MAS Proposes Changes to the Technology Risk Management Guidelines

Introduction

The Technology Risk Management Guidelines ("**TRM Guidelines**"), issued by the Monetary Authority of Singapore ("**MAS**") in 2013, provides Financial Institutions ("**FI**") with guidance on the oversight of technology risk management, security practices and controls to address technology risks. Whilst the TRM Guidelines do not have force of law, it presents a set of industry best practices that FIs are expected to adopt, taking into account the activities they engage in and the markets in which they conduct transactions. For this reason, the MAS, in performing its risk assessment of an FI, also takes into consideration the FI's degree of observance with the spirit of the TRM Guidelines.

Recognising the need for the TRM Guidelines to remain relevant in a fast evolving physical and cyber threat landscape, the MAS released in March 2019, a consultation paper proposing changes to update the TRM Guidelines. The public consultation has since closed on 8 April 2019.

In this latest consultation paper, the MAS proposed changes which require FIs to implement enhanced measures to increase their operational resilience. Highlights of the salient proposed revisions are set out in the table below.

Proposed Changes

	Proposed TRM Guidelines
Technology Risk Governance and Oversight	The proposed TRM Guidelines sets out more detailed guidance as to the responsibilities of the FI's board of directors and senior management in relation to technology risk management and oversight. In particular, the board and senior management are expected to include members equipped with the necessary skills and understanding of technology risks, including risks posed by cyber threats. The board is also responsible for appointing: (a) A Chief Information Officer, Chief Technology Officer or Head of Information Technology with the requisite expertise and experience, to be responsible for information technology and computer systems that support enterprise goals; and (b) a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme.

	Proposed TRM Guidelines
Software Development and Management	In addition to the general guidance in relation to software development set out under the existing TRM Guidelines, the proposed TRM Guidelines now provides specific guidance on various types of software developments, including: (a) "Agile" software development method (an iterative and incremental model to accelerate software development and delivery); (b) "DevOps" management practices (the practice of automating and integrating IT operations and quality assurance into the software development process); and (c) Application Programming Interface Development. The proposed TRM Guidelines also sets out in greater detail the recommended types of application security testing methods that FIs should adopt. For example, FIs should adopt a mixture of static, dynamic and interactive application security testing methods.
Emerging Technologies	The proposed TRM Guidelines provides further guidance for FIs to manage risks arising from emerging technologies such as application programming interfaces ("**APIs**"), smart electronic devices, internet of things ("**IoT**") and virtualisation, e.g.: (a) establishing adequate safeguards to manage the development and provision of APIs for secure delivery of such services, and implementing strong controls to authorise and control access to designated API services; and (b) maintaining an inventory of all its IoT devices, the networks which they are connected to and their physical locations. The FI should assess and implement processes and controls to mitigate risks arising from IoT.
Cyber Resilience	In addition to the existing internal controls and risk management practices set out under the existing TRM Guidelines, the proposed TRM Guidelines provides further guidance and supports a defence-in-depth approach to strengthen the cyber resilience of FIs. In particular, the proposed TRM Guidelines includes guidance on effective cyber surveillance, cyber security assessment and testing, as well as cyber incident management. In summary, FIs should: (a) establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment; (b) implement monitoring or surveillance systems to ensure it is alerted to any suspicious or malicious system activities, and real-time monitoring of cyber events for critical systems;

	Proposed TRM Guidelines
	(c) establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to resume affected services as soon as possible; and (d) conduct and carry out regular vulnerability assessments, penetration testing, scenario-based cyber exercises, adversarial attack simulation exercises, intelligence-based exercises and resolve the issues identified from these exercises through an established comprehensive remediation management process.

Conclusion

The proposed TRM Guidelines is a timely update in addressing issues arising from emerging technological updates, especially given the emergence of the IoT and introduction of new software development methods.

When implemented, FIs are expected to adopt and comply with the updated standards and measures to the extent that these are relevant to their operating environment, and commensurate with the level of risk and complexity of the financial services offered, and the supporting technologies deployed. Whilst not legally binding, the revised TRM Guidelines is nevertheless imperative in being supplemental to, and read in conjunction with, the applicable legislation, written directions and other notices, codes and guidelines issued by the MAS. The TRM Guidelines also serves as a measure of standards taken into account by the MAS in its supervision of FIs.

In anticipation of the upcoming developments, FIs should closely watch this space and consider reviewing their internal policies and systems to critically assess if they are in the position to comply with the revised positions and proposed changes, once these are effected.

If you would like information on this or any other area of law, you may wish to contact the partner at WongPartnership that you normally deal with or any of the following partners:

LAM Chung Nian
Head – Intellectual Property, Technology and Media, Telecommunications and Data Protection Practices
d +65 6416 8271
e chungnian.lam@wongpartnership.com
Click here to view Chung Nian's CV.

Kylie PEH
Partner – Intellectual Property, Technology and Media, Telecommunications and Data Protection Practices
d +65 6416 8259
e kylie.peh@wongpartnership.com
Click here to view Kylie's CV.

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
Beijing Representative Office
Unit 3111 China World Office 2
1 Jianguomenwai Avenue, Chaoyang District
Beijing 100004, PRC
t +86 10 6505 6900
f +86 10 6505 2562

-
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

wongpartnership.com