MAS TRM GUIDELINES

THE ULTIMATE AUTHORITY ON FINANCIAL SERVICES SECURITY

RISK-BASED SECURITY INTELLIGENCE SOLUTIONS

EXECUTIVE OVERVIEW

The Monetary Authority of Singapore (MAS) is viewed as the world's banking and financial services authority—every major financial services market around the world, from Hong Kong to New York to London, adopts the guidelines it issues. Recently, MAS issued innovative new legislation, the Technology Risk Management (TRM) guidelines, which will completely change security regulations and compliance for the financial services industry. Every major global bank either has a branch in Singapore or does business with a financial institution in Singapore, and all divisions of these banks and their business partners doing business in Singapore must comply with the new guidelines.

Previous MAS guidelines have used a traditional compliance and threat hygiene framework, with the primary focus on security controls and best practices. The new guidelines are fundamentally different, going beyond compliance and threat frameworks. They instead provide comprehensive coverage of credit, market, operational and technology risks, internal controls and risks related to insurance businesses. They also define the roles and responsibility of an institution's Board of Directors (Board) and senior management in risk management and mitigation.

The new guidelines go into effect in July 2014, with annual audits starting in 2015. The general consensus is that these guidelines will be adopted far more broadly than the current guidelines and they they have the potential to change the very fabric of the financial services industry. In large part, this belief is based on a much more holistic approach to risk as well as a dramatic increase in impact and scope of the guidelines. Previous regulation only applied to banks and Internet banking; the new TRM guidelines apply to all financial institutions that the MAS licenses, approves or regulates. The impact of non-compliance could include loss of license to operate in Singapore and the potential loss of business in other key financial markets. In short, a lack of compliance has the potential to directly impact a financial institution's bottom line.

Almost all organizations in the financial services industry will be significantly impacted by the guidelines requirements. Compared to previous MAS guidelines, the TRM requires dramatic changes in organizational risk awareness and accountability, an unprecedented level of system availability, and near real time security incident detection and response. The guidelines now view "incidents" as not only security and data breaches, but also slowdowns or disruptions of critical systems. Therefore, an unprecedented level of integration between IT operations and IT security will be necessary.

Globally, the TRM guidelines are set to become the ultimate authority on security and availability preparedness. Given the significant operational and business process changes involved in the new guidelines as well as the impact they will have on organizational operations and structure, financial institutions are advised to begin examining their processes and capabilities this year. By starting early, they can identify gaps from the expected baseline, construct a plan to fill those gaps and prepare for the upcoming compliance audits.

AN OVERVIEW OF MAS SECURITY ADVISORIES AND GUIDELINES

The world recognizes Singapore as a hub for international banking and finance. As Singapore's central bank, the Monetary Authority of Singapore (MAS) strives to ensure that those conducting financial dealings in Singapore can do so with confidence in the security and reliability of those transactions. Only with such assurances can Singapore continue to hold its leadership role in the world of finance.

The MAS understood the importance of providing these assurances and has long provided security advisories and guidelines for financial institutions that conduct business with or have established institutions in Singapore. Previously released security advisories focused on threats (such as phishing and spyware) and the risks associated with outsourcing technology to third party providers. Other MAS guidelines recommended best practices on outsourcing technology, risk management and business continuity planning.

In 2001, the MAS released the Internet Banking Technology Risk Management (IBTRM) guidelines, which provided critical security and risk management guidance to banks deploying Internet banking solutions to customers. Since then the MAS has periodically updated the IBTRM to keep pace with evolving security risks, threats and the underlying technology and processes that support online banking.

Over the last decade, however, Internet banking has become ubiquitous. Customers now perform online banking and pay bills from mobile devices, conduct trading on-line and use web-based insurance portals, while financial institutions now store customer and transactional data in the cloud. These changes make the technology systems that support the financial services industry both increasingly complex and more vulnerable to cyberattacks such as phishing, identity theft, man-in-the-middle attacks and others.

In response to these changes in the financial services industry, in June 2013 the MAS released the Technology Risk Management (TRM) guidelines, a fundamentally new set of guidelines that replace and supersede the IBTRM.

THE MAS TRM GUIDELINES

The MAS TRM represents a significant shift from all previous security guidelines. To begin with, the reach of the guidelines now extends beyond online banking services to all financial services, including banking, financial advisors and fund managers, trust companies, money changers, remittance agents, money brokers, insurance providers and brokers and payment systems operators. The guidelines also take a much broader view of risk by incorporating all elements of a financial transaction—even those outsourced to third parties.

