Sarbanes-Oxley Security Audit: Microsoft Windows Server 2012 R2 Benchmark

27/07/2017 11:36
GEN7-IP18 (169.254.251.115,192.168.1.18)

Compliance Score : 65.78%

271 of 412 rules passed

0 of 412 rules partially passed

141 of 412 rules failed

1 Build and Maintain a Secure Network and Systems: SOX Cyber Security Audit : Install and maintain a firewall

1.1 SOX Cyber Security Audit : Install and maintain a firewall configuration to protect financial data: Corporate Firewall and In-Scope Devices Internal Firewall

1.1.1 SOX Cyber Security Audit : Firewall configuration standards: Track and Approve Config Changes

Rule Name	**Result**
1.1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	Pass: This rule is not automatically assessed. You must implement change tracking and change control for any changes to firewall and router configurations. Use Change Tracker Gen 7 to detect all changes and implement procedures for reviewing and acknowledging Perimeter Firewall Device Events as Planned Changes.

1.2 SOX Cyber Security Audit : Install and maintain a firewall configuration to protect financial data: Windows Server Firewall

1.2.1 SOX Cyber Security Audit : Firewall configuration standards: Windows Firewall With Advanced Security - Domain

Rule Name	**Result**
1.2.1.1 Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)'	Pass: Rule passed : '1'.
1.2.1.2 Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)'	Pass: Rule passed : '1'.
1.2.1.3 Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)'	Fail: Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)' : .'1'. Remediation : To establish the recommended configuration via GP, set the following UI path to Allow (default).Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Outbound connections - Impact:None, this is the default configuration.
1.2.1.4 Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)'	Fail: Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)' : .'1'. Remediation : To establish the recommended configuration via GP, set the following UI path to Yes (default).Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Display a notification - Impact:If you configure this policy setting to Yes, Windows Firewall will display these notifications.
1.2.1.5 Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	Pass: Rule passed : '1'.
1.2.1.6 Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)'	Pass: Rule passed : '1'.
1.2.1.7 Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)'	Pass: Rule passed : '1'.
1.2.1.8 Set 'Windows Firewall: Domain: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	Pass: Rule passed : 'C:\Windows\system32\logfiles\firewall\domainfw.log'.
1.2.1.9 Set 'Windows Firewall: Domain: Logging: Size limit (KB)' to '16,384 KB or greater '	Pass: Rule passed : '16384'.
1.2.1.10 Set 'Windows Firewall: Domain: Logging: Log dropped packets' to 'Yes'	Pass: Rule passed : '1'.
1.2.1.11 Set 'Windows Firewall: Domain: Logging: Log successful connections' to 'Yes'	Pass: Rule passed : '1'.

1.2.2 SOX Cyber Security Audit : Firewall configuration standards: Windows Firewall With Advanced Security - Private Profile

Rule Name	**Result**

1.2.2.1 Set 'Windows Firewall: Private: Firewall state' to 'On (recommended)'	Pass: Rule passed : '1'.
1.2.2.2 Set 'Windows Firewall: Private: Inbound connections' to 'Block (default)'	Pass: Rule passed : '1'.
1.2.2.3 Set 'Windows Firewall: Private: Outbound connections' to 'Allow (default)'	Pass: Rule passed : '0'.
1.2.2.4 Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)'	Fail: Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)' : .'1'. Remediation : To establish the recommended configuration via GP, set the following UI path to Yes (default).Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Display a notification - Impact:If you configure this policy setting to Yes, Windows Firewall will display these notifications.
1.2.2.5 Set 'Windows Firewall: Private: Allow unicast response' to 'No'	Pass: Rule passed : '1'.
1.2.2.6 Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'	Pass: Rule passed : '1'.
1.2.2.7 Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)'	Pass: Rule passed : '1'.
1.2.2.8 Set 'Windows Firewall: Private: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	Pass: Rule passed : 'C:\Windows\system32\logfiles\firewall\privatefw.log'.
1.2.2.9 Set 'Windows Firewall: Private: Logging: Size limit (KB)' to '16,384 KB or greater'	Pass: Rule passed : '16384'.
1.2.2.10 Set 'Windows Firewall: Private: Logging: Log dropped packets' to 'Yes'	Pass: Rule passed : '1'.
1.2.2.11 Set 'Windows Firewall: Private: Logging: Log successful connections' to 'Yes'	Pass: Rule passed : '1'.

1.2.3 SOX Cyber Security Audit : Firewall configuration standards: Windows Firewall With Advanced Security - Public Profile

Rule Name	Result
1.2.3.1 Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)'	Fail: Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)' : .'0'. Remediation : To establish the recommended configuration via GP, set the following UI path to On (recommended).Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Firewall state - Impact:None, this is the default configuration.
1.2.3.2 Set 'Windows Firewall: Public: Inbound connections' to 'Block (default)'	Pass: Rule passed : '1'.
1.2.3.3 Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)'	Pass: Rule passed : '0'.
1.2.3.4 Set 'Windows Firewall: Public: Display a notification' to 'Yes'	Pass: Rule passed : '0'.
1.2.3.5 Set 'Windows Firewall: Public: Allow unicast response' to 'No'	Pass: Rule passed : '1'.
1.2.3.6 Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)'	Fail: Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)' : .'0'. Remediation : To establish the recommended configuration via GP, set the following UI path to Yes (default).Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Apply local firewall rules - Impact:If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.
1.2.3.7 Set 'Windows Firewall: Public: Apply local connection security rules' to 'No'	Pass: Rule passed : '0'.
1.2.3.8 Set 'Windows Firewall: Public: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	Pass: Rule passed : 'C:\Windows\system32\logfiles\firewall\publicfw.log'.
1.2.3.9 Set 'Windows Firewall: Public: Logging: Size limit (KB)' to '16,384 KB or greater'	Pass: Rule passed : '16384'.
1.2.3.10 Set 'Windows Firewall: Public: Logging: Log dropped packets' to 'Yes'	Pass: Rule passed : '1'.
1.2.3.11 Set 'Windows Firewall: Public: Logging: Log successful connections' to 'Yes'	Pass: Rule passed : '1'.

