WHITEPAPER

MAS TRM Guidelines 2021 Deconstructed:

The Future of Cyber for Financial Institutions and FinTechs.

5 FEBRUARY 2021



Table of Contents

Executive Summary	2
Expectations for Financial Institutions and Service Providers	3
Summary of Key Changes	4
TRM Deconstructed	5
Other Areas of Emphasis	15
Guide for Service Providers	17
How Intellisecure Can Help You & Contact	18
Glossary	19

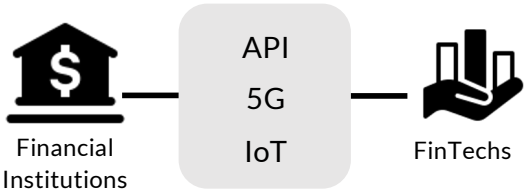
EXECUTIVE SUMMARY

The latest MAS Technology Risk Management Guidelines (TRMG) was released on January 18, 2021, eight years after the last release in 2013. TRMG 2021 accommodates the expansion of technology in the financial services industry in Singapore and worldwide.





Traditional Financial Institutions (FI's) globally are undergoing digital transformation to evolve like technology companies. To remain competitive, FI is developing complex consumer financial services and applications. There is also rapid integration of services between traditional FI's and FinTechs.



With technology playing such a crucial role in FI's, senior management and the Board of Directors must be more involved and understand technology risk in the ever-changing cyber threat landscape. There is an increased emphasis on secure development practices and API security. This includes a 'shift-left' where the security requirements of any IT project should be considered at the beginning of the design phase.

Adapting to fast-changing times, TRMG 2021 also endorses Bug Bounty programs as a legitimate complement to Penetration Testing programs in FI's. Security controls and cyber tooling are also more prescriptive. The emphasis on tools and practices improves the resilience of FI's in Singapore by improving the FI's capabilities to detect, respond and recover from cyberattacks.

We hope you find this whitepaper informative and resourceful. Please feel free to contact the Intellisecure team at contact@intellisecure.co if you have any questions.

EXPECTATIONS FOR FINANCIAL INSTITUTIONS

MAS expects FI's to be compliant with the MAS TRM Guidelines. FI's should conduct a gap analysis to determine any non-compliance to the requirements. The gaps identified should be appropriately assessed and remediated. Any non-compliance as a result of implementation difficulties should be documented and explained with mitigating controls identified. FI's compliance to MAS TRM Guidelines will be assessed by external auditors or MAS inspections.

EXPECTATIONS FOR SERVICE PROVIDERS

While MAS does not expect service providers to comply to the TRM Guidelines, any regulated client may expect you to have similar or identical requirements to MAS TRM. A baseline expectation for service providers is to have secure and resilient systems as well as competent staff. Specific provisions are mentioned in the Guide for Service Providers section.

DISCLAIMER

The guidelines provided in this whitepaper highlights key areas from the MAS TRM Guidelines 2021 and are not intended to be comprehensive nor replace or override any legislative provision. Firms should take a risk-based approach to the Guidelines and implement controls and processes that are relevant to their own risks.

All content provided is information of generic nature and does not address the circumstances of any individual or entity. Performing all recommended tasks does not make you compliant, or fully secured.

All information provided is for educational and informational purposes only and is solely based on our professional opinion. It is not intended as a substitute for the guidance and requirements provided by the Monetary Authority of Singapore.

SUMMARY OF KEY CHANGES (2013 to 2021)

01

The Role of the Board



Changes to the first sections make it clear to all Board members that this is not just an IT problem and that they have direct responsibility for overseeing technology risk. This should be a wake-up call for some institutions that see IT as a cost function.

02

Rising Cybersecurity Tooling



Achieving cyber resilience is one of MAS' s two main objectives for the TRMG, and the guidelines mention several tools and services to help FIs attain it. Specific solutions that are more focused in the 2021 Guidelines include Network Access Control, Multi-Factor Authentication, Endpoint Systems control, Bug Bounty programs, Managed Security Services, Cyber Intelligence Monitoring services, and Phishing campaign monitoring tools.

