# BeyondTrust MAS TRM

## Value

Effective as of July 2014, the Monetary Authority of Singapore (MAS) has imposed updated Technology Risk Management (TRM) Guidelines on all financial institutions that have any form of operations in the territory, no matter where in the world they are based. At the same time, MAS published several related TRM Notices, which are legally binding. Non-compliance can result in the following for financial institutions:

- Financial penalties
- Reputational damage
- Revocation of licence to operate in Singapore

Previously only applying to banks with online operations, the guidelines were updated to address the need for all financial institutions to adopt sound operational practices for managing technology risks, given factors including:

- Reliance on increasingly complex IT systems
- Recent, high-profile security incidents and system failures
- Emerging technology risks such as the increased use of mobile devices and virtual environments
- Growing concern regarding risks posed by rogue insiders

The updated guidelines are intended to ensure that all financial institutions manage risk in a way that supports MAS' approach of promoting a sound and progressive financial services sector. They aim to ensure that every financial institution establishes a sound and robust technology risk management framework by ensuring that technology controls are effective and resilient. They place a focus not only on resiliency, but also on availability and recoverability in the case of a serious security incident or systems outage. Further, they place an emphasis on ensuring that customers and sensitive data are adequately protected.

The TRM Guidelines specify technology processes and controls that financial institutions should implement in a range of functional areas, including risk management oversight and framework, system reliability, availability and recoverability, access control, provision of online services, and payment mechanisms. The guidelines are broad and detailed—to a level previously only seen in the PCI DSS industry standards.

## Features

BeyondTrust offers an integrated IT Risk Management Platform that helps financial institutions in their compliance efforts across two key areas:

- Privileged account management to enforce least-privilege best practices and provide the access employees need to perform their jobs safely, without obstructing IT or end-user productivity
- Vulnerability management to identify exposures, analyse business impact, and plan and conduct remediation across diverse IT infrastructure


Company Details

**BeyondTrust**

**North America HQ:** +1 818.575.4000
**EMEA Office:** +44 1133 970 445
**Singapore Office:** +65 6701 8267
**Email:** info@beyondtrust.com
**Twitter:** @beyondtrust
**Facebook:** facebook.com/beyondtrust
**LinkedIn:** linkedin.com.company/beyondtrust


The company's best-of-breed solutions in these areas can be deployed independently or combined as modules within BeyondInsight—a standard platform for centralised management, reporting and analytics.

### Privileged account management: PowerBroker

The TRM Guidelines specifically call out the need for privileged account management—both throughout the guidelines as well as in a specific section of the document—to limit IT access to key systems, applications and data. Within this, it describes three basic principles for protecting systems:

- Never alone principle—procedures for handling the most sensitive and critical functions should be carried out by more than one person
- Segregation of duties—certain functions must be separated and performed by different groups of employees
- Access control—access rights and system privileges should be granted based on job responsibility and should only be sufficient for the duties that a person has to fulfil

BeyondTrust offers a broad set of integrated PowerBroker solutions for addressing the TRM Guidelines for privileged account management, including:

- Privilege management for delegating server and desktop privileges without exposing passwords
- Privileged password management for delegating and auditing privileged access to servers
- Active Directory bridging to extend Active Directory and group policy to non-Windows platforms
- Auditing and protection for auditing access and system changes to Active Directory, Exchange, file system and SQL

### Vulnerability management: Retina

Much emphasis is placed on the management of risks and vulnerabilities across all IT systems in the TRM Guidelines. This requires that organisations be able to identify threats and vulnerabilities, prioritise and manage remediation, and report on risk. Functionality needed includes scanning and monitoring of the entire infrastructure, including network, virtual, web and cloud environments.

BeyondTrust's vulnerability management products satisfy a number of the key requirements included in the TRM Guidelines, including:

- Protection of information system assets—including prioritisation according to criticality
- Risk identification, assessment and treatment—including the likelihood of specific internal and external risks occurring and the consequences should they occur
- Risk monitoring and reporting—to enable continuous assessment of the risk profile
- Security requirements and testing—to ensure the integrity and recoverability of all network assets
- Network and security configuration management—to establish baseline standards and ensure compliance
- Vulnerability assessment testing using both automated tools and manual techniques
- Patch management—including rigorous testing of patches before deployment
- Security monitoring—to facilitate prompt detection of unauthorised or malicious activities by internal or external actors

## Conclusions

The updated TRM Guidelines—and associated legal notices that provide for sanctions in the case of non-compliance—are intended to ensure that all financial institutions establish a sound and robust technology risk management framework that is secure, reliable and resilient so that all customer data, transactions and systems are protected. Recoverability from a disaster is a core component and is key to avoiding sanctions. The deadline for compliance is now and all financial institutions with any kind of dealings in Singapore must ensure that they are prepared.