2 Build and Maintain a Secure Network and Systems: SOX Cyber Security Audit : Do not use vendor-supplied defaults

2.1 SOX Cyber Security Audit : Do not use vendor-supplied defaults for system passwords and other security parameters: Develop configuration standards for all system components

2.1.1 SOX Cyber Security Audit : System Hardening - Default User Accounts

Rule Name	Result
2.1.1.1 Set 'Accounts: Guest account status' to 'Disabled'	Pass: Rule passed : securitypolicy (0)'[{oval:org.cisecurity.benchmarks.microsoft_windows_8.1:obj:1051}]'.
2.1.1.2 Configure 'Accounts: Rename administrator account'	Fail: Configure 'Accounts: Rename administrator account' : securitypolicy (2 items: "Administrator", "Administrator"). Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account - Impact:You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.).
2.1.1.3 Configure 'Accounts: Rename guest account'	Fail: Configure 'Accounts: Rename guest account' : securitypolicy (2 items: "Guest", "Guest"). Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account - Impact:There should be little - Impact, because the Guest account is disabled by default.

2.1.2 SOX Cyber Security Audit : System Hardening - Personalization Rules

Rule Name	Result
2.1.2.1 Set 'Enable screen saver' to 'Enabled'	Pass: Rule passed : '1'.
2.1.2.2 Set 'Force specific screen saver: Screen saver executable name' to 'Enabled:scrnsave.scr'	Pass: Rule passed : 'scrnsave.scr'.
2.1.2.3 Set 'Password protect the screen saver' to 'Enabled'	Pass: Rule passed : '1'.

2.1.3 SOX Cyber Security Audit : System Hardening - Attachment Manager Rules

Rule Name	Result
2.1.3.1 Set 'Do not preserve zone information in file attachments' to 'Disabled'	Pass: Rule passed : '2'.

2.2 SOX Cyber Security Audit : System Hardening: Non-Default Services List - Verify that system configuration standards include the following procedures for all types of system components:

2.2.1 SOX Cyber Security Audit : System Hardening: Check for any Non-Default Services

Rule Name	Result
2.2.1.1 Check for any Non-Default Services	Fail: Services installed not covered by Default and Optional services list: TabletInputService (tabletinputservice), AdobeARMservice (adobearmservice).

2.3 SOX Cyber Security Audit : System Hardening: Mandatory Services List - Verify that system configuration standards include the following procedures for all types of system components:

2.3.1 SOX Cyber Security Audit : System Hardening: Mandatory Services List

Rule Name	Result
2.3.1.1 App Readiness Service	
2.3.1.2 Application Experience Service	
2.3.1.3 Application Host Helper Service	
2.3.1.4 Application Identity Service	
2.3.1.5 Application Information Service	
2.3.1.6 Application Layer Gateway Service	Fail: state ALG (stopped), startmode ALG (manual).
2.3.1.7 Application Management Service	Fail: state AppMgmt (running), startmode AppMgmt (manual).
2.3.1.8 AppX Deployment Service (AppXSVC) Service	Fail: state AppXSVC (), startmode AppXSVC ().
2.3.1.9 ASP.NET State Service (aspnet_state) Service	
2.3.1.10 Background Intelligent Transfer Service	
2.3.1.11 Background Tasks Infrastructure (BrokerInfrastructure) Service	
2.3.1.12 Base Filtering Engine Service	
2.3.1.13 Certificate Propagation Service	Fail: state CertPropSvc (running), startmode CertPropSvc (manual).
2.3.1.14 CNG Key Isolation Service	
2.3.1.15 COM+ Event System Service	
2.3.1.16 COM+ System Application Service	Fail: state COMSysApp (stopped), startmode COMSysApp (manual).
2.3.1.17 Computer Browser Service	

