Singapore Regulatory Update – MAS Updates Technology Risk Management Guidelines (January 2021)

On 18 January 2021, the Monetary Authority of Singapore ("MAS") released updated Technology Risk Management Guidelines ("TRM Guidelines") to take into account the emergence of new technologies and the continual evolving sophistication of cyber threats.

The updates made to the TRM Guidelines focus on Financial Institutions ("FIs") that utilise cloud technologies, application programming interfaces, and rapid software development. The TRM Guidelines stress the importance for FIs incorporation security controls and emerging technologies into their technology risk management framework.

Recent Cyber Attacks

Cyber threats are becoming more common in today's technology driven environment. This has been made clear with the recent spike of cyber-attacks on supply chains, which are targeting multiple IT service providers through the exploitation of widely-used network management software. To mitigate potential threats the updated TRM Guidelines sets out the following enhanced strategies for FIs:

- To establish a robust process for the timely analysis and sharing of cyber threat intelligence within the financial ecosystem; and
- To conduct cyber exercises to allow FIs to stress test their cyber defences by stimulating the attack tactics, techniques, and procedures used by real-world attackers.

Board of Directors / Senior Management

The Board of Directors (or a committee delegated by it) (the "Board") is ultimately responsible for ensuring that the FI has a technology risk management framework ("TRFM") and strategy suitable for its business. The Board is expected to provide an independent view of the technology risks faced by the FI and ensure that an independent audit function is established to assess the effectiveness of the controls, risk management and governance of the FI.

The Board and senior management must ensure they appoint and approve suitably experienced individuals as either a Chief Information Officer, Chief Technology Officer or Head of IT, and a Chief Information Security Officer or Head of Information Security.

The Board and senior management are expected to ensure a technology risk management strategy is established and implemented. When making any key IT decisions the Board and senior management should assess the decision against the FIs risk appetite and ensure full documentation of any key decisions are kept.

Senior management are responsible for the establishment and implementation of a suitable technology risk management framework and strategy for the FI.

ComplianceAsia Consulting Pte Ltd. 137 Telok Ayer Street #03-06, Singapore 068602
Tel: (65) 6533 8834 www.complianceasia.com

Third Party Providers

It is common for FIs to outsource and rely on third party providers for IT system matters. The use of third-party services may not always constitute outsourcing as per the Outsourcing Guidelines.

Nevertheless, before entering into any third-party contractual arrangement, FIs should assess and manage the exposure they face to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party.

On an ongoing basis, an FI should review the conduct of the third party to ensure they employ a high standard of care and diligence in protecting data confidentiality and integrity and the overall resilience of the IT systems.

When performing a risk identification assessment FIs should look to identify any threats and vulnerabilities applicable to its IT environment and this includes information assets that are either maintained or supported by the third-party provider. Security threats that may have an adverse impact on an FI include internal sabotage, malware and data theft.

An FI should establish a procedure for the use of a third party and open-source software codes to ensure these codes are reviewed and tested before they are integrated into the FIs software.

Risk Assessment and Management

To ensure technology risks are a core priority of an FI, the MAS expects FIs to design and establish a set method to measure and determine the likelihood and potential impact of the risk scenarios.

The FI should utilise risk mitigation measures to mitigate the impact of any considerable technology risk. IT controls and risk mitigation practices should be regularly reviewed and updated, taking into account the changing threat landscape and variations in the FIs risk profile.

Software Application Development and Management

If an FI is using any open-source software codes provided by a third party the FI is expected to have in place policies and procedures to ensure the codes are subject to adequate review and testing prior to being integrated into the FIs software.

If any IT vulnerabilities that present issues for an FI arise it is important that the FI has in place procedures to remediate the vulnerabilities in a timely fashion. The FI must keep a register of updates and reported vulnerabilities for third party and open-source software codes that are incorporated into the FIs software.

An FI must ensure software developers are appropriately trained with the necessary skills to apply the secure coding and application security standards when developing applications.