03

Significant Expansion in Testing



A notable addition to TRMG 2021 is the introduction of cyber exercises and red-teaming, intended to enhance FI's' readiness in dealing with cyber threats. MAS encourages operating from secondary or alternate sites periodically during disaster recovery testing to assess its ability to support business needs for an extended period. For Penetration Testing, MAS explicitly mentions conducting this on systems' production environments, a change from 2013.

04

Focus on Secure Development



Security used to focus more on Infrastructure than development, but the new Guidelines has a major shift towards coding standards, Security by Design, and DevSecOps. Infrastructure still exists, and stronger than ever, but the guidelines on application development, procurement, and project management have increased enormously.

05

New Sections on IoT, BYOD, Virtualisation, Cyber Security Operations



Traditional perimeters are down, and MAS gives due recognition to this fact in the TRMG 2021. The 2013 section on Cloud Computing was removed, and the cloud is now treated as part of the FI's' IT landscape. TRMG requirements are expected to apply whether systems sit on-premises or cloud. TRMG 2021 also introduced new chapters dedicated to "non-traditional" areas such as the Internet of Things (IoT), Shadow IT, and Bring Your Own Device (BYOD). The widening of the FI's IT landscape comes with increased security risks. A new TRMG chapter on Cyber Security Operations was created to aid FI's in guarding against threats

TRM DECONSTRUCTED

We dissect key statements and show what they mean for your organisation.



1. Board and Senior Management | TRMG 2021 Chapter 3

TRMG says:

One of the key TRMG 2021 highlights is higher management's increased role and involvement in managing the FI's technology strategy and operations. For bigger organisations, higher management can pertain to the local Board of Directors (BoD), while smaller FIs may have a regional oversight body on top of local management, who should take up these responsibilities.

Some key requirements to note are as follows:

- BoD and Senior Management must have members with knowledge to understand and manage technology risks.
- FI should appoint a Chief Technology Officer and a Chief Security Officer (or equivalent, for smaller FI's).
- BoD should have governance and oversight over technology risks, including making key IT decisions.
- FI's should have a technology risk management strategy in place.
- BoD should undergo security awareness training.

For those leading technology and information security for their respective organisations, TRMG 2021 presents a new window of opportunity to engage your higher management on technology and security matters. It is essential to clearly communicate what the FI's' technology risks are and, more importantly, how it impacts the business. It is equally important to present a plan of action to manage these risks.

The key takeaway of this requirement is that all FI's should move from a siloed perspective and view technology as an integral part of the business. Technology comes with costs and risks, but it is also a business enabler that can provide value and efficiency if a proper strategy is implemented. It is a culture change for higher management to have an open mind when understanding technology opportunities, challenges, and risks. For technology and security professionals, the challenge is to deliver a technology risk management strategy that clearly explains the impact on business objectives for higher management to understand and appreciate.

FI task list:

- ✓ Update the BoD Charter to include technology risk-related responsibilities
- ✓ Have BoD member/s who are experienced on technology risk management
- ✓ Appoint senior technology and security-related roles in the FI who have reporting lines to the BoD and Senior Management
- ✓ Establish a governance process to enable effective reporting of technology matters to higher management
- ✓ Conduct security awareness training for BoD and Senior Management

References:

- Sections: 1, 3.1, 3.6, 4.1.4

2. IT Project Management | TRMG 2021 Chapter 5

TRMG says:

Chapter 5 provides guidelines for the governance of IT projects undertaken by FI's. This includes creating project committee for large and complex projects, clear requirements for conducting vendor due diligence, Security-by-Design and a quality management process.

Senior management are expected to be involved large and complex IT projects that impact the business. This is to ensure that the any business and security project risk are adequately addressed.