2.3.1.18 Credential Manager Service	
2.3.1.19 Cryptographic Services Service	
2.3.1.20 DCOM Server Process Launcher Service	
2.3.1.21 Device Association (deviceassociationservice) Service	Fail: state deviceassociationservice (), startmode deviceassociationservice ().
2.3.1.22 Device Install (deviceinstall) Service	Fail: state deviceinstall (), startmode deviceinstall ().
2.3.1.23 Device Setup (dsmsvc) Service	Fail: state dsmsvc (), startmode dsmsvc ().
2.3.1.24 DHCP Client Service	Fail: state Dhcp (running), startmode Dhcp (auto).
2.3.1.25 Diagnostic Policy Service	Fail: state DPS (running), startmode DPS (auto).
2.3.1.26 Diagnostic Service Host Service	Fail: state WdiServiceHost (stopped), startmode WdiServiceHost (manual).
2.3.1.27 Diagnostic System Host Service	Fail: state WdiSystemHost (stopped), startmode WdiSystemHost (manual).
2.3.1.28 Distributed Link Tracking Client Service	Fail: state TrkWks (running), startmode TrkWks (auto).
2.3.1.29 Distributed Transaction Coordinator Service	Fail: state MSDTC (running), startmode MSDTC (auto).
2.3.1.30 DNS Client Service	
2.3.1.31 The Enhanced Mitigation Experience Toolkit (EMET) Service	Fail: state emet_service (), startmode emet_service ().
2.3.1.32 Encrypting File System (EFS) Service	
2.3.1.33 Extensible Authentication Protocol Service	
2.3.1.34 Function Discovery Provider Host Service	Fail: state fdPHost (stopped), startmode fdPHost (manual).
2.3.1.35 Function Discovery Resource Publication Service	Fail: state FDResPub (stopped), startmode FDResPub (manual).
2.3.1.36 Group Policy Client Service	
2.3.1.37 Health Key and Certificate Management Service	
2.3.1.38 Human Interface Device Access Service	Fail: state hidserv (stopped), startmode hidserv (manual).
2.3.1.39 Hyper-V Data Exchange Service (vmickvpexchange) Service	Fail: state vmickvpexchange (stopped), startmode vmickvpexchange (manual).
2.3.1.40 Hyper-V Guest Service Interface (vmicguestinterface) Service	Fail: state vmicguestinterface (stopped), startmode vmicguestinterface (manual).
2.3.1.41 Hyper-V Guest Shutdown Service (vmicshutdown) Service	Fail: state vmicshutdown (stopped), startmode vmicshutdown (manual).
2.3.1.42 Hyper-V Heartbeat Service (vmicheartbeat) Service	Fail: state vmicheartbeat (stopped), startmode vmicheartbeat (manual).
2.3.1.43 Hyper-V Remote Desktop Virtualization Service (vmicrdv) Service	Fail: state vmicrdv (stopped), startmode vmicrdv (manual).
2.3.1.44 Hyper-V Time Synchronization Service (vmictimesync) Service	Fail: state vmictimesync (stopped), startmode vmictimesync (manual).
2.3.1.45 Hyper-V Volume Shadow Copy Requestor (vmicvss) Service	Fail: state vmicvss (stopped), startmode vmicvss (manual).
2.3.1.46 IKE and AuthIP IPsec Keying Modules Service	Fail: state IKEEXT (running), startmode IKEEXT (auto).
2.3.1.47 Interactive Services Detection Service	Fail: state UI0Detect (stopped), startmode UI0Detect (manual).
2.3.1.48 Internet Connection Sharing (ICS) Service	Fail: state SharedAccess (stopped), startmode SharedAccess (manual).
2.3.1.49 Internet Explorer ETW Collector Service	
2.3.1.50 IP Helper Service	
2.3.1.51 IPsec Policy Agent Service	Fail: state PolicyAgent (running), startmode PolicyAgent (manual).
2.3.1.52 KDC Proxy Server service (kpssvc) Service	Fail: state kpssvc (), startmode kpssvc ().
2.3.1.53 KtmRm for Distributed Transaction Coordinator Service	Fail: state KtmRm (stopped), startmode KtmRm (manual).
2.3.1.54 Link-Layer Topology Discovery Mapper Service	Fail: state lltdsvc (stopped), startmode lltdsvc (manual).
2.3.1.55 Microsoft iSCSI Initiator Service	
2.3.1.56 Microsoft Software Shadow Copy Provider Service	
2.3.1.57 Microsoft Storage Spaces SMP (smphost) Service	
2.3.1.58 Multimedia Class Scheduler Service	
2.3.1.59 Net.Tcp Port Sharing Service	
2.3.1.60 Netlogon Service	Fail: state Netlogon (stopped), startmode Netlogon (manual).
2.3.1.61 Network Access Protection Agent Service	
2.3.1.62 Network Connections Service	
2.3.1.63 Network Connectivity Assistant (ncasvc) Service	Fail: state ncasvc (), startmode ncasvc ().
2.3.1.64 Network List Service	Fail: state netprofm (running), startmode netprofm (manual).
2.3.1.65 Network Location Awareness Service	
2.3.1.66 Network Store Interface Service	
2.3.1.67 Optimize Drives (defragsvc) Service	
2.3.1.68 Performance Counter DLL Host (perfhost) Service	Fail: state perfhost (), startmode perfhost ().
2.3.1.69 Performance Logs and Alerts Service	

