Monetary Authority of Singapore's (MAS) Technology Risk Management (TRM) Guidelines

MAS TRM GUIDELINES	Network Security	Compliance Monitor	Authority Broker	Interact	DataThread	StandGuard Anti-Virus	Command Security
6.2 Security Requirements and Testing							
6.2.1 The financial institution (FI) should clearly specify security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking, and exception handling in the early phase of system development or acquisition. The FI should also perform a compliance check on the FI's security standards against the relevant statutory requirements.	◉	◉		◉	◉		
9.3 Networks and Security Configuration Management							
9.3.3 The FI should deploy anti-virus software to servers, if applicable, and workstations. The FI should regularly update anti-virus definition files and schedule automatic anti-virus scanning on servers and workstations on a regular basis.						◉	
9.6 Security Monitoring							
9.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorised or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.	◉	◉					
9.6.2 The FI should implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the FI against network intrusion attacks, as well as provide alerts when an intrusion occurs.	◉			◉			
9.6.3 The FI should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs to facilitate the identification of unauthorised changes.			◉		◉		
9.6.4 The FI should perform real-time monitoring of security events for critical systems and applications to facilitate the prompt detection of malicious activities on these systems and applications.				◉			
9.6.5 The FI should regularly review security logs of systems, applications, and network devices for anomalies.		◉					
9.6.6 The FI should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, the FI should take into account statutory requirements for document retention and protection.		◉					

The PowerTech Group, Inc.
www.powertech.com • info@powertech.com
TEL U.S. +1 253-872-7788
TEL AP +61 (3) 9558 6366

MAS TRM GUIDELINES (CONTINUED)	Network Security	Compliance Monitor	Authority Broker	Interact	DataThread	StandGuard Anti-Virus	Command Security
11.0 Access Control							
c. Access control principle — The FI should only grant access rights and system privileges based on job responsibility and the necessity to have them to fulfil one's duties. The FI should check that no person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources, or facilities. The FI should only allow staff with proper authorisation to access confidential information and use system resources solely for legitimate purposes.	◎		◎		◎		◎
11.1 User Access Management							
11.1.1 The FI should only grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. The FI should ensure that the resource owner duly authorises and approves all requests to access IT resources.	◎		◎				◎
11.1.2 Employees of vendors or service providers, who are given authorised access to the FI's critical systems and other computer resources, pose similar risks as the FI's internal staff. The FI should subject these external employees to close supervision, monitoring, and access restrictions similar to those expected of its own staff.	◎	◎	◎				◎
11.1.3 For accountability and identification of unauthorised access, the FI should ensure that records of user access are uniquely identified and logged for audit and review purposes.	◎	◎	◎				
11.1.4 The FI should perform regular reviews of user access privileges to verify that privileges are granted appropriately and according to the "least privilege" principle. The process may facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access.		◎	◎				
11.1.5 Passwords represent the first line of defence, and if not implemented appropriately, they can be the weakest link in the organisation. Thus, the FI should enforce strong password controls over users' access to applications and systems. Password controls should include a change of password upon first logon, minimum password length and history, password complexity, as well as maximum validity period. [1]		◎					
11.1.6 The FI should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. The FI should also ensure that any person who needs to access backup files or system recovery resources is duly authorised for a specific reason and a specified time only. The FI should only grant access for a specific purpose and for a defined period.		◎	◎				

1. The IBM OS does the enforcement; HelpSystems can report on the current state and compare it to a desirable baseline policy. It also reports on whether there are default passwords present.

MAS TRM GUIDELINES (CONTINUED)	Network Security	Compliance Monitor	Authority Broker	Interact	DataThread	StandGuard Anti-Virus	Command Security
11.2 Privileged Access Management							
11.2.2 Some common tactics used by insiders to disrupt operations include planting logic bombs, installing stealth scripts, and creating system backdoors to gain unauthorised access, as well as sniffing and cracking passwords. System administrators, IT security officers, programmers, and staff performing critical operations invariably possess the capability to inflict severe damage on critical systems they maintain or operate by virtue of their job functions and privileged access.	◎	◎	◎				
11.2.3 The FI should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. The FI should adopt the following controls and security practices:							
a. Implement strong authentication mechanisms such as two-factor authentication for privileged users			◎				
b. Institute strong controls over remote access by privileged users	◎						
c. Restrict the number of privileged users	◎	◎	◎				
d. Grant privileged access on a "need-to-have" basis	◎		◎				
e. Maintain audit logging of system activities performed by privileged users	◎	◎	◎				
f. Disallow privileged users from accessing systems logs in which their activities are being captured			◎				
g. Review privileged users' activities on a timely basis		◎	◎				
h. Prohibit sharing of privileged accounts			◎				
i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring	◎		◎				◎
j. Protect backup data from unauthorised access	◎		◎				