netwrix

Saudi Arabian Monetary Authority: Cyber Security Framework

Saudi Arabian Monetary Authority

3.2 Cyber Security Risk Management and Compliance				
3.2.3 Compliance with (inter)national industry standards	Principle: The Member Organization should comply with mandatory (inter)national industry standards.	Objective: To comply with mandatory (inter)national industry standards.	Control considerations 1. The Member Organization should comply with: a. **Payment Card Industry Data Security Standard (PCI-DSS);** b. EMV (Europay, MasterCard and Visa) technical standard; c. **SWIFT Customer Security Controls Framework – March 2017.**	Using Netwrix Change Tracker, FAST Cloud, Netwrix Log Tracker and Greenbone Enterprise will satisfy 45% of total PCI compliance requirements (https://www.netwrix.com/download/documents/PCI_DSS_Requirements.pdf), but with typical implementation times of just a few hours. In addition, Netwrix's solution will enable you to quickly establish the security controls required by the SWIFT Framework.
3.3.3 Asset Management	Principle: The Member Organization should define, approve, implement, communicate and monitor an asset management process, which supports an accurate, up-to-date and unified asset register.	Objective: To support the Member Organization in having an accurate and up-to-date inventory and central insight in the physical / logical location and relevant details of all available information assets, in order to support its processes, such as financial, procurement, IT and cyber security processes.	Control considerations 3. The asset management process should include: a. a unified register; b. ownership and custodianship of information assets; c. the reference to relevant other processes, depending on asset management; d. information asset classification, labeling and handling; e. the discovery of new information assets.	Greenbone Enterprise addresses this security control by providing an accurate inventory of all devices on your network, allowing you to ensure that the devices are authorized with up to date configurations, patches, and appropriate user access controls. Netwrix Change Tracker will track installed software and updates to expose any additions/changes/removals, and identify any drift from the Authorized software list. Greenbone Enterprise will identity all missing or recommended patches and version updates to software products. FAST Cloud provides intervention-less validation of whitelisted files which may be preferred to process blocking technology. Netwrix recommends implementing Netwrix Change Tracker with its integrated ITSM option to assist aligning with SAMA 3-3-3 Control. Greenbone Enterprise and Netwrix Change Tracker can provide direct asset discovery and tracking of any new/changed/removed devices. Netwrix Change Tracker will also integrate with ITSM systems such as ServiceNow, Remedy or Cherwell to leverage CMDB information as an asset inventory source.
3.3.6 Application Security	Principle: The Member Organization should define, approve and implement cyber security standards for application systems. The compliance with these standards should be monitored and the effectiveness of these controls should be measured and periodically evaluated.	Objective: To ensure that sufficient cyber security controls are formally documented and implemented for all applications, and that the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.	Control considerations 5. The application security standard should include: b. the cyber security controls implemented (e.g., configuration parameters, events to monitor and retain [including system access and data], identity and access management) d. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage); e. vulnerability and patch management; g. periodic cyber security compliance review	Netwrix Change Tracker automatically scans all systems on the network continuously to identify all potential configuration-related-vulnerabilities on the organization's systems. Once installed Netwrix Change Tracker agent gathers a comprehensive baseline of all installed software and patches. From this point all changes to existing software and the installation of new software and patches will be tracked. Greenbone Enterprise continuously scans operating systems, network devices and web applications to assign risk rankings for any identified vulnerabilities, with detailed remediation guidance provided. Greenbone Enterprise provides a 'live feed' of any new vulnerabilities identified and relevant tests to expose the existence within the network. Any vulnerabilities identified are reported with full background and remediation guidance.
3.3.7 Change Management	Principle: The Member Organization should define, approve and implement a change management process that controls all changes to information assets. The compliance with the process should be monitored and the effectiveness should be measured and periodically evaluated.	Objective: To ensure that all change in the information assets within the Member Organization follow a strict change control process.	Control considerations 4. The change management process should include: 3. The effectiveness of the cyber security controls within the change management process should be measured and periodically evaluated. 4.The change management process should include: a. cyber security requirements for controlling changes to information assets, such as...the review of changes b. security testing, which should (if applicable) include penetration testing f. post-implementation review of the related cyber security controls h. the procedure for emergency changes and fixes	Greenbone Enterprise can be used for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks and it can also be used for both external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Netwrix's Intelligent change control technology cuts out change noise, which leads to improved operational integrity and protection from all forms of cyberattack, even zero-day threats and ransomware. Functions such as Post-Implementation Reviews, Emergency Changes and the Review of Changes for compliance are all automated.
3.3.8 Infrastructure Security	Principle: The Member Organization should define, approve and implement cyber security standards for their infrastructure components. The compliance with these standards should be monitored and the effectiveness should be measured and periodically evaluated.	Objective: To support that all cyber security controls within the infrastructure are formally documented and the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization	Control considerations: 6. The infrastructure security standard should include: a. the cyber security controls implemented (e.g. configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance); b. the segregation of duties within the infrastructure component (supported with a documented authorization matrix);c. the protection of data aligned with the (agreed) classification scheme(including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage); d. the use of approved software and secure protocols; f. malicious code/software and virus protection (and applying application whitelisting and APT protection); g. vulnerability and patch management; j. periodic cyber security compliance review.	Netwrix Change Tracker is a CIS Certified Vendor solution for assessing and advising on the most secure configuration settings recommended for all platforms, applications and devices. Netwrix Change Tracker will apply CIS Benchmark expert secure configuration analysis to all systems. Detecting and alerting to any suspicious activity that may represent a security or performance threat, Netwrix Change Tracker audits and monitors changes to: - files, file contents, file attributes and folder structures - file secure hash value, to give a unique DNA Fingerprint for each file, essential to detect Trojan malware - running processes (checked against blacklists and whitelists) - Windows registry keys and values - installed applications and patches - local and domain user accounts - services' startup and running states - windows audit and security policy settings - configuration settings for audit and security policy - command line process output, for example a netstat query - open network ports, both UDP and TCP scanned externally on a scheduled basis - enforces CIS Benchmark Checklists for vulnerability mitigation - Username and Process used to make file changes By integrating the FAST Cloud File Whitelist repository, file changes can be automatically and instantly verified as 'known safe' as they are detected.