2.3.1.70 Plug and Play Service	
2.3.1.71 Portable Device Enumerator Service	Fail: state WPDBusEnum (stopped), startmode WPDBusEnum (manual).
2.3.1.72 Power Service	
2.3.1.73 Print Spooler Service	Fail: state Spooler (running), startmode Spooler (auto).
2.3.1.74 Printer Extensions and Notifications Service	Fail: state printnotify (), startmode printnotify ().
2.3.1.75 Problem Reports and Solutions Control Panel Support Service	Fail: state wercplsupport (stopped), startmode wercplsupport (manual).
2.3.1.76 Remote Access Auto Connection Manager Service	Fail: state RasAuto (stopped), startmode RasAuto (manual).
2.3.1.77 Remote Access Connection Manager Service	Fail: state RasMan (stopped), startmode RasMan (manual).
2.3.1.78 Remote Desktop Configuration Service	Fail: state SessionEnv (running), startmode SessionEnv (manual).
2.3.1.79 Remote Desktop Services Service	Fail: state TermService (running), startmode TermService (manual).
2.3.1.80 Remote Desktop Services UserMode Port Redirector	Fail: state UmRdpService (running), startmode UmRdpService (manual).
2.3.1.81 Remote Procedure Call (RPC) Service	
2.3.1.82 Remote Procedure Call (RPC) Locator Service	Fail: state RpcLocator (stopped), startmode RpcLocator (manual).
2.3.1.83 Remote Registry Service	Fail: state RemoteRegistry (stopped), startmode RemoteRegistry (auto).
2.3.1.84 Resultant Set of Policy Provider Service	Fail: state RSoPProv (stopped), startmode RSoPProv (manual).
2.3.1.85 Routing and Remote Access Service	
2.3.1.86 RPC Endpoint Mapper Service	
2.3.1.87 Secondary Logon Service	Fail: state seclogon (running), startmode seclogon (manual).
2.3.1.88 Secure Socket Tunneling Protocol Service	Fail: state SstpSvc (stopped), startmode SstpSvc (manual).
2.3.1.89 Security Accounts Manager Service	Fail: state SamSs (running), startmode SamSs (auto).
2.3.1.90 Server Service	Fail: state LanmanServer (running), startmode LanmanServer (auto).
2.3.1.91 Shell Hardware Detection Service	
2.3.1.92 Smart Card Service	Fail: state SCardSvr (stopped), startmode SCardSvr (disabled).
2.3.1.93 Smart Card Device Enumeration Service	
2.3.1.94 Smart Card Removal Policy Service	
2.3.1.95 SNMP Trap Service	Fail: state SNMPTRAP (stopped), startmode SNMPTRAP (manual).
2.3.1.96 Software Protection Service	
2.3.1.97 Special Administration Console Helper Service	Fail: state sacsvr (stopped), startmode sacsvr (manual).
2.3.1.98 Spot Verifier Service	
2.3.1.99 SSDP Discovery Service	Fail: state SSDPSRV (running), startmode SSDPSRV (manual).
2.3.1.100 Storage Tiers Management Service	
2.3.1.101 Superfetch Service	
2.3.1.102 System Event Notification Service	Fail: state SENS (running), startmode SENS (auto).
2.3.1.103 System Events Broker Service	
2.3.1.104 Task Scheduler Service	
2.3.1.105 TCP/IP NetBIOS Helper Service	Fail: state lmhosts (running), startmode lmhosts (manual).
2.3.1.106 Telephony Service	Fail: state TapiSrv (stopped), startmode TapiSrv (manual).
2.3.1.107 Themes Service	Fail: state Themes (running), startmode Themes (auto).
2.3.1.108 Thread Ordering Server Service	
2.3.1.109 UPnP Device Host Service	Fail: state upnphost (stopped), startmode upnphost (manual).
2.3.1.110 User Access Logging Service	
2.3.1.111 User Profile Service	
2.3.1.112 Virtual Disk Service	
2.3.1.113 Volume Shadow Copy Service	
2.3.1.114 Windows Audio Service	
2.3.1.115 Windows Audio Endpoint Builder Service	Fail: state AudioEndpointBuilder (stopped), startmode AudioEndpointBuilder (manual).
2.3.1.116 Windows Color System Service	
2.3.1.117 Windows Connection Manager (wcmsvc) Service	
2.3.1.118 Windows Driver Foundation - User-mode Driver Framework Service	Fail: state wudfsvc (running), startmode wudfsvc (manual).
2.3.1.119 Windows Encryption Provider Host Service	Fail: state WEPHOSTSVC (stopped), startmode WEPHOSTSVC (manual).
2.3.1.120 Windows Error Reporting Service	Fail: state WerSvc (stopped), startmode WerSvc (manual).
2.3.1.121 Windows Event Collector Service	Fail: state Wecsvc (stopped), startmode Wecsvc (manual).

2.3.1.122 Windows Event Log Service	
2.3.1.123 Windows Firewall Service	
2.3.1.124 Windows Font Cache (fontcache) Service	Fail: state fontcache (), startmode fontcache ().
2.3.1.125 Windows Installer Service	
2.3.1.126 Windows Management Instrumentation Service	
2.3.1.127 Windows Modules Installer Service	
2.3.1.128 Windows Pres'tion Found'n Font Cache (fontcache3.0.0.0) Service	Fail: state fontcache3.0.0.0 (), startmode fontcache3.0.0.0 ().
2.3.1.129 Windows Process Activation Service Service	Fail: state WAS (running), startmode WAS (manual).
2.3.1.130 Windows Remote Management (WS-Management) Service	Fail: state WinRM (running), startmode WinRM (auto).
2.3.1.131 Windows Store Service (WSService)	Fail: state WSService (), startmode WSService ().
2.3.1.132 Windows Time Service	
2.3.1.133 Windows Update Service	
2.3.1.134 WinHTTP Web Proxy Auto-Discovery Service	
2.3.1.135 Wired AutoConfig Service	Fail: state dot3svc (stopped), startmode dot3svc (manual).
2.3.1.136 WMI Performance Adapter Service	
2.3.1.137 Workstation Service	

2.4 SOX Cyber Security Audit : System Hardening: Optional Services List - - Verify that system configuration standards include the following procedures for all types of system components:

2.4.1 SOX Cyber Security Audit : System Hardening: Optional Services List

Rule Name	Result
2.4.1.1 Optional Services List: NNT Agent Service (NNTAgentService)	
2.4.1.2 Optional Services List: NNT Proxy Agent Service (NNTAgentProxyService)	
2.4.1.3 Optional Services List: NNT Change Tracker Gen 7 MongoDB Service	
2.4.1.4 Optional Services List: NNT Change Tracker Gen 7 Redis Service	
2.4.1.5 Optional Services List: ASP.NET State Service (aspnet_state) Service	
2.4.1.6 Optional Services List: World Wide Web Publishing Service	
2.4.1.7 Optional Services List: W3C Logging Service	

2.5 SOX Cyber Security Audit : Do not use vendor-supplied defaults for system passwords and other security parameters: Develop configuration standards for all system components

2.5.1 SOX Cyber Security Audit : System Hardening: Group Policy Rules

Rule Name	Result
2.5.1.1 Set 'Configure registry policy processing: Do not apply during periodic background processing' to 'False'	Pass: Rule passed : '0'.
2.5.1.2 Set 'Configure registry policy processing: Process even if the Group Policy objects have not changed' to 'True'	Pass: Rule passed : '0'.