The TRMG 2021 recommendations for Security-by-Design is in line with the industry trend of shifting security left of the software development lifecycle. A Security-by-Design approach streamlines the development of a secure application, avoiding the complications that normally arise from having security as an afterthought.



Security-by-Design

A 'shift-left' in application security means that the security requirements of an application or IT system are considered at the design phase rather than bolted on at the end.

Requirements for vendor due diligence are made more explicit in the TRMG 2021. FI's should establish standards and procedures for assessing the security of the vendor and its applications. Depending on the criticality of the application, the TRMG suggests that the FI should have access to the source code of the third-party software.

FI task list:

- ✓ Establish standards and procedures for vendor due diligence
- ✓ Design secure architecture for systems and applications
- ✓ Develop vendor due diligence process and procedures
- ✓ Establish a project steering committee for large and complex projects that involves key stakeholders and senior management

References:

Sections: 5.1, 5.2, 5.3, 5.4

3. Software Application Development and Management | TRMG 2021 Chapter 6

TRMG says:

This Chapter discusses security guidelines for designing, developing, testing and reviewing applications and Application Programming Interfaces (APIs). It also includes source code reviews, DevSecOps management, Agile development and end-user IT management.

The secure development of APIs is a key highlight of this chapter. TRMG 2021 recognises that financial services have become an interconnected ecosystem. FIs will increasingly collaborate and provide complex financial services to consumers by connecting to each other's systems using APIs. APIs should be sufficiently secure for the fintech ecosystem to flourish. Although API security is a complex topic which overlaps into other technology domains, the TRMG 2021 sufficiently expounds on key points. For example, the governance of third-party API access, security standards for API development and design, strong encryption, API security testing during pre-production, and real-time monitoring of API calls and availability. A new requirement has been introduced that requires FI's to vet customers who want to consume their APIs.

Guidelines for software development methodologies like DevSecOps and Agile are also mentioned. When practising DevSecOps, segregation of duties should be enforced, ensuring that highly integrated development and operational practices do not compromise the integrity and security of the application.

The TRMG recommends that FIs practising Agile incorporate secure coding practices, source code reviews and application security testing into their development lifecycle. This ensures that security does not take a backseat to faster software releases.

Unauthorised use of end-user applications should also be managed. Employees should be explicitly authorised to use any applications for business purposes. Unauthorised use of software, also known as Shadow IT, can introduce security risks to the FIS.

FI task list:

- ✓ Design, establish and enforce API standards during the software development lifecycle
- ✓ Develop secure software development lifecycle
- ✓ Establish policies and procedures to govern and manage third-party access to APIs
- ✓ Establish segregation of duties for DevSecOps
- ✓ Establish secure coding practices, source code reviews and application security testing, especially if practicing Agile
- ✓ Manage end-user applications risk using whitelists

References:

- Sections: 6.1, 6.2, 6.3, 6.4, 6.5

4. Remote Access Management | TRMG 2021 Chapter 9.3

TRMG says:

TRMG 2021 provides foundational guidelines for remote access management. It focuses on secure authentication of the remote connection and the security of the devices used to remotely access an FI's information assets.

Strong authentication refers to using multi-factor authentication to verify the identity of the entity requesting access to the FI's IT environment. Industry-accepted encryption algorithms should be used to secure communication channels, safeguarding data integrity or API calls. TRMG has an entire chapter outlining security practices on cryptography.