netwrix

Saudi Arabian Monetary Authority: Cyber Security Framework

مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Authority

3.2 Cyber Security Risk Management and Compliance				
3.3.9 Cryptography	Principle: The use of cryptographic solutions within the Member Organizations should be defined, approved and implemented.	Objective: To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.	Control considerations: 1. A cryptographic security standard should be defined, approved and implemented. 2. The compliance with the cryptographic security standard should be monitored. 3. The effectiveness of the cryptographic security controls should be measured and periodically evaluated. 4. The cryptographic security standard should include: a. an overview of the approved cryptographic solutions and relevant restrictions (e.g., technically, legally); b. the circumstances when the approved cryptographic solutions should be applied; c. the management of encryption keys, including lifecycle management, archiving and recovery.	Netwrix Change Tracker automates CIS Benchmarks auditing for the use of non-encrypted console access methods being enabled, thereafter monitor for any configuration change affecting the devices' hardened state. Greenbone Enterprise will test for weak cryptography algorithms and expired certificates.
3.3.13 Electronic Banking Services	Principle: The Member Organization should define, approve, implement and monitor a cyber security standard for electronic banking services. The effectiveness of this standard should be measured and periodically evaluated.	Objective: To ensure the Member Organization safeguards the confidentiality and integrity of the customer information and transactions.	Control Considerations: 1. The cyber security standards for electronic banking services should be defined, approved and implemented. 2. The compliance with cyber security standards for electronic banking services should be monitored. 3. The effectiveness of the cyber security standard for electronic banking services should be measured and periodically evaluated. 4. Electronic banking services security standard should cover: c. ATMs and POSs: 1. prevention and detection of exploiting the ATM/POS application and infrastructure vulnerabilities (e.g., cables, (USB)-ports, rebooting); 2. cyber security measures, such as hardening of operating systems, malware protection, anti-skimming solutions (hardware/software)	Netwrix Change Tracker is a CIS Certified Vendor solution for assessing and advising on the most secure configuration settings recommended for all platforms, including POS and ATMs. Netwrix Change Tracker will apply CIS Benchmark expert secure configuration analysis to all systems. Detecting and alerting to any suspicious activity that may represent a security or performance threat, Netwrix Change Tracker audits and monitors changes to: files, file contents, file attributes and folder structures - file secure hash value, to give a unique DNA Fingerprint for each file, essential to detect Trojan malware - running processes (checked against blacklists and whitelists) - Windows registry keys and values - installed applications and patches - local and domain user accounts - services' startup and running states - windows audit and security policy settings - configuration settings for audit and security policy - command line process output, for example a netstat query - open network ports, both UDP and TCP scanned externally on a scheduled basis - enforces CIS Benchmark Checklists for vulnerability mitigation - Username and Process used to make file changes
3.3.14 Cyber Security Event Management	Principle: The Member Organization should define, approve and implement a security event management process to analyze operational and security loggings and respond to security events. The effectiveness of this process should be measured and periodically evaluated.	Objective: To ensure timely identification and response to anomalies or suspicious events within regard to information assets.	