2.5.2 SOX Cyber Security Audit : System Hardening: Internet Communication settings Rules

Rule Name	Result
2.5.2.1 Set 'Turn off downloading of print drivers over HTTP' to 'Enabled'	Pass: Rule passed : '1'.
2.5.2.2 Set 'Turn off Internet download for Web publishing and online ordering wizards' to 'Enabled'	Pass: Rule passed : '1'.
2.5.2.3 Set 'Turn off printing over HTTP' to 'Enabled'	Pass: Rule passed : '1'.
2.5.2.4 Set 'Turn off Search Companion content file updates' to 'Enabled'	Pass: Rule passed : '1'.
2.5.2.5 Set 'Turn off the "Publish to Web" task for files and folders' to 'Enabled'	Pass: Rule passed : '1'.
2.5.2.6 Set 'Turn off the Windows Messenger Customer Experience Improvement Program' to 'Enabled'	Pass: Rule passed : '2'.

2.5.3 SOX Cyber Security Audit : System Hardening: Personalization Rules

Rule Name	Result
2.5.3.1 Set 'Prevent enabling lock screen camera' to 'Enabled'	Pass: Rule passed : '1'.
2.5.3.2 Set 'Prevent enabling lock screen slide show' to 'Enabled'	Pass: Rule passed : '1'.

2.5.4 SOX Cyber Security Audit : System Hardening: Search Rules

Rule Name	Result
2.5.4.1 Set 'Allow indexing of encrypted files' to 'Disabled'	Pass: Rule passed : '0'.

2.5.5 SOX Cyber Security Audit : System Hardening: Windows Installer Rules

Rule Name	Result
2.5.5.1 Set 'Always install with elevated privileges' to 'Disabled'	Pass: Rule passed : '0'.

2.5.6 SOX Cyber Security Audit : System Hardening - Additional Measues: Administrative Templates (Computer) Rules

Rule Name	Result
2.5.6.1 Set 'Apply UAC restrictions to local accounts on network logons' to 'Enabled'	Pass: Rule passed : '0'.
2.5.6.2 Set 'WDigest Authentication' to 'Disabled'	Pass: Rule passed : '0'.

2.5.7 SOX Cyber Security Audit : System Hardening - Additional Measues: App runtime Rules

Rule Name	Result
2.5.7.1 Set 'Allow Microsoft accounts to be optional' to 'Enabled'	Pass: Rule passed : '1'.

2.5.8 SOX Cyber Security Audit : System Hardening - Additional Measues: User Account Control Rules

Rule Name	Result
2.5.8.1 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'	Pass: Rule passed : '1'.
2.5.8.2 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'	Pass: Rule passed : '0'.
2.5.8.3 Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop'	Fail: Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop' : .'5'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Prompt for consent on the secure desktop.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode - Impact:This policy setting controls the behavior of the elevation prompt for administrators.
2.5.8.4 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	Fail: Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests' : .'3'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Automatically deny elevation requests:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users - Impact:Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are - Impacted are identified and standard operating procedures are modified to support least privilege operations.
2.5.8.5 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'	Pass: Rule passed : '1'.
2.5.8.6 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'	Pass: Rule passed : '1'.
2.5.8.7 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	Pass: Rule passed : '1'.
2.5.8.8 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	Pass: Rule passed : '1'.
2.5.8.9 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	Pass: Rule passed : '1'.

2.5.9 SOX Cyber Security Audit : System Hardening - Additional Measues: AutoPlay Policies Rules

Rule Name	Result

2.5.9.1 Set 'Turn off Autoplay' to 'Enabled:All drives'	Pass: Rule passed : '255'.

2.5.10 SOX Cyber Security Audit : System Hardening - Additional Measues: EMET Rules

Rule Name	Result
2.5.10.1 Ensure EMET is installed	Pass: Rule passed : '2'.
2.5.10.2 Set 'Default Protections for Internet Explorer' to 'Enabled'	Pass: Rule passed : '*\Internet Explorer\iexplore.exe'.
2.5.10.3 Set 'Default Protections for Popular Software' to 'Enabled'	Fail: Set 'Default Protections for Popular Software' to 'Enabled' : .'*\7-Zip\7z.exe -EAF' '*\7-Zip\7zFM.exe -EAF' '*\7-Zip\7zG.exe -EAF' '*\Google\Chrome\Application\chrome.exe -SEHOP' Remediation : To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer.
2.5.10.4 Set 'Default Protections for Recommended Software' to 'Enabled'	Fail: Set 'Default Protections for Recommended Software' to 'Enabled' : Remediation : To establish the recommended configuration via GP, set the following UI path to Enabled.Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software.
2.5.10.5 Set 'System ASLR' to 'Enabled:Application Opt-In'	Pass: Rule passed : '3'.
2.5.10.6 Set 'System DEP' to 'Enabled:Application Opt-Out'	Pass: Rule passed : '2'.
2.5.10.7 Set 'System SEHOP' to 'Enabled:Application Opt-Out'	Pass: Rule passed : '2'.

2.5.11 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - User Rights Assignment

