White Paper

IT Security Guidance for Monetary Authority of Singapore

avanade

Monetary Authority of Singapore (MAS)

What is it?
The Monetary Authority of Singapore (MAS) is the central bank of Singapore. The MAS was established by the Monetary Authority of Singapore Act. This Act provides for the MAS to exercise control over financial institutions and their related entities, and empowers it to issue legal instruments for such regulation and supervision. The MAS also exercises powers under specific legislation directed at particular types of financial institution and financial services provider, including the Banking Act, the Insurance Act, the Securities and Futures Act and the Financial Advisers Act.[1]

Why does this matter?
As MAS is the central bank of Singapore, it has regulatory oversight of all the financial operations performed by financial institutions (FIs) within Singapore.

The TRM Guidelines

Issued by MAS who has operational and regulatory oversight over the FIs, the Technology Risk Management (TRM) Guidelines are statements of best practices that are expected of the FIs. The TRM Guidelines are to protect the customer financial data, transactional data, and systems, to strengthen system security and to establish a sound and robust technology risk management framework.[2]

Guidelines	Brief Synopsis
1. Oversight of Technology Risks by Board of Directors and Senior Management	Recommendation to the board and senior management of the FI to establish sound risk management framework including roles and responsibilities, IT policies, standards and procedures. It also includes a recommendation on People Selection Process with a focus on IT Security Awareness within the staff, vendors, and contractors of the FI.
2. Technology Risk Management Framework	Lays out the guidelines on how to protect the information system assets, risk identification, risk assessment, risk treatment and tisk monitoring and reporting.
3. Management of IT Outsourcing Risks	Advice to the FI on how to perform due diligence on service providers (vendors). This guideline highlights the risks of outsourcing particularly operational risks. It advises the FIs to ensure that service providers implement security policies, procedures and controls at least as stringent as it would expect for its own operations. This guideline also advises that the FI to carry out reviews or assessments for regulatory, audit or compliance purposes.
4. Acquisition and Development of Information Systems	This guideline lists out all the secure practices expected when developing applications. The list includes detailed guidelines for IT project management, security requirements and testing, source code review and end user development.
5. IT Service Management	Details different types of service management frameworks that the FIs need to adopt. They include change management, program migration, incident management, problem management and capacity management.
6. System Reliability, Availability and Recoverability	This section has recommendations for what contingency procedures need to be considered for high systems availability. Guidelines include systems availability, disaster recovery plan, disaster recovery testing and data backup management.
7. Operational Infrastructure Security Management	In this section, the details of how to protect data and systems are listed. Data Loss Prevention (DLP), Technology Refresh Management, Networks and Security Configuration Management, Vulnerability Assessment (VA) and Penetration Testing (PT), Patch Management and Security Monitoring are the highlighted guidelines in this section.
8. Data Centres Protection and Controls	As the name suggests, this section has a list of guidelines to protect the Data Centres. MAS has listed them as Threat and Vulnerability Risk Assessment (TVRA), Physical Security and Data Centre Resiliency.
9. Access Control	Details the access management guidelines including user access management and privileged access management.
10. Online Financial Services	As most of the financial transactions are conducted online, MAS has listed the guidelines under this section. Subsections include Online Systems Security and Mobile Online Services, and Payments Security.
11. Payment Card Security (ATMs, Credit and Debit Cards)	Guidelines for payment card fraud and ATMs and payment kiosks security are listed under this section.
12. IT Audit	Audit planning and remediation tracking guidelines are detailed in this section.

The Guidelines on Outsourcing

In the Guidelines on Outsourcing MAS has clarified the following conditions when outsourcing to any service provider (like Avanade):

1. To employ due diligence in evaluating the service provider's physical and IT security controls, business reputation and financial strength, ethical and professional standards held and the service provider's ability to meet service obligations under the outsourcing agreement.[3] Additional checks including recruitment practices, insurance held for liability etc. are also listed in the Guidelines on Outsourcing.
2. For the FI to reserve the right to detail in writing all conditions about outsourcing. These conditions may be subject to regular audits and compliance checks either by the FIs, internal or external auditors or by agents appointed by the institution.

The TRM Notices

In the TRM Notices, further specific instructions have been provided as below:

1. To put in place a framework and process to identify critical systems.
2. To make all reasonable effort to maintain high availability of the critical systems. The bank shall ensure that these critical systems do not have a total downtime of more than 4 hours in any 12-month period.
3. To establish a 4-hour Recovery Time Objective (RTO) for each critical system. Further, the bank should validate and document system recovery testing and check if the 4-hour RTO is validated.
4. The bank should notify MAS of a 'relevant' incident (system malfunction or IT security incident) within 1 hour of discovery of the incident.
5. To submit a Root Cause Analysis (RCA) and impact analysis report to MAS within 14 days of the relevant incident occurring. The prescribed format for the report has been published.
6. To implement IT controls to protect customer information from unauthorised access or disclosure.

Why You Want to Follow Them

Loss of Reputation
The TRM Guidelines are not legally binding and non-compliance does not attract any kind of penalties. However, the extent of the following of the TRM Guidelines will affect the MAS' risk assessment of the institution. As these general-purpose guidelines cover large aspects of the operational and technology risks, following these TRM Guidelines will help the FIs in conserving their reputation as a sound financial organisation.

