Avecto Whitepaper

Compliance series

Guide to meeting requirements of MAS

Contents

Introduction to MAS TRM

To address the changing threat landscape and new ways of doing business, the Monetary Authority of Singapore has issued its Technology Risk Management document to supersede advice that was previously available as the Internet Banking Technology Risk Management guidelines.

The Internet Banking Technology Risk Management (IBTRM) guidelines were first published by MAS in 2001 to help provide banks with a risk management framework for providing Internet services. A high profile hacking incident led MAS to reissue the guidelines in 2003, and were updated again in 2008 to version 3.0. In June 2012, MAS began a consultation process to revise the guidelines once more, including a Notice on Technology Risk Management paper, which stipulates various legal requirements. Prior to the public consultation in 2012, a workgroup of IT security experts and specialists from major financial institutions helped to draft the new guidelines.

TRM guidelines overview

The Technology Risk Management guidelines and legal notice will apply to all financial institutions, not just banks. Furthermore, the new guidelines apply to all IT systems; unlike IBTRM, which was relevant only for systems used to provide online services. Additionally, the legal notice will allow MAS to impose a financial penalty on institutions that don't comply with the TRM guidelines.

TRM includes new and updated advice for data centers, mobile banking, payment security, payment card system, ATM security, cyber threats and customer protection and education. Information on IT outsourcing, endpoint security, data protection, systems reliability, resiliency and recoverability have been combined into a single document to make it easier to find the relevant information.

Data confidentiality and system integrity, and specific requirements—such as limiting exposure to cyber and man-in-the-middle attacks—are covered in detail in the document and are difficult to achieve if least privilege security is not utilized on end user systems and servers.

> "Data confidentiality and system integrity, such as limiting exposure to cyber and man-inthe-middle attacks are difficult to achieve if least privilege security is not utilized on end user systems and servers."

Microsoft Certified Systems Engineer (MCSE)

Legal notice

The legal notice requires that financial institutions under the jurisdiction of MAS manage critical systems in such a way as to protect customer information and provide a high level of integrity and reliability. Some of the main points of the notice include:

- Identify critical systems
- MAS must be informed within 30 minutes of any critical system failure or hacking incident
- The financial institution shall implement IT controls to protect customer information from unauthorized access or disclosure

Privileged access management

The TRM document refers to least privilege security throughout and has a section dedicated to privileged access management. There's common-sense advice on the basics of privilege management, including restricting the number of privileged accounts, granting privileged access on a 'need-to-have' basis and disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring.

Insiders are singled out as a threat to information security and system availability, with common tactics used to disrupt operations being logic bombs, stealth scripts and cracking passwords. Staff with privileged access, such as system administrators, are in a good position to implement these attack methods, and therefore should be carefully vetted before being trusted with highly-privileged access and closely monitored.

11.0.1c Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfil one's duties.

The TRM guidelines also describe the 'never alone' principle, which should be incorporated into business processes so that at least two people must be present to ensure that actions are carried out according to policy; for example, the use of privileged accounts on highly-sensitive systems. Never alone functionality can be achieved with the help of challenge/response authentication or enforcing a process to be authorized by a second user before it can be run.

> "The TRM document refers to least privilege security throughout and has a section dedicated to privileged access management."
>
> Microsoft Certified Systems Engineer (MCSE)

Any privilege management solution used for compliance should be tamper-proof so that users can't disable the management software or otherwise modify assigned privileges. Furthermore, there must be assurance that access policies have not been modified before being applied.

User access

While system administrators and external contractors often have access to privileged accounts, other employees can also pose a significant risk, especially if granted privileged access to devices from which sensitive data is accessed.

11.1.1 User access to IT systems and networks should only be granted on a need-to-use basis and within the period when the access is required. All requests to access IT resources must be duly authorised and approved by the resource owner.

Occasionally, users – or applications if a privilege management solution is deployed - are granted elevated privileges on a semipermanent basis for a legitimate reason, but these privileges are rarely reviewed and revoked as appropriate. MAS requires that all privileges be regularly assessed to ensure that they are still appropriately assigned.

Auditing and logging

Auditing privileged access and monitoring log files is an important part of the TRM guidelines, and it's stressed that users must not be given access to logs which are used to collect audit information on their own activity. Likewise, users should not have concurrent access to production and backup systems. Simple points like these are regularly overlooked. External users and contractors must be monitored closely, and auditing of their activity carefully logged and observed to ensure system and data integrity.

"Any privilege management solution used for compliance should be tamper-proof so that users can't disable the management software or otherwise modify assigned privileges."

Microsoft Certified Systems Engineer (MCSE)

Defendpoint helps businesses achieve MAS compliance

While there are some privilege management functions built-in to Windows in the form of User Account Control (UAC), this technology is largely intended to protect home and small business users from themselves, in the absence of IT support and a properly managed environment. UAC requires that users have permanent access to an account with administrator-level access, thus enabling them to elevate privileges on demand and without approval from IT.

Avecto Defendpoint enables IT departments to implement more granular control over privilege use by eliminating the need for employees to have permanent access to an administrator account and to elevate applications and processes instead. Elevation might be required to run legacy business applications or Windows features. Defendpoint includes comprehensive auditing capabilities, including Enterprise Reporting. Elevation prompts can be customized with company logos, hyperlinks and there's also multilingual support.

Not only can Defendpoint enable financial institutions to meet the privileged management access requirements of the TRM guidelines and other industry mandates, but it goes even further by providing additional functionality, such as application whitelisting for blocking unauthorized applications and scripts, and challenge/response authentication, which allows organizations to respond quickly to changing needs and remote users. With Avecto Defendpoint installed on end user devices and servers, you can be sure that privilege access is managed by policies set by the business, and access events can be monitored to comply with the TRM guidelines. The implementation of least privilege security on desktops and servers is essential for securing enterprise IT systems and complying with all major industry regulations.

“ The implementation of least privilege security on desktops and servers is essential for securing enterprise IT systems and complying with all major industry regulations. ”

Microsoft Certified Systems Engineer (MCSE)

About Avecto

Avecto is an innovator in endpoint security.

Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development