Rule Name	Result
2.5.11.1 Set 'Access Credential Manager as a trusted caller' to 'No One'	Pass: Rule passed : securitypolicy ().
2.5.11.2 Set 'Access this computer from the network'	Fail: Configured Setting is securitypolicy (3 items: EVERYONE, BUILTIN\USERS, BUILTIN\BACKUP OPERATORS) Remediation : To implement the recommended configuration state, set the following Group Policy setting:Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network - Impact:If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use ne... (truncated).
2.5.11.3 Set 'Act as part of the operating system' to 'No One'	Pass: Rule passed :.
2.5.11.4 Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Fail: Set 'Adjust memory quotas for a process' to 'Administrators, Local Service, Network Service' : securitypolicy (4 items: IIS APPPOOL\NNT WEB APPLICATIONS, IIS APPPOOL\.NET V4.5, IIS APPPOOL\DEFAULTAPPPOOL, IIS APPPOOL\.NET V4.5 CLASSIC). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators, Local Service, Network Service. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory... (truncated).
2.5.11.5 Set 'Allow log on locally' to 'Administrators'	Fail: Set 'Allow log on locally' to 'Administrators' : securitypolicy (2 items: BUILTIN\USERS, BUILTIN\BACKUP OPERATORS). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally - Impact:If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your enviro... (truncated).
2.5.11.6 Configure 'Allow log on through Remote Desktop Services'	Pass: Rule passed : securitypolicy (2 items: BUILTIN\ADMINISTRATORS, BUILTIN\REMOTE DESKTOP USERS).
2.5.11.7 Set 'Back up files and directories' to 'Administrators'	Fail: Set 'Back up files and directories' to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories - Impact:Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigne... (truncated).
2.5.11.8 Set 'Change the system time' to 'Administrators, LOCAL SERVICE'	Pass: Rule passed : securitypolicy (2 items: NT AUTHORITY\LOCAL SERVICE, BUILTIN\ADMINISTRATORS).
2.5.11.9 Set 'Change the time zone' to 'Administrators, LOCAL SERVICE'	Pass: Rule passed : securitypolicy (2 items: NT AUTHORITY\LOCAL SERVICE, BUILTIN\ADMINISTRATORS).
2.5.11.10 Set 'Create a pagefile' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.11 Set 'Create a token object' to 'No One'	Pass: Rule passed : securitypolicy ().
2.5.11.12 Set 'Create global objects' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass: Rule passed : securitypolicy (4 items: NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, BUILTIN\ADMINISTRATORS, NT AUTHORITY\SERVICE).
2.5.11.13 Set 'Create permanent shared objects' to 'No One'	Pass: Rule passed : securitypolicy ().
2.5.11.14 Set 'Create symbolic links' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.15 Set 'Debug programs' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).

2.5.11.16 Set 'Enable computer and user accounts to be trusted for delegation'	Pass: Rule passed : securitypolicy ().
2.5.11.17 Set 'Force shutdown from a remote system' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.18 Set 'Impersonate a client after authentication' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Fail: Set 'Impersonate a client after authentication' to 'Administrators, SERVICE, Local Service, Network Service' : securitypolicy (BUILTIN\IIS_IUSRS). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators, SERVICE, Local Service, Network Service. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication - Impact:In most cases this configuration will have no ... (truncated).
2.5.11.19 Set 'Increase scheduling priority' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.20 Set 'Load and unload device drivers' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.21 Set 'Lock pages in memory' to 'No One'	Pass: Rule passed : securitypolicy ().
2.5.11.22 Set 'Modify an object label' to 'No One'	Pass: Rule passed : securitypolicy ().
2.5.11.23 Set 'Modify firmware environment values' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.24 Set 'Perform volume maintenance tasks' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.25 Set 'Profile single process' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
2.5.11.26 Set 'Profile system performance' to 'Administrators, NT SERVICE\WdiServiceHost'	Pass: Rule passed : securitypolicy (2 items: BUILTIN\ADMINISTRATORS, NT SERVICE\WDISERVICEHOST).
2.5.11.27 Set 'Replace a process level token' to 'LOCAL SERVICE, NETWORK SERVICE'	Fail: Set 'Replace a process level token' to 'Local Service, Network Service' : securitypolicy (4 items: IIS APPPOOL\NNT WEB APPLICATIONS, IIS APPPOOL\.NET V4.5, IIS APPPOOL\DEFAULTAPPPOOL, IIS APPPOOL\.NET V4.5 CLASSIC). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Local Service, Network Service. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token - Impact:On most comput... (truncated).
2.5.11.28 Set 'Restore files and directories' to 'Administrators'	Fail: Set 'Restore files and directories' to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories - Impact:If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for us... (truncated).
2.5.11.29 Set 'Shut down the system' to 'Administrators'	Fail: Set 'Shut down the system' to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system - Impact:The - Impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You... (truncated).
2.5.11.30 Set 'Take ownership of files or other objects' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).

2.5.12 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Security Options

Rule Name	Result
2.5.12.1 Set 'Accounts: Block Microsoft accounts' to 'Users can't add or log on with Microsoft accounts'	Pass: Rule passed : '3'.
2.5.12.2 Set 'Accounts: Guest account status' to 'Disabled'	Pass: Rule passed : securitypolicy (0)'[{oval:org.cisecurity.benchmarks.microsoft_windows_8.1:obj:1051}]'.
2.5.12.3 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'	Pass: Rule passed : '1'.
2.5.12.4 Configure 'Accounts: Rename administrator account'	Fail: Configure 'Accounts: Rename administrator account' : securitypolicy (2 items: "Administrator", "Administrator"). Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account - Impact:You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.).
2.5.12.5 Configure 'Accounts: Rename guest account'	Fail: Configure 'Accounts: Rename guest account' : securitypolicy (2 items: "Guest", "Guest"). Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account - Impact:There should be little - Impact, because the Guest account is disabled by default.

2.5.13 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Devices Rules

Rule Name	Result

2.5.13.1 Set 'Devices: Allowed to format and eject removable media' to 'Administrators'	Fail: Set 'Devices: Allowed to format and eject removable media' to 'Administrators' : .''. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Administrators.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media - Impact:Only Administrators will be able to format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they will need to be informed of the change in policy.
2.5.13.2 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled'	Pass: Rule passed : '1'.

2.5.14 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Domain member Rules

Rule Name	Result
2.5.14.1 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'	Pass: Rule passed : '1'.
2.5.14.2 Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'	Pass: Rule passed : '1'.
2.5.14.3 Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled'	Pass: Rule passed : '1'.
2.5.14.4 Set 'Domain member: Disable machine account password changes' to 'Disabled'	Pass: Rule passed : '0'.
2.5.14.5 Set 'Domain member: Maximum machine account password age' to 30 or fewer days, but not 0	Pass: Rule passed : '30' '30'.
2.5.14.6 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled'	Pass: Rule passed : '1'.

