netwrix

Risk Management in Technology (RMiT)

In common with other financial markets around the world, the Bank Negara Malaysia has taken a lead in defining a stringent security controls framework for Malaysian financial institutions. Sustained, APT attacks on the banking industry such as the Carbanak hack shook the banking world. This coordinated and sophisticated attack really was a wake-up call to banks that cyber-crime was becoming more organized and effective. Carbanak not only resulted in core banking systems being infiltrated allowing fraudulent electronic fund transfers to be used, but ATM systems were also hacked to allow cash to be stolen directly.

The RMiT provides clear guidance for minimum expected standards in cyber security and serves to provide a level of confidence within the market, covering everything from the data center to the ATM/SST.

Banking and finance is always a high-risk industry with respect to hackers and it is crucial that awareness of threats is always maintained and new technological innovations are being utilized, for example, leveraging One Time Passwords (OTP) to reduce the opportunity for fraudulent transactions.

Significantly, the RMiT is very clear in placing responsibility at Board level for an understanding of the ‘financial institution’s risk appetite’ and its ‘corresponding risk tolerances for technology-related events’. Furthermore it is also a board-level responsibility to ensure an ‘effective implementation of a sound and robust technology risk management framework (TRMF) and cyber resilience framework (CRF), for the financial institution to ensure the continuity of operations and delivery of financial services’

Timeline

- October 2019 Internal gap analysis results to be submitted by all financial institutions
- January 1, 2020 RMiT is now effective and compulsory for all organizations
- December 31, 2022 or whenever there is a ‘material change in the data centre infrastructure’ External audit required of Data Centre and Network Resilience.

In other words, external audits are required regularly and at least every 3 years. But like all cyber security controls, the real need is to operate security best practices continuously and as embedded processes.

Netwrix Solution for RMiT

Netwrix solutions portfolio is carefully assembled so that, when used in a coordinated fashion as part of an overall security controls framework, all key controls are automated and utilized to maximum effect.

Netwrix delivers Secure Operations. It includes a combination of the essential, foundational security controls as prescribed by all leading security frameworks such as The CIS and NIST – and of course, RMiT too - with the operational discipline of change management and the innovation of change control, pioneered by Netwrix.
By ensuring the basic and essential security controls are in place, combined with the ability to validate the safety of all changes, organizations can prevent and protect against cyber-attack while improving IT Service Delivery quality.

Netwrix solution includes:

- Asset discovery and Inventory
- Secure system configuration for all assets
- Regular vulnerability scanning
- Change monitoring and control
- Whitelist approved File Integrity Monitoring
- Integration with operational Change Management process and systems
- Security Information and Event Log Management (SIEM)

netwrix

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:	PHONES:
6160 Warren Parkway, Suite 100 Frisco, TX, US 75034	1-949-407-5125 Toll-free (USA): 888-638-9749
565 Metro Place S, Suite 400 Dublin, OH 43017	1-201-490-8840
5 New Street Square London EC4A 3TW	+44 (0) 203 588 3023

OTHER LOCATIONS:	
Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social