ComplianceAsia Consulting Pte Ltd. 137 Telok Ayer Street #03-06, Singapore 068602
Tel: (65) 6533 8834 www.complianceasia.com

End User Computing and Applications

Any IT infrastructure that has not been properly managed or implemented internally present an increased risk for leakage of sensitive data or malware infection. It is crucial that any shadow IT structures are managed as part of the FIs information assets. The FI must have in place measures to control and monitor the use of any shadow IT in its environment.

FIs should establish a process to assess the risk of end user developed or acquired applications which includes appropriate controls and security measures to address risks identified. Any outside applications should be appropriately tested prior to roll out throughout the FI.

Incident Management

It is inevitable that at one point in time an FI will experience some form of IT related incident. When this unfortunate event occurs, it is important that the incident is carefully managed. The MAS believes that it is useful for an FI to provide timely updates to clients on the progress of its incident management and the measures used to protect its clients and continue its business activities.

How we can help

In order to ensure continued compliance with the TRM Guidelines it is important that your IT department critically assess the IT Policies and Procedures to ensure that they are robust and reflect the expectations of the MAS.

ComplianceAsia's dedicated projects team can provide you with a full gap analysis of your existing Technology Risk Management Framework to ensure that it is compliant with the revised MAS Technology Risk Management Guidelines and industry best practices. If your firm does not yet have a Technology Risk Management Framework in place, we can provide you with a customised TRM framework that provides you with the practical steps needed to comply with the revised guidelines.

About ComplianceAsia

ComplianceAsia is the longest established compliance consulting firm in Asia Pacific established in 2003 with key offices in Hong Kong, Shanghai, Singapore, Tokyo and London. We have an unmatched track record of completing complex compliance consulting projects for financial firms in the APAC region.

With over 70 staff, including compliance experts with experience in dealing with the SFC, HKMA, MAS, CSRC, JFSA and Asian exchanges, we provide independent, unbiased advice on Asian financial industry legislation and regulations. Our international client base consists of asset managers, hedge funds, private equity funds, family offices, broker-dealers, insurers, wealth managers and investment banks.

ComplianceAsia Consulting Pte Ltd. 137 Telok Ayer Street #03-06, Singapore 068602
Tel: (65) 6533 8834 www.complianceasia.com

Contact Us Today

HONG KONG
Suite 1102
ChinaChem Tower
34 – 37 Connaught Road
Central

T: +852 2868 9070

SINGAPORE
137 Telok Ayer Street
#03-06
Singapore 068602

T: +65 6533 8834

MAINLAND CHINA
Room 132, Unit 1301-1308
13/F, Shanghai Tower
No.479 Lujiazui Ring Road
Pudong New Area Shanghai

T: +86 147 1431 1859

JAPAN
Level 2
Marunouchi Nijubashi Building
3-2-2 Marunouchi Chiyoda-ku
Tokyo 100-0005

T: +81 3 6837 5483

UNITED KINGDOM
1 St. Andrew's Hill
London
EC4V 5BY

T: +44 (0) 20 7213 0300
M: +44 (0) 7310 972435

ComplianceAsia

W: www.complianceasia.com

Philippa Allen
CEO
E: philippa.allen@complianceasia.com

Alex Duperouzel
Managing Director
E: alex.duperouzel@complianceasia.com

Lachlan Chubb
Regional Head of Regulatory Advisory and Projects
E: lachlan.chubb@complianceasia.com

Geralllt Owen
Regional Head of Client Relations
E: geralllt.owen@complianceasia.com

Cherry Chan
Regional Head of Ongoing Support and Client Services
E: cherry.chan@complianceasia.com

Rachel Wu
Head of Mainland China Client Engagements
E: rachel.wu@complianceasia.com

Robert Lind
Senior Representative, UK and Europe
E: robert.lind@complianceasia.com

Hanae Kuroda
Compliance Consultant
E: hanae.kuroda@complianceasia.com