2.5.15 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Interactive logon Rules

Rule Name	Result
2.5.15.1 Set 'Interactive logon: Do not display last user name' to 'Enabled'	Fail: Set 'Interactive logon: Do not display last user name' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name - Impact:Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.
2.5.15.2 Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'	Pass: Rule passed : '0'.
2.5.15.3 Configure 'Interactive logon: Message text for users attempting to log on'	Fail: Configure 'Interactive logon: Message text for users attempting to log on' : .'.
2.5.15.4 Configure 'Interactive logon: Message title for users attempting to log on'	Fail: Configure 'Interactive logon: Message title for users attempting to log on' : .''. Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on - Impact:Users will see a message in a dialog box before they can log on to the server console.Note Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer. Important If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.
2.5.15.5 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'	Fail: Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)' : .'10'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to 4 or fewer logon(s).Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available) - Impact:Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.
2.5.15.6 Set 'Interactive logon: Prompt user to change password before expiration' to 'between 5 and 14 days'	Pass: Rule passed : '5' '5'.

2.5.15.7 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation'	Fail: Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Lock Workstation.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior - Impact:If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

2.5.16 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Microsoft network client Rules

Rule Name	Result
2.5.16.1 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	Fail: Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) - Impact:The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.
2.5.16.2 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'	Pass: Rule passed : '1'.
2.5.16.3 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'	Pass: Rule passed : '0'.

2.5.17 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Microsoft network server Rules

Rule Name	Result
2.5.17.1 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'	Fail: Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) - Impact:The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

2.5.17.2 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'	Fail: Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) - Impact:The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.
2.5.17.3 Set 'Microsoft network server: Server SPN target name validation level' to 'Accept if provided by client'	Pass: Rule passed : '1'.

2.5.18 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - MSS Rules

Rule Name	Result
2.5.18.1 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled'	Pass: Rule passed : '0'.
2.5.18.2 Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Pass: Rule passed : '2'.
2.5.18.3 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	Pass: Rule passed : '2'.
2.5.18.4 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled'	Pass: Rule passed : '1'.
2.5.18.5 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90% or less'	Pass: Rule passed : '90'.

2.5.19 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Recovery console Rules

Rule Name	Result
2.5.19.1 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'	Pass: Rule passed : '0'.
2.5.19.2 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled'	Pass: Rule passed : '0'.

2.5.20 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - Shutdown Rules

Rule Name	Result
2.5.20.1 Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'	Pass: Rule passed : '0'.

2.5.21 SOX Cyber Security Audit : System Hardening - Security parameters to prevent misuse: Account Policies - System objects Rules

Rule Name	Result
2.5.21.1 Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled'	Pass: Rule passed : '1'.
2.5.21.2 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled'	Pass: Rule passed : '1'.

3 Protect financial Data: SOX Cyber Security Audit : Protect stored financial data

3.1 SOX Cyber Security Audit : Protect stored financial data: Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)

3.1.1 SOX Cyber Security Audit : Protect stored financial data: Render stored PANs unreadable

Rule Name	Result
3.1.1.1 Verify that financial Data Encryption and Tokenization measures are in place (Rule not automatically assessed)	Pass: This rule is not automatically assessed. You must implement data encryption and consider using other technologies such as tokenization.

4 Protect financial Data: SOX Cyber Security Audit : Encrypt transmission of financial data across open networks

4.1 SOX Cyber Security Audit : Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive financial data during transmission over open, public networks

4.1.1 SOX Cyber Security Audit : Encrypt transmission of financial data: Use strong cryptography and security protocols

Rule Name	Result

4.1.1.1 Configure 'System cryptography: Force strong key protection for user keys stored on the computer'	Note: this test is not automatically evaluated. It is up to you to implement the recommended items and verify compliance. Remediation : Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization: - Impact:Users will have to enter their password every time they access a key that is stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they will be forced to enter the password for that certificate every time they send a signed e-mail message. For some organizations the overhead that is involved using this configuration may be too high. For end user computers that are used to access sensitive data this setting could be set to "User is prompted when the key is first used," but Microsoft does not recommend enforcing this setting on servers due to the significant - Impact on manageability. For example, if this setting is configured to "User is prompted when the key is first used" you may not be able to configure Remote Desktop Services to use SSL certificates. More information is available in the Windows PKI blog: http://blogs.technet.com/b/pki/archive/2009/06/17/what-is-a-strong-key-protection-in-windows.aspx. Pass: Rule passed : '2'.
4.1.1.2 Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'	Fail: Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled. Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing - Impact:Client computers that have this policy setting enabled will be unable to communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms will not be able to use servers that require them for network communications. For example, many Apache-based Web servers are not configured to support TLS. If you enable this setting, you also need to configure Internet Explorer to use TLS. This policy setting also affects the encryption level that is used for the Remote Desktop Protocol (RDP). The Remote Desktop Connection tool uses the RDP protocol to communicate with servers that run Terminal Services and client computers that are configured for remote control; RDP connections will fail if both computers are not configured to use the same encryption algorithms. To enable Internet Explore to use TLS 1. On the Internet Explorer Tools menu, click Internet Options. 2. Click the Advanced tab. 3. Select the Use TLS 1.0 check box. It is also possible to configure this policy setting through Group Policy or by using the Internet Explorer Administrators Kit. Client computers running Windows XP, Windows XP SP1 and Windows XP SP2 that try to connect to a Terminal Services server that has this setting enabled will be unable to communicate with the server until an updated version of the Terminal Services client is installed. This issue could allo affect Remote Assistance and Remote Desktop connections. For more information about the issue and how to resolve it see "Remote Assistance connection to Windows Server 2003 with FIPS encryption does not work" at http://support.microsoft.com/default.aspx?scid=kb;en-us;811770. Microsoft .NET Framework applications such as Microsoft ASP.NET that use use cryptographic algorithms which are not validated by NIST to be FIPS 140 compliant may fail. Use of cryptographic algorithm classes that are not FIPS validated will cause an InvalidOperationException exception to occur. See ""System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows" for more information: http://support.microsoft.com/kb/811833. For more information about the - Impact of this setting see "FIPS 140 Evaluation" available at: http://technet.microsoft.com/en-us/library/cc750357.aspx.
4.1.1.3 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	Pass: Rule passed : '5'.
4.1.1.4 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher	Pass: Rule passed : '1'.
4.1.1.5 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	Fail: Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption' : .'536870912'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security,Require 128-bit encryption.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients - Impact:Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could - Impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