Many view the TRM as the ultimate authority on risk management in the financial industry, believing it to have a far greater impact than the Payment Card Industry Data Security Standard (PCI) on a financial institution's ability to do business in the financial sector. In addition to extending its reach to all financial institutions, the TRM introduces fundamental changes in two main ways: it clarifies an organization's accountability and responsibility for financial transactions, and includes new, more stringent technology requirements.

STRONG EMPHASIS ON ACCOUNTABILITY AND RESPONSIBILITY

Perhaps the single biggest change in the TRM guidelines is its emphasis on accountability and responsibility. The new guidelines elevate responsibility for security risk management and mitigation to the executive and board level.

With executives and the board clearly designated as responsible for security risks, the traditionally poor communications between IT security, operations and the executive team will have to improve. To meet the guidelines these groups will have to regularly hold more detailed and nuanced conversations about security risk. They'll also have to work together to create internal metrics that reflect the organization's security risk from an operations standpoint.

The TRM also addresses another key issue: outsourcing. Financial institutions often outsource part or all of a financial transaction to a third party partner that likely is not subject to previous guidelines. In the past, financial institutions were not responsible for the compliance of those third parties, but the TRM closes that loophole—they will soon be responsible for the security risks of the complete transaction, even if partly outsourced.

NEW TECHNOLOGY FOCUS AREAS

The TRM also adds new technology guidelines that further necessitate the integration of IT operations and security. Whereas most organizations have two different teams for these functions, with their own goals and objectives, under the TRM operational risk and security risk are no longer viewed separately. System downtime and system slowdowns are both viewed as incidents, and both are subject to the same reporting guidelines as security incidents.

New guidelines require near real-time detection of security incidents and fast forensics and reporting after the incident. The guidelines mandate that organizations:

- Establish a framework and process to identify critical systems for their operations
- Ensure high availability of those critical systems, with a maximum window of four hours of downtime for each critical system in a 12-month period
- Meet recovery time objectives for disrupted or unavailable critical systems, with a maximum window of four hours allowed from point of disruption to restoration
- Report security incidents to the MAS within one hour when incidents have a widespread or material impact on the financial institution or its customers
- Submit a detailed root cause and impact analysis to the MAS no later than 14 days after a breach
- Implement IT controls to protect customer information from unauthorized access or disclosure

ENFORCING THE TRM

As of July 1, 2014, trained TRM auditors will assess financial institutions against a checklist of 12 notices. Institutions are assessed as having "Full Compliance," "Partial Compliance," "Non-compliance" or "NA" (if the requirement does not apply). When the institution selects anything other than "Full Compliance," it must explain why in the associated "Comments" column—along with mitigation plans for each issue.

While the TRM guidelines are not legally binding, the 12 notices from MAS that specify the guidelines are. A financial institution that fails the audit or outsources to an organization that fails an audit may have its license revoked and be prevented from conducting financial business in Singapore until they can achieve compliance. Given the heightened responsibility and accountability specified for executives and the board, these individuals will have a personal stake in meeting compliance. Ultimately, it comes down to this: no financial institution—or its leadership—can afford to lose business routed through Singapore and other key financial markets.

PREPARING TO COMPLY WITH GAME-CHANGING GUIDELINES

The TRM guidelines represent a game-changer for the financial services industry. They expand compliance for all financial institutions, raise accountability and clearly identify the board and company executives as the responsible parties for the security and reliability of the entire financial transaction, close outsourcing loopholes and specify new, more stringent technology requirements. The TRM guidelines set an extremely high bar for financial institutions; the general sentiment globally is that they will serve as the ultimate authority on security and availability in the finance sector.

With audits for TRM compliance starting so soon, financial institutions have their work cut out, especially for those organizations that have not previously been subject to MAS security guidelines. As a key first step, financial institutions are advised to evaluate their current processes and capabilities and identify gaps they must fill to meet the TRM. They can then begin building a plan that addresses any identified gaps and ensures that they are well-prepared for the upcoming compliance audits. As a result they can provide their customers highly reliable and secure financial services.

HOW TRIPWIRE HELPS MEET THE RECOMMENDATIONS

Tripwire helps financial institutions meet many key areas of the TRM guidelines through Tripwire's industry-leading security configuration management, vulnerability management, and log intelligence solutions. In addition, Tripwire's professional services team has already helped some of the largest banks in Singapore develop secure configurations that pass many of the security configuration management requirements.

TRIPWIRE ENTERPRISE & TRIPWIRE CONFIGURATION COMPLIANCE MANAGER

Award-winning security configuration management solutions Tripwire® Enterprise and Tripwire Configuration Compliance Manager™ (CCM) primarily help address requirements in sections 4 (Technology risk management framework), 6 (Acquisition and development of information systems) and 9 (Operational infrastructure security management). These solutions also provide some assistance with requirements in sections 7 (IT service management), 11 (Access control) and 13 (Payment card security).

