MAS Technology Risk Management Guidelines

The Monetary Authority of Singapore ("MAS") issued a revised Technology Risk Management Guidelines ("Guidelines") on 18 January 2021.

The MAS shared that the revised Guidelines focus on addressing technology and cyber risks by financial institutions (FIs) with the growing use of cloud technologies, application programming interfaces, and rapid software development. It reinforces the importance of incorporating security controls as part of FIs technology development and delivery lifecycle and the deployment of emerging technologies.

The MAS also highlighted the growing reliance of FIs on third-party service providers on technology solutions and development. MAS expects FIs will assess and manage their exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data before entering into a contractual agreement or partnership. FIs are expected to employ a high standard of care and diligence in protecting data confidentiality and integrity and ensure system resilience.

The revised Guidelines include feedback received by the MAS from the Consultation Paper on the proposed revisions to the MAS Technology Risk Management Guidelines on 7 March 2019. It sets out the technology risk management principles and best practices for FIs to:

a. Establish Sound and Robust Technology Risk Governance and Oversight
b. Maintain Cyber Resilience

The purpose of the Guidelines is to promote the **adoption of sound** and **robust practices** for the management of technology risk. The extent and degree to which FIs implement the Guidelines should commensurate with the level of risk and complexity of the financial services offered and the technology supporting such services.

Key Takeaways:

a. Establish a sound and robust Technology Governance and Oversight

i. Role of the Board of Director and Senior Management

- Establish effective internal controls & risk management practices
- Senior Management / Board should have members with knowledge to understand and manage technology risks
- Appoint CTO / IT Head or its equivalent with relevant experience and qualification
- Senior Management / Board ensure that TRM strategy is established & implemented
- Ensure IT decisions are made within the FIs risk appetite
- Cultivate tone from the top and strong culture of technology risk awareness within the FI
- Ensure sound and robust risk management framework and function are in place
- Board should ensure that senior management is given sufficient authority, resources
- Approve the risk appetite and tolerance statement that establish the nature and extent of technology risk the FIs are willing and able to assume
- Establish regular reviews, management competencies assessment and independent audit function to assess the effectiveness of controls, risk management and governance

ii. Policies, Standards and Procedure

- Establish policies and procedures, incorporating industry standards and best practices to manage technology risks and safeguard information assets
- Any deviations should be thoroughly reviewed and assessed
- Compliance processes should be implemented to verify that the policies, standards and procedures are adhered to

iii. Management of Information Assets

- Identification of information assets
- Classification of information based on its criticality
- Roles and responsibility of staff managing the information assets
- Policies, standards and procedure to manage the information assets

iv. Management of Third Party Services

- Perform an assessment to establish if the service is considered outsourced and the impact on operations if there is a system breach with the outsourced vendor holding confidential and sensitive customer information
- Assess and manage technology risk exposure by the IT system and data of the third party
- Ensure high standard are maintained on an ongoing basis

v. Competency and Background Review

- Competency and experience of service providers and contractors
- Background checks on the staff, contractors and service providers who have access to confidential data and critical IT systems to minimize the risk

vi. Security Awareness and Training

- Establish an IT security awareness and training program
- Recommended to conduct at least annually
- Content of training should be reviewed and updated periodically

b. Technology Risk Management Framework

Risk Management Framework

- Established a framework to manage technology risk
- Establish effective internal controls and risk management practices
- Identify risk owner (individual / group) who is accountable for proper risk treatment and implementation
- Framework should: **identify** risk, **assess** risk, risk **treatment** and risk **monitoring**
- Framework should be reviewed regularly

* Risk Identification

- Clear identification of threats and vulnerabilities
- Information assets maintained and supported by third-party service providers

* Risk Assessment

- Analyze potential threats and vulnerabilities impact and consequences (financial, reputational, operational, legal and regulatory)

* Risk Treatment

- Develop and implement risk mitigation and control measures
- Documentation of acceptance of residual risk that cannot be fully eliminated

* Risk Monitoring, Review and Reporting

- Process of assessing and monitoring effective IT controls
- Maintainance of risk register
- Develop technology risk metrics to facilitate risk reporting to management

c. Roles and responsibilities of Board and Senior Management Assessment of vendors (Technology)

Factors to consider

- Quality assurance practice, security practices in place to safeguard the sensitive data, access to FIs system should be controlled and monitored

d. Assessment of third parties' suitability in connection to the FIs Application Programming Interface (API)

Factors to consider

- Vendors' nature of business, cyber security posture, reputation, and track records

e. Cyber Threat Monitoring and Information Sharing

Factors to consider

- Analyze cyber related incidents to the relevance and potential impact on FI's business and IT environment

f. Cyber Incident Response and Management

Factors to consider

- Swift isolation & neutralise cyber threat
- Communicate, coordinate and response

g. Cyber Security Assessment

Factors to consider

- Vulnerability Assessment (VA) and Penetration Testing (PT)

h. Simulation of Cyber attacks tactics, techniques and procedure

i. IT Audit

RHT Compliance Solutions

RHT Compliance Solutions is a premier Compliance Service Advisory firm based in Singapore.

Our team comprises experienced and certified professionals with extensive regulatory, compliance and risk management experience from Singapore, Indonesia, Hong Kong and the broader region. The team is well equipped to provide clients with intelligent, risk-focused and cost-effective solutions.

RHT Group of Companies is an integrated ecosystem offering consultancy and fintech advisory services. When you engage us, you can be assured of a one-stop seamless service and multi-dimensional advisory afforded by our network of companies, backed by a team of capable leaders and effective individuals with expert knowledge. We are equipped to serve you at every stage of your business.

Reach out to us:

Jayaprakash Jagateesan
Executive Director and CEO
RHT Compliance Solutions
prakash.j@rhtgoc.com

Tony Yeow
Associate Director
tony.yeow@rhtgoc.com

RHT Compliance Solutions
1 Paya Lebar Link #06-08
PLQ 2 Paya Lebar Quarter
Singapore 408533
cs@rhtgoc.com

Visit us Follow us