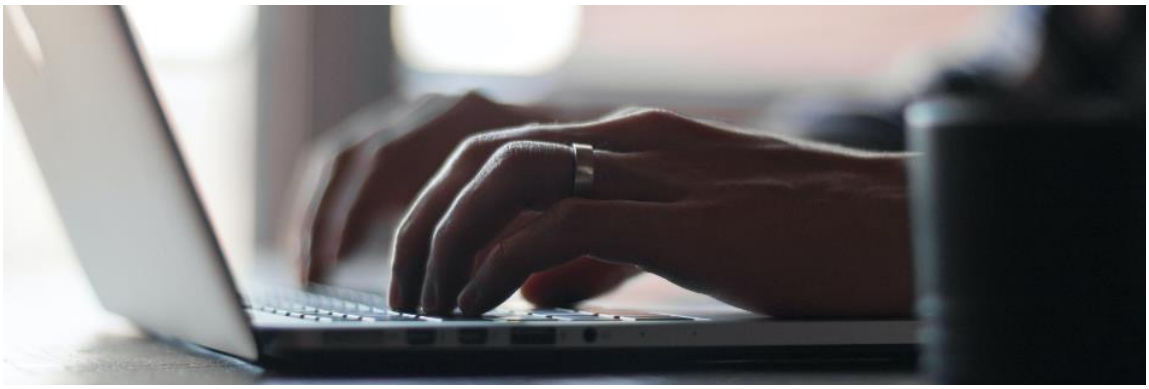
FIs should also ensure that the devices used to access their information assets have been hardened and adequately protected before access is granted. For example, devices should have endpoint protection solutions installed and be securely configured. Such practices allow secure remote connections by protecting the physical and network infrastructure supporting the remote connections.

FI task list:

- ✓ Establish processes and procedures to harden devices
- ✓ Develop a secure identity and access management (IAM) model
- ✓ Implement endpoint protection solutions to protect and monitor devices
- ✓ Use industry-accepted encryption algorithms to protect communication channels
- ✓ Implement multi-factor authentication

References:

Sections: 9.3, 10, 11.3.1, 11.3.2



5. Bring Your Own Device | TRMG 2021 Annex B

TRMG says:

Bring Your Own Device (BYOD) refers to employees using personal devices to access business information and systems. BYOD allows for a mobile and dynamic workforce but also introduces security risks that should be addressed by FI's.

The TRMG 2021 recommends that FI's augment their BYOD policies and procedures with security controls such as Mobile Device Management (MDM) or virtualisation solutions. MDM solutions can manage and control mobile devices and have features such as storage encryption, remote wipe and baseline security monitoring. Virtualisation solutions allow end-users to remotely access the FI's IT systems and applications via mobile devices by using a virtual environment or sandbox.

FI task list:

- ✓ Implement MDM and/or virtualisation solutions
- ✓ Establish BYOD policies and procedures around how personal devices can be used for business purposes

References:

Sections: 11.3.7, Annex B: BYOD Security



6. Data and Infrastructure Security | TRMG 2021 Chapter 11

TRMG says:

Chapter 11 of TRMG 2021 touches on various topics, such as virtualisation, IoT, network, data and system security. It is also more prescriptive than its 2013 predecessor.

There is more emphasis on endpoint protection, with MAS recommending hardening endpoints in line with industry best practices, such as CIS Benchmarks. This includes secure configurations and the implementation and maintenance of endpoint protection solutions.

The network security section recommends using Network Intrusion Protection Systems and Network Access Control (NACs) to detect and block malicious traffic, along with more traditional network security devices like firewalls. These devices should be constantly updated.

A new significant section on Virtualisation Technology has been introduced. Appropriate policies and procedures to manage virtual machines and snapshots should be implemented. Access to hypervisors and system hosting hypervisors should be restricted.

TRMG 2021 introduces the concept of sandboxed browsing — "isolating internet web browsing activities from its endpoint devices" – and a new section on IoT Security. IoT devices need to be hardened, and IoT networks need to be segregated from networks that host the FI's data and systems.

FI task list:

- ✓ Review your security architecture and ensure Network Intrusion Prevention Systems (NIPS) and Network Access Control (NAC) are setup effectively.
- ✓ Review your IT environments and security architecture to define clear zones that prevent attacker's movement.
- ✓ Evaluate the internet browsers in use and sandbox browsing for implementation.
- ✓ Ensure policy, standards and access controls are implemented for the lifecycle of virtual images, snapshots and hypervisors.
- ✓ Segregate IoT devices from your core operations and subject them to security testing and security controls (e.g., access control and security monitoring).