Notification to Regulators about non-compliance
Where MAS is not satisfied with the FI's observance of the Guidelines on Outsourcing, they may require the FI to take additional measures to address the deficiencies. MAS may also notify the home or host regulators of the FI and the service provider on their ability and willingness to cooperate with MAS in supervising the outsourcing risks to the institution.[4]

Regulatory Consequences
The TRM Notices have legal force, and violation of the TRM Notices can result in financial penalties and revocation of license to operate in Singapore.

How Avanade Helps You Meet the MAS Guidelines and Requirements

Avanade understands financial services clients are deeply committed to both protecting their customers and maintaining a trusted reputation in the marketplace. With in-depth knowledge of compliance rules and deep experience with protecting information, Avanade helps organizations utilize robust technology solutions to enhance business operations, while also navigating the complex security guidelines and requirements put in place by MAS.

Working with a variety of FIs, each with its own set of objectives and challenges, Avanade has created a broad library of data security best practices that form its **Client Data Protection (CDP) program**. Avanade assigns every engagement to the CDP and, in helping an FI protect its sensitive and personal data, uses a prevention-focused methodology built on the following foundational principles:

- **Senior-level oversight** responsibility for all engagements where client data is accessible
- **Clear communication and documentation** of all CDP requirements
- **Required controls** for secure handling of client data while in Avanade's custody
- **Service-specific controls** tied to vulnerabilities inherent to unique types of work, such as the needs of financial services clients
- **Technology controls** deployed to enforce mandatory baseline protection mechanisms
- **Tools, processes and subject matter specialist support** for project teams
- **Standardized data protection** tools and templates

Program execution begins with a risk assessment to determine each client's risk in relation to their precise project requirements. The second mitigation phase uses an implementation plan consisting of up to 24 control families operated by the project team.

Avanade requires that a CDP plan be established before any delivery tasks begin, and everyone working on behalf of the client engagement must adhere to the plan for the life of the engagement. Plan execution is periodically reviewed by independent internal teams to gauge both compliance and the effectiveness of the controls to manage the client's risk. Any identified gaps are tracked and escalated to the assigned Client Data Protection Executive (CDPE) for corrective action.

Avanade's knowledge of financial services regulations around the world – and its experience helping clients protect their systems and information – have enabled the company to develop effective approaches to security. Avanade knows, however, that every client is different, and each has its own set of requirements and challenges. That is why Avanade makes sure it understands these elements during the assessment process so that the company can develop and put in place the right security controls to fit a client's individual needs. Moreover, Avanade continues to reassess those needs throughout delivery, ensuring that the company provides services that its clients can count on to help keep data safe and systems protected.

Avanade's Business Continuity Management

Avanade will work the FI to first identify critical systems and then to provide a resilient architecture with Disaster recovery RTO of 4 hours. With our Platinum+ design option, we can provide a hot site business continuity management solution to have an active/active design so that we can achieve the required 4-hour RTO time frame.

Avanade's Reporting of Critical Incidents

Avanade Asset Protection (AAP) team tracks resolves all incidents including security incidents. Our process currently involves reporting to our leadership team about critical incidents. One part of the process also involves notifying of any authorities of any incidents that are critical in nature. While Avanade does not have a 1-hour time frame of reporting currently. The AAP team is working towards a framework for reporting of breaches to the relevant authorities within the suggested timeframes of various regulatory authorities.

Summary

Takeaways
The Monetary Authority of Singapore, as part of its ongoing responsibility for overseeing the country's financial industry, has put in place a comprehensive listing of IT and security standards, which help financial institutions protect data, manage risk, and safeguard their reputations. Moreover, widespread adherence to the MAS guidelines and requirements helps protect Singapore's financial industry and the significant role the country plays in the global financial community.

Avanade can help FIs take effective steps to protect privacy, keep data secure, and quickly detect and report incidents. The company's CDP program is a proven approach to assessing risk, implementing security controls, and providing ongoing services and support. Moreover, with its deep experience helping financial services companies around the world manage and secure data, Avanade can help FIs implement controls that support their business objectives while keeping their IT operations protected and in adherence to the MAS guidelines and requirements.

About Avanade
Avanade is the leading provider of innovative digital services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Our 29,000 professionals across 20 countries combine technology, business and industry expertise to build and deploy solutions to realize results for clients and their customers. Visit us at www.avanade.com

Disclaimer
The contents in this document are intended to convey general information only and not to provide legal advice or opinions. You should contact your attorney to obtain advice on specific legal issues.

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Africa
Pretoria
Phone +27 12 622 4400
SouthAfrica@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
Asia-Pacific@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

[1] http://www.mas.gov.sg/
[2] Section 1.0.4, Technology Risk Management Guidelines, issued by the MAS on 21 June 2013
[3] Section 5.4.2, Guidelines on Outsourcing, issued by the MAS on 27 July 2016
[4] Section 4.1.2, Guidelines on Outsourcing, issued by the MAS on 27 July 2016