

Technology, Media and Telecommunications, Financial Institutions, Funds and Investment Management

2021 Technology Risk Management Guidelines: Enhanced Requirements on Financial Institutions Concerning Technology Risk Governance and Security Controls

Introduction

The revised [Technology Risk Management Guidelines](#) ("**2021 TRM Guidelines**") published on 18 January 2021 by the Monetary Authority of Singapore ("**MAS**") impose additional and/or more stringent requirements on financial institutions ("**FIs**"), their boards of directors ("**Boards**") and senior management concerning technology risk governance and security controls in FIs. The revisions focus on the following key areas: (i) increased responsibilities of the Boards and senior management of FIs concerning technology risk governance and oversight; (ii) secure software development practices; (iii) managing risks from emerging technologies; and (iv) an enhanced focus on cyber resilience.

The 2021 TRM Guidelines is effective from **18 January 2021** and apply to all FIs, including banks licensed under the Banking Act (Chapter 19), payment services licensees under the Payment Services Act 2019, capital markets intermediaries regulated under the Securities and Futures Act (Chapter 289), as well as insurers licensed or regulated under the Insurance Act (Chapter 142).

These revisions follow the [public consultation](#) conducted in 2019 where MAS proposed revisions to the TRM Guidelines published in 2013 ("**2013 TRM Guidelines**") to keep pace with the changing cyber threat landscape. MAS also issued its [response](#) to the consultation on 18 January 2021.

This Update provides a summary of the key areas of revisions in the 2021 TRM Guidelines, along with suggested action items for FIs' consideration to facilitate compliance with the 2021 TRM Guidelines.

Enhanced Requirements on FIs, their Boards and Senior Management Regarding Technology Risk Governance/Oversight

To ensure that the FI's Board and senior management can exercise effective oversight over the FI's technology strategy, operations, and risks, the 2021 TRM Guidelines provide additional guidance in this regard, including:

Technology, Media and Telecommunications, Financial Institutions, Funds & Investment Management

- The Board and senior management of FIs must include members with knowledge of technology and cyber risks, including risks from cyber threats.
- The Board and senior management should ensure that the Chief Information Officer, Chief Technology Officer or Head of IT, and Chief Information Security Officer or Head of Information Security (or similar senior manager roles that have oversight and management of technology risks, including cyber risks) who are appointed have requisite experience and expertise. At the minimum, such appointments must be approved by the Chief Executive Officer.
- Compared to the 2013 TRM Guidelines, the 2021 TRM Guidelines detail an expanded list of responsibilities for the Board (or a committee delegated by it) and senior management. For instance, the Board is required, among other things, to: (i) assess management competencies for managing technology risks; and (ii) ensure that an independent audit function is established to assess the effectiveness of controls, risk management, and governance of the FI. The senior management is responsible, among other things, for (i) ensuring the roles and responsibilities of staff in managing technology risks are clearly delineated and; (ii) apprising the Board of salient and adverse technology risk developments and incidents that are likely to have a major impact on the FI in a timely manner.

The reliance on the board of directors and senior management of FIs to ensure effective internal controls and risk framework to achieve security, reliability, and resilience of the IT operating environment is a consistent theme under the broader culture and conduct focus to promote behaviour and culture that is conducive to meet the regulatory expectations of these guidelines through the tone from the top.

Evaluation of Third Party Vendors

Compared to the 2013 TRM Guidelines, the 2021 TRM Guidelines provide more detailed guidance on the level of assessment by the FI of third party vendors and entities with access to the FI's IT systems. For instance, under the 2021 TRM Guidelines, FIs should establish standards and procedures for the evaluation and selection of vendors, such as conducting detailed analysis of the vendor's software development and assessing the vendor's security practices.

The level of an FI's assessment and due diligence of the vendor should be proportionate to the criticality of the project deliverables. This is to ensure that the selected vendor is qualified and capable of meeting the project requirements and deliverables.

Technology, Media and Telecommunications, Financial Institutions, Funds & Investment Management

Additional Guidance on Managing Risks Concerning Application Programming Interfaces ("APIs"), Agile Software Development and DevSecOps; Data and Infrastructure Security

The 2021 TRM Guidelines emphasise the adoption of secure software development best practices and include additional guidance to manage risks from emerging technologies. These include additional guidance concerning:

- **Securing APIs.** APIs enable various software applications to communicate and interact with each other and exchange data. The 2021 TRM Guidelines provide guidance on safeguards to deal with concerns of open APIs that are used by third parties to implement products and services for customers and the marketplace. For instance, FIs must have a well-defined security process to assess and govern third party API access. Before allowing third parties to connect to the FI's IT system, the FI must perform a risk assessment and ensure that the implementation of each API is commensurate with the sensitivity and business criticality of the data being exchanged, among other things.

In addition, FIs must establish security standards for designing and developing secure APIs and adopt strong encryption standards and key management controls to secure transmission of sensitive data through APIs. Before deploying the API, the FI must conduct a robust security screening and testing of the API between the FI and its third parties. The FI must also conduct real-time monitoring of suspicious activities and establish remedial measures to revoke the API keys or access token in the event of a breach.

- **Security testing for Agile software development.** Agile software development is based on an iterative and incremental development model to accelerate software development and delivery to accommodate business and customer needs. When adopting Agile software development methods, an FI should incorporate the necessary security practices throughout its Agile process to ensure the security of the application is not compromised, such as secure coding and source code review.
- **Recommended best practices for DevSecOps.** DevSecOps involves automating and integrating IT operations and quality assurance into the software development process to enable frequent, efficient, and reliable releases of software products. To manage associated risks, the FI must ensure its DevSecOps activities and processes are aligned with its software development life cycle ("**SDLC**") framework and IT service management processes, for instance configuration management, change management, software release management. The FI should also enforce segregation of duties for the development, testing, and operations functions in its DevSecOps processes, and ensure the respective DevOps activities are logged and reviewed in a timely manner.

Technology, Media and Telecommunications, Financial Institutions, Funds & Investment Management

The 2021 TRM Guidelines also provide further guidance for FIs concerning data and infrastructure security, such as:

- **Safeguarding against risks arising from virtualisation.** Virtualisation is employed to optimise the use of computing resources and to enhance resilience. The 2021 TRM Guidelines provide additional guidance on virtualisation security. For instance, FIs must ensure all components of a virtualisation solution have the same level of security and resilience as a non-virtualised IT environment. This includes implementing strong access controls to restrict administrative access to the hypervisor and host operating system, as well as establishing policies and standards to manage virtual machines images and snapshots.
- **Mitigating risks arising from Internet of Things ("IoT").** IoT includes any electronic devices, such as smart phones and multi-function printers which are connected to the FI's network or the Internet. FIs should maintain an inventory of all its IoT devices, the networks which they are connected to, and their physical locations. Also, FIs should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with the function and criticality of the data that is collected, stored, and processed by the IoT devices.

Strengthening Cyber Resilience with Enhanced Risk Mitigation Strategies

To sustain confidence in financial services amid more frequent cyber incidents, the 2021 TRM Guidelines provide a defence-in-depth approach to strengthening cyber resilience. Among other things, the 2021 TRM Guidelines provide further guidance to FIs on mitigating risks from cyber threats in the following areas:

- **Cyber threat monitoring and information sharing.** FIs must establish a robust process for the timely analysis and sharing of cyber threat intelligence within the financial ecosystem. This process should include collecting, processing and analysing cyber-related information (for instance, cyber events, cyber threat intelligence, and information on system vulnerabilities). FI should engage cyber intelligence monitoring services and actively participate in information-sharing arrangements with trusted parties. In addition, an FI should set up a security operations centre or acquire managed security services.
- **Cyber incident response and management.** To quickly deal with cyber threats and securely resume affected services, FIs should establish a cyber incident response and management plan that provides for communication, coordination, and response procedures to address various scenarios. The plan should also include a process to investigate and identify the security or control deficiencies as well as evaluate the impact on the FI.

Technology, Media and Telecommunications, Financial Institutions, Funds & Investment Management

- **Cyber security assessments (including cyber exercises simulating real-world attacks).** The 2021 TRM Guidelines provide FIs with further guidance on establishing procedures for regular assessment of vulnerabilities to their IT systems and prescribe minimal standards for such assessments, for instance, identification of weak security configurations, open network ports and application vulnerabilities. It also elaborates on penetration testing by FIs which should comprise a combination of blackbox and greybox testing for online financial services.

