# MAS Releases Revised Technology Risk Management Guidelines

## Introduction

On 18 January 2021, the Monetary Authority of Singapore ("**MAS**") issued the revised Technology Risk Management Guidelines ("**TRM Guidelines**"). The updated guidelines consolidate the feedback gathered from the MAS' 2019 public consultation, as well as the input from the MAS' engagement with industry stakeholders and its cybersecurity advisory panel.

This revision comes amidst a series of global cyberattacks such as the SolarWinds cyberattack, and reflects the higher standards of risk governance and strategy that financial institutions ("**FIs**") are expected to observe in dealing with risks that may arise from the adoption of new technology as well as the use of existing technology in innovative ways to increase operational efficiency and to enrich financial service offerings.

To this end, the revised TRM Guidelines set out risk management principles and industry best practices to guide FIs in establishing a sound and robust technology risk management framework and maintaining cyber resilience. While the revised TRM Guidelines are not legally binding, observance of the revised guidelines will be considered as part of the MAS' risk assessment of FIs.

Highlights of the key changes introduced in the revised TRM guidelines are set out below.

## Guidance Introduced in Revised TRM Guidelines

### Technology Risk Governance and Oversight

The revised TRM Guidelines provide additional guidance on the role of the board of directors and senior management by, among other things, setting out with greater granularity their specific responsibilities.

In addition, the revised TRM Guidelines also provide that both the board of directors and senior management should:

(a) have members with the knowledge to understand and manage technology risks; and

(b) appoint, with the approval by at least the Chief Executive Officer, a:

(i) Chief Information Officer, Chief Technology Officer or Head of IT with the requisite expertise and experience to establish and implement the FI's information technology ("**IT**") strategy, oversee daily IT operations and manage the relevant risks; and

(ii) Chief Information Security Officer or Head of Information Security with the requisite expertise and experience to manage the FI's information security strategy and programme, including information security policies and procedures.

To assist FIs in having an accurate and complete view of their IT operating environment, the revised TRM Guidelines recommend that FIs establish the following information asset (i.e., data, hardware and software, including those owned by, entrusted to, rented or leased by, or used by service providers to deliver their services to, FIs) management practices:

(a) identification of information assets supporting the FI's business and delivery of financial services;

(b) classification of information assets based on security classification and criticality;

(c) ownership of information assets and roles and responsibilities of staff managing them;

(d) establishment of policies, standards and procedures to manage information assets according to security classification and criticality; and

(e) maintenance of an information assets inventory which should be reviewed periodically and updated as and when there are changes.

## IT Project Management and Security-by-Design

To manage the risks involved in IT outsourcing, the revised TRM Guidelines introduce new guidance on the management of IT projects undertaken by FIs. Some key points that FIs should note are:

(a) for large and complex projects, FIs should form a project steering committee to provide direction, guidance and oversight;

(b) when acquiring software, FIs should put in place standards and procedures (comprising, among other things, the level of assessments and due diligence to be performed) for the evaluation and selection of vendors;

(c) FIs should control and monitor vendors' access to their IT systems and sensitive data;

(d) FIs should establish a framework to manage their system development life cycle ("**SDLC**") and utilise a Security-by-Design approach where security is built into each phase of the SDLC;

(e) FIs should identify, define, document and assess the functional requirements for the IT system as well as its system performance, resilience and security controls to determine the requisite level of security to be established;

(f) FIs should establish a methodology for system testing of the unit, modular, integration, system and user acceptance and any issues identified during testing should be properly tracked and addressed; and

(g) the expected quality attributes and assessment metrics for the project deliverables should be defined and quality assurance should be performed by an independent quality assurance function.

## Software Application Development and Management

The revised TRM Guidelines also set out specific guidance points on software development practices relating to:

(a) **Agile software development**: As Agile software development is based on an iterative and incremental development model to respond to business and customer needs, FIs should incorporate the necessary SDLC and security-by-design approach throughout the development process. Secure coding, source code review and application security testing standards should similarly be applied.

(b) **DevSecOps processes**: DevSecOps is the practice of automating and integrating IT operations, quality assurance and security practices in the software development process. Where this practice is deployed, FIs should ensure that the DevSecOps are aligned with their SDLC framework and IT service management processes. There should be adequate security measures and segregation of duties for the software development, testing and release functions.

(c) **Application Programming Interfaces** ("**APIs**"): APIs enable various software applications to communicate and interact with each other and exchange data. In this regard, FIs should ensure that adequate safeguards are established to manage the development and provision of open APIs for use by third parties to implement products and service customers. For example, third parties should be assessed on their suitability to access the APIs and connect to the FI's IT systems. There should also be measures in place to provide visibility of the usage and performance of APIs.

## IT Service Management and Access Controls

The revised TRM Guidelines provide additional guidance to FIs in the establishment and conduct of IT service management. Specifically, these points of guidance pertain to:

(a) **Configuration management**: FIs should maintain accurate and up-to-date information of their hardware and software to have visibility and maintain effective control over their IT systems.

(b) **Technology refresh management**: To avoid using outdated and unsupported hardware or software, FIs should monitor the end-of-support ("**EOS**") dates of hardware and software and establish a technology refresh plan for their replacement before they reach EOS.