Asset tagging in Tripwire Enterprise lets organizations assign business-relevant tags to IT assets. For example, they can tag IT assets by criticality level, location or function. Asset tagging helps financial institutions meet requirements in section 4 of the TRM, by providing a framework that identifies critical systems as well as a method to report on the security and operational state of those systems.

In addition, Tripwire Enterprise/CCM provides security teams an out-of-the box security configuration policy that fully meets the TRM requirement

Tripwire IT Security Solutions

Tripwire helps organizations around the world address their IT security and risk and compliance needs with industry-recognized solutions that include:

- Tripwire Enterprise and Tripwire Configuration Compliance Manager for security configuration management
- Tripwire IP360 with Tripwire WebApp360 and Tripwire PureCloud Enterprise for enterprise vulnerability management
- Tripwire Log Center for log intelligence

6.2.1. Tripwire customers can apply this policy to systems under development or being acquired and use automation to continuously verify that critical systems maintain continuous compliance with the TRM.

Tripwire Enterprise also identifies and alerts IT to unauthorized changes, including those that cause system slowdowns, service disruption and breaches. These alerts allow IT to promptly identify and report security events. Because Tripwire Enterprise provides real-time evidence on what changed, when it changed and who made the change, operations can understand the incident's root cause and recover quickly in order to meet TRM recovery time objectives. This detailed evidence also provides critical input for the root cause analysis report required by the TRM. Together, these capabilities meet the requirement for ensuring high availability of critical systems.

TRIPWIRE IP360 (WITH TRIPWIRE WEBAPP360 AND PURECLOUD ENTERPRISE)

Tripwire IP360™, a global-leading vulnerability and risk management solution, complements Tripwire Enterprise by addressing additional requirements in sections 4, 6, 9 and 11. For example, Tripwire IP360 squarely and completely addresses requirement 9.4.1, which requires the institution to regularly conduct vulnerability assessments to detect vulnerabilities in the IT environment.

TRIPWIRE LOG CENTER

Tripwire Log Center®, a powerful log intelligence system, also complements the Tripwire set of vulnerability and security compliance solutions for addressing the TRM. Tripwire Log Center detects threats and breaches through automated collection and analysis of activity logs. Tripwire Log Center meets many requirements in sections 4 and 9, with partial coverage for sections 7 and 11. For example, requirement 9.6.4 requires the use of real-time monitoring tools on critical systems and applications to detect malicious activities.

COMBINED TRIPWIRE SOLUTIONS PROVIDE GREATER TRM COVERAGE

While each Tripwire solution addresses many of individual TRM requirements, when used together they almost completely address sections 4 and 9 and significant portions of sections 6, 7, 11 and 12. Collectively, the security information these solutions provide can more definitively identify "super events"—those security incidents that warrant immediate investigation because all signals indicate an attack is in progress or a breach has occured.

Tripwire analytics solutions provide even greater insight into the institution's security and compliance status and better ways to communicate that status. Tripwire Data Mart lets security teams create reports and dashboards that provide intuitive, executive-level visibility into the cost, performance and efficiency of all their Tripwire IT security controls, while Tripwire Security Intelligence Hub (SIH) provides audit-ready reporting from Tripwire IP360 and Tripwire CCM.

TRIPWIRE AND THE TRM CHECKLIST

Because no single vendor provides a complete TRM compliance solution, financial institutions will need to combine several solutions to address the full range of requirements outlined in the sections and subsections of the guidelines. The following table indicates the degree to which Tripwire industry-leading security and compliance solutions help financial institutions meet compliance with the various sections of the TRM.

TRM REQUIREMENT SECTION/APPENDIX	
Section 3: Oversight of technology risks by board of directors and senior management	
Section 4: Technology risk management framework	●
Section 5: Management of IT outsourcing risks	
Section 6: Acquisition and development of information systems	◑
Section 7: IT service management	◑
Section 8: Systems reliability, availability and recoverability	
Section 9: Operational infrastructure security management	◕
Section 10: Data centres protection and controls	
Section 11: Access control	◑
Section 12: Online financial services	◑
Section 13: Payment card security (automated teller machines, credit and debit cards)	◔
Section 14: IT audit	
Appendix A: Systems security testing and source code review	◔
Appendix B: Storage system resiliency	
Appendix C: Cryptography	
Appendix D: Distributed denial-of-service protection	
Appendix E: Security measures for online systems	◔
Appendix F: Customer protection and education	