To stress test their cyber defences, FIs should conduct regular scenario-based cyber exercises, such as simulating the attack tactics, techniques, and procedures used by real-world attackers. This is aimed at validating the FI's response, recovery, and communication plans against cyber threats. Apart from the exercises, FIs should establish a comprehensive remediation process to track and resolve issues identified from the assessments and exercises.

Action Items for FIs

Although contravening the 2021 TRM Guidelines is not a criminal offence and does not attract civil penalties, the degree of observance with the spirit of the 2021 TRM Guidelines by the FI is one of the factors considered by MAS in its supervision of the FI.

Below are some action items for FIs' consideration to facilitate compliance with the 2021 TRM Guidelines:

- (i) Conducting a holistic assessment to identify gaps from their current practices against the 2021 TRM Guidelines that are relevant to their operations and address them appropriately. FIs may adopt a risk-based approach in implementing the 2021 TRM Guidelines;
- (ii) Ensuring that the Board and senior management appreciate and are able to competently carry out their expanded roles and responsibilities;
- (iii) Instituting processes that will facilitate compliance with the more stringent requirements to assess third party vendors and implement risk mitigation strategies to deal with threats from emerging technologies;
- (iv) Maintaining good cyber situational awareness by implementing and executing appropriate cyber security operations and assessment frameworks; and
- (v) Other than the 2021 TRM Guidelines which sets out technology risk management principles and best practices which FIs should adopt based on the nature, size and complexity of their business, relevant FIs should comply with legally binding requirements under applicable MAS Notices, for instance the MAS Notice on Technology Risk Management and Notice on Cyber Hygiene.

Technology, Media and Telecommunications, Financial Institutions, Funds & Investment Management

Concluding Remarks

To mitigate the burgeoning risks in the accelerated digital transformation of the financial sector, the 2021 TRM Guidelines underscore MAS' focus on FIs incorporating security controls as part of the technology development and delivery lifecycle, as well as in the deployment of emerging technologies. If you have any queries or wish to know how the 2021 TRM Guidelines impact your business operations and/or require assistance with compliance and/or implementation of the 2021 TRM Guidelines, please feel free to contact our team members below who will be happy to assist you.

Contacts

Technology, Media & Telecommunications



Rajesh Sreenivasan
Head, Technology, Media &
Telecommunications

T +65 6232 0751

rajesh@rajahtann.com



Steve Tan
Deputy Head, Technology, Media
& Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com



Lionel Tan
Partner, Technology, Media
& Telecommunications

T +65 6232 0752

lionel.tan@rajahtann.com



Benjamin Cheong
Partner, Technology, Media &
Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com



Tanya Tang
Partner (Chief Economic
and Policy Advisor),
Technology, Media &
Telecommunications

T +65 6232 0298

tanya.tang@rajahtann.com

Financial Institutions



Regina Liew
Head, Financial Institutions
Group

T +65 6232 0456

regina.liew@rajahtann.com



Larry Lim
Deputy Head, Financial
Institutions Group

T +65 6232 0482

larry.lim@rajahtann.com



Benjamin Liew
Partner, Financial Institutions
Group

T +65 6232 0686

benjamin.liew@rajahtann.com

Funds & Investment Management



Arnold Tan
Co-head, Funds &
Investment Management

T +65 6232 0701

arnold.tan@rajahtann.com



Anne Yeo
Co-head, Funds & Investment
Management

T +65 6232 0628

anne.yeo@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海

SHANGHAI REPRESENTATIVE OFFICE | *China*

**Rajah & Tann Singapore LLP
Shanghai Representative Office**
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office

T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office

T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*

Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL

GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited

T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office

T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office

T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.

The contents of this Update are owned by Rajah & Tann Singapore LLP and subject to copyright protection under the laws of Singapore and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Rajah & Tann Singapore LLP.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in Rajah & Tann Singapore LLP or email Knowledge & Risk Management at eOASIS@rajahtann.com.