(c) **Change management**: FIs should ensure changes to information assets are assessed, tested, reviewed and improved before implementation. A separate procedure for assessing, approving and implementing emergency changes should also be put in place.

(d) **Software release management**: FIs should practice segregation of duties in the software release process to ensure that no single individual can develop, compile and move software codes from one environment to another. This is to maintain the traceability and integrity of software codes.

Further, the revised TRM Guidelines set out practices that FIs should adopt in relation to access controls. For instance, where users are allowed to connect to the FI's internal network *via* an external network to access the FI's data and systems, it is recommended that such remote connections be encrypted to prevent data leakage, and that remote access to the FI's information assets only be allowed from devices that have been secured according to the FI's security standards.

## Data and Infrastructure Security

In addition to prescribing best practices for maintaining data and network security, the revised TRM Guidelines introduce further guidance and practice standards in relation to:

(a) **System security**: FIs should verify security standards in relation to their hardware and software to identify and address any deviations that might expose the system to cyber threats and establish safeguards such as endpoint protection, anti-malware signatures, detection and response mechanisms and white-listing to maintain integrity of their systems.

(b) **Virtualisation security**: Virtualisation refers the simulation of software or hardware upon which other software runs and is used by organisations to optimise the use of computing resources and to enhance resilience. Where such virtualisation solutions are used, FIs should introduce security standards and access controls for all components of such solutions, and manage virtual images and snapshots to guard against unauthorised access or modifications.

(c) **Internet of Things ("IoT") devices**: An IoT device includes any electronic device which can be connected to FIs' network or the Internet. As with all information assets, FIs should maintain an inventory of all their IoT devices, including information on the networks that they are connected to and their physical locations. Further, since many IoT devices are designed without or with minimal security controls, FIs should also implement controls on access to IoT devices, and continuously monitor these devices for suspicious activities.

## Cyber Security

The revised TRM Guidelines also set out additional controls and practices to improve the cyber resilience of FIs – namely, cyber threat intelligence and information sharing, cyber event monitoring and detection, cyber incident response and cyber security assessment.

To summarise, FIs should:

(a) establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to their business and IT environment;

(b) set up a process to detect and respond to misinformation related to FIs that is propagated *via* the Internet;

(c) establish a process to collect, process, review and retain systems logs to facilitate security monitoring operations;

(d) create baseline profiles of their IT systems to better analyse system activities and establish a process to escalate any suspicious system activities or user behaviour;

(e) establish a cyber incident response and management plan to isolate and neutralise cyber threats and to securely resume affected services;

(f) establish a process to investigate security or control deficiencies that result in any security breach; and

(g) conduct regular vulnerability assessments, penetration testing, scenario-based cyber exercises and adversarial attack simulation exercises to validate the effectiveness of their cyber defence and response procedure and rectify any issues identified from these assessments *via* a comprehensive remediation process.

**Online Financial Services**

On the management of online financial services, the revised TRM Guidelines provides FIs with additional guidance on customer authentication and transaction signing as well as fraud monitoring in order to ensure the integrity and authenticity of online transactions. In particular, FIs should:

(a) deploy multi-factor authentication for access to online financial services to secure customer authentication process;

(b) implement end-to-end encryption for transmission of customer passwords;

(c) implement transaction-signing for authorising high-risk activities to protect integrity of customer accounts' data and transaction details;

(d) store customer authentication credentials in a form that is resistant to reverse engineering; and

(e) implement real-time fraud monitoring systems to identify and block suspicious or fraudulent online transactions and establish a process to investigate such transactions or payments.

## Conclusion

The revised TRM Guidelines provide a timely update in the face of growing threats to the cyberspace environment, increasing prevalence of arrangements between FIs and third party service providers as well as the incremental use of emerging technologies. Incorporating the new points of guidance will provide FIs with an essential baseline in order to evaluate the efficacy of their internal policies and safeguards.

Given that the observance of the revised TRM Guidelines will be considered as part of the MAS' risk assessment of FIs, FIs should proactively review and update their systems, policies and operating procedures to account for the standards set out in the revised TRM Guidelines.

If you would like information or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

**LAM Chung Nian**
Head – Intellectual Property, Technology & Data
**d:** +65 6416 8271
**e:** chungnian.lam@wongpartnership.com
Click here to view Chung Nian's CV.

**Elaine CHAN**
Joint Head – Financial Services Regulatory
**d:** +65 6416 8010
**e:** elaine.chan@wongpartnership.com
Click here to view Elaine's CV.

**Kylie PEH**
Partner – Intellectual Property, Technology & Data
**d:** +65 6416 8259
**e:** kylie.peh@wongpartnership.com
Click here to view Kylie's CV.

**TIAN Sion Yoong**
Partner – Financial Services Regulatory, Derivatives & Structured Products and FinTech
**d:** +65 6416 2488
**e:** sionyoong.tian@wongpartnership.com
Click here to view Sion Yoong's CV.

Connect with WongPartnership.

# WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

### SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

### CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Corporate Avenue 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

### MYANMAR

-
WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

### INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

### MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

### MIDDLE EAST

-
Al Aidarous International Legal Practice
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com
-
Al Aidarous International Legal Practice
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

### PHILIPPINES

-
ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw