Revisions to guidelines on technology risk management

January 2021

Overview of the revisions to technology risk management guidelines

On 18 January 2021, the Monetary Authority of Singapore (MAS) released the revised technology risk management (TRM) guidelines, an update from the 2013 guidelines. Cyber security assessment and cyber surveillance and security operations are **two new sections** that have been introduced. F**ive sections have undergone significant revisions** and, **three new annexes have been added** focusing on application security testing and device security (BYOD and mobile application security).

Key revisions to the TRM guidelines

MAS has updated the TRM guidelines with the following new and enhanced requirements:

1. **Technology risk governance and oversight** which articulates the need for members of board and senior management to have necessary **skills and understanding of technology risks,** having distinct roles & responsibilities, with an emphasis on a sound and robust technology risk management framework through effective information asset management and third party services management:
    - **Roles & responsibilities** – Board of directors to appoint certain technology related roles e.g. CIO, CISO to establish a risk management strategy, set a suitable risk appetite etc. Board of directors to ensure an independent audit function to assess the effectiveness of controls, risk management and governance within the Financial Institution (FI).
    - **Management of information assets** – Scope of information assets includes assets entrusted to the FI, rented or leased by the FI, assets used by service providers to deliver their services to the FI, as well as requirements to maintain an **inventory of all its information assets**.
    - **Management of third party services** – Conduct an assessment of service providers' **exposure to various technology risks** associated with the loss of data confidentiality, integrity and service availability, manage the associated risks, as well as appropriate due diligence.

https://www.pwc.com/sg/en/risk-assurance/technology-risk-management.html

   - **Risk management framework** – Perform scenario-based risk assessment, identify a **risk owner** accountable for ensuring proper risk treatment measures are implemented and enforced. Criteria for acceptance of residual risks should be clearly defined and should commensurate with the FI’s risk tolerance.

2. **IT project management and security-by-design** – Establish standards and procedures for vendor evaluation and selection, monitor vendors’ controls, implement safeguards and put in place source code escrow agreement in the event that the vendor is unable to support the FI. Establish a **framework to manage its system development life cycle (SDLC)** based on the **security-by-design principles**. **Quality assurance** performed by an independent quality assurance function to assess whether project activities and deliverables comply with the FI’s policies, procedures and standards.

3. **Software development and management** which advocates the adoption of secure software development best practices in relation to:
   - **Agile** – Incorporate **secure coding, code review and application security testing** when using Agile framework.
   - **DevSecOps** – Align DevSecOps activities and processes with its SDLC framework and IT service management processes including enforcement of **segregation of duties** in key DevSecOps practices**.**
   - **APIs** – Establish adequate **safeguards to manage the development and provision of APIs** for secure delivery of such services. Build capability to monitor the usage of APIs and measures to handle high volumes of API call requests by legitimate applications and mitigate denial-of-service attacks should be implemented based on criticality and availability requirements of the applications.

4. **Access management** – Access controls for users performing **remote access connection** to include strong authentication, such as **multi-factor authentication**. Remote access to information assets is only allowed for devices that are **secured** to FI’s security standards.

5. **Management of operational infrastructure security risks** arising from emerging technologies such as Internet of Things (IoT) and virtualisation, as follows:
   - **IoT** – Maintain an **inventory of all its IoT devices** (e.g. smart phones, multi-function printers, security cameras and smart televisions), the networks which they are connected to and their physical locations. Implement processes and controls to mitigate risks arising from IoT, including securing networks that host IoT devices using strong authentication and network access controls.
   - **Virtualisation** – Implement all components of a virtualisation solution, virtual machines images and snapshots with the **same level of security and resilience as a non-virtualised IT environment**.

6. **Defence-in-depth approach to strengthen cyber resilience** which includes **collecting, processing and analysing cyber-related information** for its relevance and potential impact to the FI's business and IT environment. Additionally, carrying out regular **scenario-based cyber exercises**, and performing an **adversarial attack simulation exercise**. The new guidelines set guidance on:
   - **Cyber threat intelligence and information sharing** – Procure cyber intelligence monitoring services and using cyber threat intelligence to facilitate its risk assessment on prevailing cyber threats.
   - **Cyber event monitoring and security operations** – Implement monitoring and surveillance system to detect suspicious and malicious system activity. Consider implementing **real-time monitoring** and facilitate the analysis and correlation of cyber events and **user behavioural analytics** to enhance the effectiveness of security monitoring. Consider **establishing a security operations centre** with cyber surveillance and incident response capability to achieve continuous monitoring and analysis of cyber events.
   - **Cyber security assessment and testing** – Carry out vulnerability assessment on their systems and **penetration testing** (a combination of blackbox and greybox testing) for online financial services, **in the production environment** to obtain a more accurate assessment of the robustness of the FI's security measures.
   - **Cyber incident management** – Establish a cyber incident response and management plan to **swiftly detect, respond to and limit consequences** of a cyber incident. The plan should describe procedures to respond to plausible cyber threat scenarios, be reviewed, updated and tested at least annually.
   - **Cyber exercises** – Carry out regular **scenario-based cyber exercises** (such as **social engineering, table-top, or cyber range**) to validate and review its response and recovery. Perform an **adversarial attack simulation exercise** to test and validate the effectiveness of its cyber defence and response plan against prevalent cyber threats.

Next steps

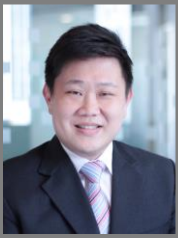
FIs should consider:

- Assessing their ability to meet the new requirements from the TRM guidelines.
- Determining key actions that commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services to adhere to the new requirements.
- Where technology services are outsourced (to intra-group entities or other third party service providers), assessing their ability to meet the new TRM requirements.

Contact us

Tan Shong Ye
Digital Trust Leader
shong.ye.tan@pwc.com

Kyra Mattar
Digital Trust, Financial Services
kyra.mattar@pwc.com



Jimmy Sng
Digital Trust, Cyber Security
jimmy.sng@pwc.com

If you would like to kickstart conversations on the requirements, do leave your details here.

If you have any enquiries, feel free to reach out to sg_risk_assurance@pwc.com

https://www.pwc.com/sg/en/risk-assurance/technology-risk-management.html

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.