References:

- Sections: 11.1, 11.2, 11.3, 11.4, 11.5

7. Cyber Security Operations | TRMG 2021 Chapter 12

TRMG says:

TRMG 2021 advocates the procurement of cyber intelligence monitoring services and participation in cyber threat information-sharing arrangements. Threat intelligence includes but is not limited to, services that keep FIs updated on the latest malware, system vulnerabilities, and Tactics, Techniques and Procedures (TTPs) used by Advanced Persistent Threat (APT) groups targeting FIs.

FIs should also participate in or subscribe to cyber intelligence sharing platforms like FS-ISAC, IT-SAC, SingCert or CVE. Such activities help to improve their resilience to cyberattacks.

Other recommendations include the capability to detect and respond to misinformation propagated via the Internet and the establishment of cyber incident response capabilities.

FI task list:

- ✓ Subscribe to or participate in ISACs and Certs, as well as other commercial alternatives
- ✓ Develop a threat and vulnerability management program
- ✓ Procure threat intelligence monitoring services
- ✓ Develop incident response capabilities
- ✓ Establish policies and procedures for dealing with misinformation propagated via the internet

References:

- Sections: 12.1, 12.2, 12.3





8. Cyber Exercises | TRMG 2021 Chapter 13.3 to 13.5

TRMG says:

Sections 13.3-13.5 highlight the requirements for carrying out scenario-based cyber exercises based on threat intelligence, including social engineering, table-top exercises, and adversarial attack simulation exercises. Such exercises allow FIs to test their detect and response capabilities and decision-making during a real crisis.

FI task list:

- ✓ Conduct scenario-based cyber exercises involving key stakeholders and senior management
- ✓ Conduct adversarial attack simulation exercises

References:

- Sections: 13.3, 13.4, 13.5



9. Penetration Testing | TRMG 2021 Chapter 13.2

TRMG says:

TRMG 2021 calls for penetration testing (PT) of internet-facing systems to be conducted at least annually or after a major change. It also recommends that penetration testing be conducted on production environments.

More notably, as a sign of changing times, the TRMG 2021 endorses bug bounty programs as an acceptable method to complement an FI's vulnerability and penetration testing program.

FI task list:

- ✓ Review the scope of penetration testing to include internal and production systems
- ✓ Conduct penetration tests annually or after a major change

References:

- Sections: 13.2

10. Online Financial Services | TRMG 2021 Chapter 14

TRMG says:

Chapter 14: Online Financial Services includes new requirements to actively monitor for phishing campaigns against the users of your services, encryption and digital signatures, application sandboxing, device root protection, and mobile application security.

TRMG 2021 covers Customer Authentication and Transaction Signing requirements such as MFA, transaction signing, adaptive authentication, time-based OTPs, biometrics, soft tokens, session protection, maker-checker functions, and secure credential storage.

Additionally, section 14.3 requires real-time fraud monitoring systems. While this is common practice in some areas, such as credit card transactions, TRMG 2021 has expanded the scope to include any online transaction. This is a significant new requirement for services that don't already do this.

FI task list:

- ✓ Monitor phishing campaigns, tighten mobile app and end-user mobile device security, review your online MFA and its technical implementation
- ✓ Implement fraud monitoring for online transactions



OTHER AREAS OF EMPHASIS

01 Establish a proper risk management framework

Risk management is a key concept in the TRMG. MAS encourages a risk-based approach in the adoption of the TRMG when FI's assess their compliance with the requirements. Various sections of the TRMG also emphasise the need to do risk assessments and take actions based on the impact of the risk on the FI. Examples include policy deviations, use of API, change management, end-of-life software, use of untested DR plans, and BYOD. FI's should have a mechanism in place to identify, assess, treat, and monitor its risks.

TRMG 3.2.2, 4, 6.4.3, 7.3.2, 7.5.2, 8.2.3, 8.5, 11.3.7, 13.6, 14.2.10, 15.1.2

02 Implement Your Policies and Keep Track of Compliance

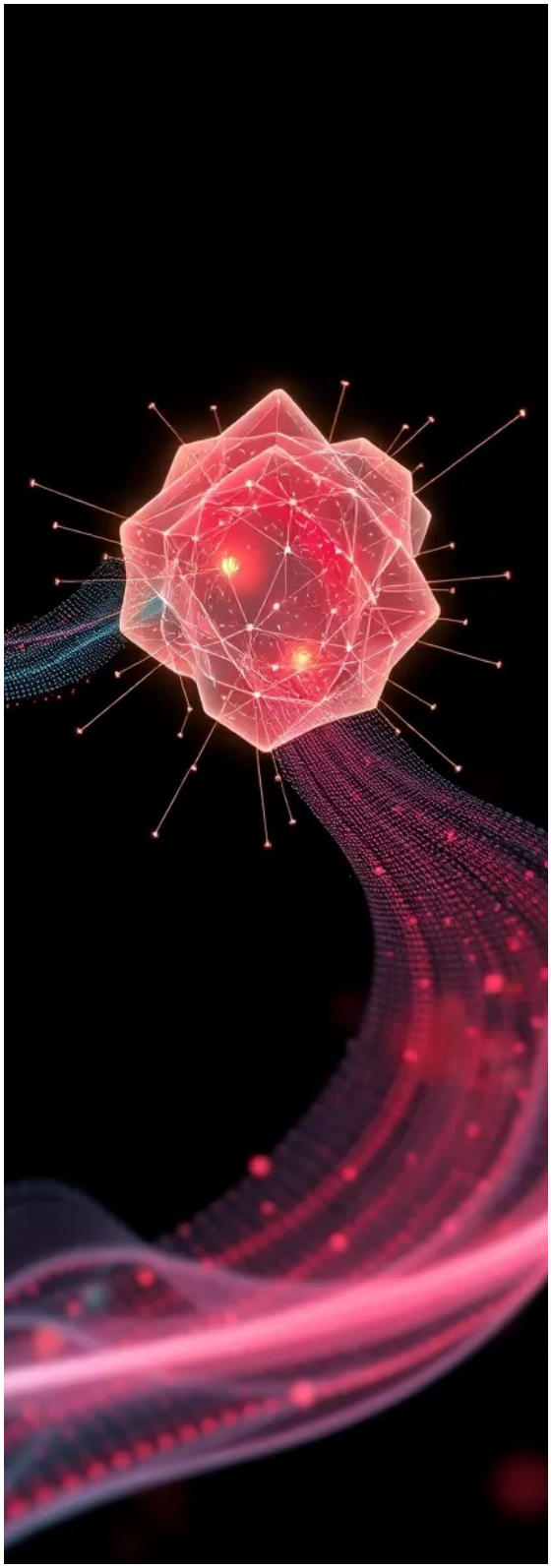
TRMG includes requirements such as implementing compliance processes, conducting periodic assessments of controls, tracking deviations from policies, and IT auditing. These requirements emphasise that policies and procedures should not be a mere piece of a document but should rather drive the consistent implementation of controls to protect the FI's assets and help achieve business objectives.

TRMG 3.2, 4.5.1, 15

03 Insure Yourself Against Cyber Risk

MAS now requires FI's to take technology risk insurance. As well as financial protection, insurance gives FI's access to a panel of experts such as lawyers and forensic specialists to aid FI's in responding to cyber incidents more effectively.