Control considerations 4. The security event management process should include requirements for: d. resources required continuous security event monitoring activities (24x7) e. detection and handling of malicious code and software f. detection and handling of security or suspicious events and anomalies g. deployment of security network packet analysis solution h. adequately protected logs i. periodic compliance monitoring of applications and infrastructure cyber security standards j. automated and centralized analysis of security loggings and correlation of event or patterns (i.e., Security Information and Event Management (SIEM)) k. reporting of cyber security incidents	With Netwrix Log Tracker all event logs are analyzed and correlated automatically, applying a comprehensive series of rules pertinent to any Security or Governance policy. Any breach of compliance will be alerted immediately allowing pre-emptive action to be taken before a problem arises. Pre-defined rules templates allow you to be in control of compliance, straight out-of-the box. And of course, even subtle hacker activity will be highlighted in real-time using Netwrix Log Tracker SIEM threat detection rules. Netwrix Change Tracker intelligently monitors and analyzes all events in real time leveraging the world's largest repository of independently whitelisted files (FAST Cloud) combined with intelligent and automated planned change rules to significantly reduce typical FIM change noise. Crucially, this will allow you to alert on unusual, unexpected and potentially harmful events along with valuable context such as who made the change and precisely what changed. Netwrix Change Tracker is able to monitor unauthorized changes to files, registry keys and values, directories, processes, services, open ports, and much more.
3.3.16 Threat Management	Principle: The Member Organization should define, approve and implement a threat intelligence management process to identify, assess and understand threats to the Member Organization information assets, using multiple reliable sources. The effectiveness of this process should be measured and periodically evaluated.	Objective: To obtain an adequate understanding of the Member Organization's emerging threat posture.	Control considerations 3. The threat intelligence management process should include: a. the use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tooling, Security Information and Event Monitoring (SIEM), support functions (e.g., Legal, Audit, IT Helpdesk, Forensics, Fraud Management, Risk Management, Compliance);	Netwrix Log Tracker has built-in support for all major GRC standards, protecting customer data and customer privacy to auditor-ready levels. All event logs are analyzed and correlated automatically, applying a comprehensive series of rules pertinent to any Security or Governance policy. Any breach of compliance will be alerted immediately allowing pre-emptive action to be taken before a problem arises. Pre-defined rules templates allow you to be in control of compliance, straight out-of-the box. And of course, even subtle hacker activity will be highlighted in real-time using Netwrix Log Tracker SIEM threat detection rules. Netwrix Change Tracker identifies suspicious activity using highly sophisticated contextual change control underpinned by threat intelligence to spot breach activity while reducing change noise and alert fatigue.
3.3.17 Vulnerability Management	Principle: The Member Organization should define, approve and implement a vulnerability management process for the identification and mitigation of application and infrastructural vulnerabilities. The effectiveness of this process should be measured and the effectiveness should be periodically evaluated.	Objective: To ensure timely identification and effective mitigation of application and infrastructure vulnerabilities in order to reduce the likelihood and business impact for the Member Organization.	Control considerations 3. The vulnerability management process should include: a. all information assets; b. frequency of performing the vulnerability scan (risk-based); c. classification of vulnerabilities; d. defined timelines to mitigate (per classification); e. prioritization for classified information assets; f. patch management and method of deployment.	Netwrix Change Tracker automatically scans all systems on the network continuously to identify all potential configuration-related-vulnerabilities on the organization's systems. Greenbone Enterprise is an Enterprise-class vulnerability scanning solution, automatically running a comprehensive asset discovery, software inventory and configuration audit, assigning risk rankings for any identified vulnerabilities, with detailed remediation guidance provided. Greenbone Enterprise uses a 'live feed' of any new vulnerabilities identified and relevant tests to expose the existence of new threats within the network. Any vulnerabilities identified are reported with full background and remediation guidance.