available, and recoverable, for example, banks shall ensure that these critical systems do not have a total downtime of more than 4 hours in any 12-month period.
- FIs to establish a 4-hour Recovery Time Objective (RTO) for each critical system. In addition, FIs shall validate and document system recovery testing and check if the 4-hour RTO is validated.
- FIs required to notify MAS of a “relevant incident”, e.g., system malfunction or IT security incident, within 1-hour of discovery of the incident.
- FIs shall submit a root-cause and impact analysis report to MAS within 14 days of the relevant incident occurring using MAS’ Incident Reporting Template.

Why You Should Adopt TRM Guidelines and Notices

Loss of Reputation

There are no penalties for breaking the TRM Guidelines because they are not mandated by law. However how closely the TRM Guidelines are adhered to will impact how the MAS evaluates the institution's risk. The fact that these TRM Guidelines cover a wide range of operational and technological risk management issues means that adhering to them will help FIs keep their reputation as reliable financial institutions.

Regulatory Consequences on TRM Notices

Unlike TRM Guidelines, the TRM Notices are enforceable in court. Financial penalties and the loss of an operating permit in Singapore may follow FIs' violations of the Notices.

Notification of noncompliance to regulators

The FI may ask to take extra measures to correct the deficiencies if MAS is not satisfied with the FI's compliance with the TRM Guidelines. For instance, if the FI does not follow the Third-Party Management provision, MAS may notify the FI's home or host regulators, as well as the service provider, of their capacity and readiness to work with MAS in regulating the outsourcing risks to the institution.

TRM Guidelines Checklist

MAS published a TRM Checklist to guide all Singapore FIs in their compliance journey and efforts. The checklist document is a comprehensive catalogue, which includes over two hundred items covering many attack vectors related to security threats. While the checklist can assist FIs to establish a multi-layered security strategy to protect their assets and systems, the volume and depth of the requirements may be considered overwhelming to most FIs. Many checklist items are difficult to achieve without the usage of proper security tools and solutions due to the sophisticated nature of the security threats.

Summary

The Monetary Authority of Singapore has established a comprehensive set of IT and security requirements to assist financial institutions in protecting data, managing risk, and safeguarding their reputations as part of its continuous role in monitoring the country's financial industry. Furthermore, broad compliance with the MAS TRM guidelines and notices is supporting Singapore's financial and fintech industry, and the country's key position in the global financial community.

The Monetary Authority of Singapore has continuously improved its efforts in promoting a sound and progressive financial services sector. This is also to ensure the success and resilience of the Singapore economy.

How EVVO Can Help You

At Evvo Labs, we help and guide organisations to meet or exceed key TRM requirements. We understand how important it is for FIs to protect their customers while also maintaining a good reputation. Hence, our consultant will support you in understanding compliance rules and implementing security best practices within your organisation.

We have worked with a variety of FIs, each with its own set of objectives and challenges in implementing the TRM Guidelines. We can help FIs to take effective steps to maintain confidentiality, integrity, and availability of their information assets. This is our approach:

Our Approach

Scoping

To identify business objectives and high-level priorities, as well as to define cybersecurity implementation scope.

Current Security Posture

To determine the current security posture of the organisation.

Risk Assessment

To identify threats and vulnerabilities that existed in the organisation and determine the likelihood and impact of cybersecurity risks.

Gap Analysis

To determine the target security posture and analyse the gap between current vs. target security posture.

Prioritise Action Plan

To address the gaps and implement security controls to achieve the desired cybersecurity outcomes.

Appendix:
https://www.mas.gov.sg/regulation/acts/mas-act
https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/FAQs_Notice-on-TRM-Jan-22.pdf

evvolabs™
ai • blockchain • cloud • cybersecurity • iot • media • mobility

www.evvolabs.com