TRMG 4.4.3



OTHER AREAS OF EMPHASIS

04 Know Your Assets and Assign Accountability

It is essential to know what to protect, else there may be critical assets that are left unprotected or expensive tools that are not fully utilised or are used for the wrong purpose. FI's should start with understanding their assets, where they are, and who has access to them. It is also important to assess their impact on the organisation such that better decisions can be made on the right level of protection. Assets must have assigned owners who are responsible for ensuring that assets are properly managed throughout its lifecycle.

TRMG 3.3, 7.2.1

05 Conduct Background Checks on Personnel with Access to FI's Systems and Data, including third parties

Background screening is needed to support hiring decisions based on candidate suitability, and to protect against operational risk. From a cybersecurity perspective, background screening is a key preventive control against insider threats.

TRMG 3.5.2

06 Assess Risks Arising from Third-Party Services

The TRMG 2021 highlights the increasing ubiquity of third-party services in the IT ecosystem. Hence, FI's should regularly assess and manage exposure to technology risks brought about using third-party IT services. FI's should keep track of their third parties and establish processes around due diligence and periodic monitoring based on criticality of services provided.

TRMG 3.4

07 Establish a Resilient Architecture and Test for Recovery

FI's should document their architecture diagrams and ensure redundancies are in place for their systems to avoid single points of failure (including any external dependencies). Redundancy solutions should allow the FI to meet business RTO and RPO requirements, especially for critical systems with legally binding requirements on high availability based on the TRM Notice. FI's should document recovery plans and test these periodically using plausible disruption scenarios. FI's should also aim to operate from a recovery or alternate setup for an extended period for a more relevant test.

TRMG 8.1 to 8.3, TRM Notice para 4 to 6

GUIDE FOR SERVICE PROVIDERS

TRMG 2021 lays out several expectations for service providers to securely and reliably support FI's.

Stringent Due Diligence

The TRMG 2021 expects FI's to conduct stringent due diligence on service providers to ensure that they do not pose any unnecessary risks to the FI's. These due diligence exercises are holistic and include many aspects of technology risk management. Service providers should consider undertaking industry-recognized security compliance certifications and attestations like ISO 27001 and SOC 2 Type II to help ensure they have the right control framework and can demonstrably meet this due diligence.

Competency and Background Checks

Service providers must also prove that their employees are competent and sufficiently skilled. This can be fulfilled by providing professional development opportunities like training and certifications. Background checks should also be conducted on the staff of service providers. This reduces any risks related to insider threats.

Disaster Recovery Capability

FI's and their service providers should have advanced disaster recovery capabilities to promote a resilient financial services ecosystem. Service providers should have disaster recovery policies and procedures in place. Disaster recovery testing and arrangements should be carried out regularly to meet target RTO (Recovery Time Objective) and RPO (Recovery Point Objectives). Additionally, disaster recovery testing should be a coordinated effort between service providers and the FI to troubleshoot potential problems during a disaster recovery situation.

System Security

Service providers managing any systems on behalf of FI's should ensure that these systems are appropriately protected and adhere to FI's system security standards. The service provider should conduct system hardening activities to meet the applicable security standards. Additionally, reputable endpoint protection solutions should also be installed. These activities help secure the software security supply chain as all systems with access to the FI's IT environment and systems managed by service providers are appropriately secured.

Interconnected Ecosystem

The MAS also expects FI's and service providers to work closer together for a more resilient financial services ecosystem. Service providers are expected to undergo security awareness training programs conducted by the FI's and be part of the FI's cyber exercises, if applicable. Such partnership will foster a more dynamic and closer working relationship, which will be crucial in times of crisis.

HOW INTELLISECURE CAN HELP YOU

Compliance with the new regulations is just the first step in managing risk in a Financial Institution and its supply chain. Are organisations ready to adopt these changes internally, and if they do, what are their capabilities?

At IntelliSecure, we are here to help. As a Cyber Consultancy with an in-depth understanding of the MAS TRM, we can support your organisation in successfully and practically implementing the new guidelines.

CONTACT US FOR A FREE CONSULTATION

contact@intellisecure.co | +65 9180 1882

Manish Chawda
Founder
+65 9180 1882
manish@intellisecure.co

About IntelliSecure | www.Intellisecure.co
IntelliSecure is a cybersecurity consultancy with an experienced team that offers Cyber and Regulatory Consultancy.

GLOSSARY

These are some terminologies highlighted in the revised MAS TRM Guidelines 2021 that reflect digital transformations globally.

Agile software development is based on an iterative and incremental model to accelerate software development and delivery to meet business and customer needs. When adopting Agile software development methods, the FI should continue incorporating the necessary SDLC and Security-by-Design principles throughout its Agile process.

Application Programming Interfaces (APIs) are sets of protocols that define how one application interacts with another, usually to facilitate an information exchange.

Behavioural Analytics is a form of analytics that focuses on transactions or payments that exhibit behaviour that deviates significantly from a customer's usual usage behaviours or abnormal system activities.

Bring Your Own Device (BYOD) enables staff to access corporate email, calendars, applications and data from their personal mobile devices.

Confidentiality, Integrity and Availability (CIA) triad is at the heart of information security. Confidentiality refers to an organisation's efforts to ensure information is not made available or disclosed to unauthorised individuals, entities, or processes. Integrity refers to the accuracy and completeness of the data over its entire life cycle. Availability refers to the constant availability of resources and services to only authorised parties promptly.

The Chief Information Officer (CIO) / Chief Technology Officer (CTO) / Head of Information Technology is principally responsible for establishing and implementing the overall information technology strategy, overseeing the day-to-day information technology operations, and managing the financial institution's information technology risks.

The chief information security officer (CISO) or "Head of Information Security" is principally responsible for the FI's information security strategy and programme, including, but not limited to, information security policies and procedures to safeguard information assets, information security controls, and information security management.

DevSecOps is the practice of automating and integrating IT operations, quality assurance, and security practices into the software development process. It constitutes continuous integration, delivery and IT security practices for frequent, efficient, reliable and secure software product development, testing and release. The FI should ensure its DevSecOps activities and processes are aligned with its SDLC framework and IT Service Management processes.

An information asset is any data, hardware or software owned by the FI. However, information assets are not limited to those owned by the FI. They also include those entrusted to the FI by customers or third parties, rented or leased by the FI, and used by service providers to deliver their services to the FI.

The Internet of Things (IoT) includes any electronic device, such as smartphones, multi-function printers, security cameras and smart televisions, that can be connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, including information such as the networks they are connected to and their physical locations.

Jailbreaking or Rooting is the process of allowing users to attain privileged control over smartphone operating systems. This allows a user to alter or replace system applications and settings and run specialised applications requiring administrator-level permissions. A rooted device is more vulnerable to threats.

GLOSSARY

Multi-Factor Authentication (MFA) refers to the use of two or more factors to verify a user's claimed identity. Such factors include, but are not limited to:

a) something that the user knows such as a password or a PIN;

b) something that the user has such as a cryptographic identification device or token;

c) and something that the user is such as his biometrics or behaviour.

Outsourcing is the practice of hiring a party outside an organisation to perform services which would otherwise be performed in-house by the employees of an organisation.

Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications.

A risk owner is a person/entity responsible for the mitigation of an individual risk.

Recovery Point Objective (RPO) describes the recovery point to which an enterprise's operations must be restored following a disruptive event.

Recovery Time Objective (RTO) is the maximum acceptable amount of time for restoring a network or application and regaining access to data after an unplanned disruption.

Virtualisation is the simulation of the software or hardware upon which other software runs. This simulated environment is called a virtual machine.

Virtual Private Network (VPN) is an encrypted connection over a public network between two endpoints. This allows the sensitive transmission of data and prevents unauthorised access to the data in motion.

Waterfall Model is a sequential model that divides software development into pre-defined phases, often including requirement analysis, system design, implementation, system testing, system development and system maintenance.