4.1.1.6 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'	Fail: Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption' : .'536870912'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security,Require 128-bit encryption.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers - Impact:Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could - Impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
4.1.1.7 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled'	Pass: Rule passed : '1'.

5 Maintain a Vulnerability Management Program: SOX Cyber Security Audit : Protect all systems against malware

5.1 SOX Cyber Security Audit : Protect all systems against malware and regularly update anti-virus software or programs

5.1.1 SOX Cyber Security Audit : Anti-Virus Protection Check

Rule Name	Result
5.1.1.1 Verify Virus Protection is enabled and updated	Pass: This rule is not automatically assessed. Once you have selected an AV system please contact NNT to incorporate checks for associated AV services that can be validated as part of your compliance report.

5.1.2 SOX Cyber Security Audit : Protect all systems against malware: Early Launch Antimalware Rules

Rule Name	Result
5.1.2.1 Set 'Boot-Start Driver Initialization Policy' to 'Enabled: Good, unknown and bad but critical'	Pass: Rule passed : '3'.

5.1.3 SOX Cyber Security Audit : Protect all systems against malware: Attachment Rules

Rule Name	Result
5.1.3.1 Set 'Notify antivirus programs when opening attachments' to 'Enabled'	Fail: Set 'Notify antivirus programs when opening attachments' to 'Enabled' : .'1'. Remediation : To establish the recommended configuration via GP, set the following UI path to Enabled.User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments - Impact:When the Notify antivirus programs when opening attachments setting is Enabled, every downloaded file or e-mail attachment that the user opens will be scanned.

6 Maintain a Vulnerability Management Program: SOX Cyber Security Audit : Develop and maintain secure systems and applications

6.1 SOX Cyber Security Audit : Develop and maintain secure systems and applications

6.1.1 SOX Cyber Security Audit : Develop and maintain secure systems and applications - Windows Update Rules

Rule Name	Result
6.1.1.1 Set 'Configure Automatic Updates' to 'Enabled'	Pass: Rule passed : '0'.
6.1.1.2 Set 'Configure Automatic Updates: Scheduled install day' to '0 - Every day'	Pass: Rule passed : '0'.
6.1.1.3 Set 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' to 'Disabled'	Pass: Rule passed : '0'.
6.1.1.4 Set 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' to 'Disabled'	Pass: Rule passed : '0'.
6.1.1.5 Set 'No auto-restart with logged on users for scheduled automatic updates installations' to 'Disabled'	Pass: Rule passed : '0'.
6.1.1.6 Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled:1 minute'	Pass: Rule passed : '1' '1'.

7 Implement Strong Access Control Measures: SOX Cyber Security Audit : Restrict access to financial data by business need to know

7.1 SOX Cyber Security Audit : SOX Cyber Security Audit : Restrict access to financial data by business need to know: Restriction of access to privileged user IDs to least privileges necessary to perform job

7.1.1 SOX Cyber Security Audit : Restrict access to financial data by business need to know - Network Access Rules

Rule Name	Result

7.1.1.1 Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'	Pass: Rule passed : 0'0'.
7.1.1.2 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'	Pass: Rule passed : '1'.
7.1.1.3 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'	Fail: Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to Enabled.Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares - Impact:It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.
7.1.1.4 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'	Pass: Rule passed : '0'.
7.1.1.5 Configure 'Network Access: Named Pipes that can be accessed anonymously'	Pass: Rule passed : ' '.
7.1.1.6 Set 'Network access: Remotely accessible registry paths'	Pass: Configured Setting is securitypolicy (3 items: SYSTEM\CURRENTCONTROLSET\CONTROL\PRODUCTOPTIONS, SYSTEM\CURRENTCONTROLSET\CONTROL\SERVER APPLICATIONS, SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION).
7.1.1.7 Set 'Network access: Remotely accessible registry paths and sub-paths'	Pass: Configured Setting is securitypolicy (11 items: SYSTEM\CURRENTCONTROLSET\CONTROL\PRINT\PRINTERS, SYSTEM\CURRENTCONTROLSET\SERVICES\EVENTLOG, SOFTWARE\MICROSOFT\OLAP SERVER, SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PRINT, SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS, SYSTEM\CURRENTCONTROLSET\CONTROL\CONTENTINDEX, SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER, SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER\USERCONFIG, SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER\DEFAULTUSERCON... (truncated).
7.1.1.8 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'	Pass: Rule passed : '1'.
7.1.1.9 Set 'Network access: Shares that can be accessed anonymously' to 'None'	Pass: Rule passed : ''.
7.1.1.10 Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves'	Pass: Rule passed : '0'.

7.1.2 SOX Cyber Security Audit : Restrict access to financial data by business need to know - Network Security Rules

Rule Name	Result
7.1.2.1 Set 'Do not display network selection UI' to 'Enabled'	Pass: Rule passed : '1'.
7.1.2.2 Set 'Configure Offer Remote Assistance' to 'Disabled'	Pass: Rule passed : '0'.
7.1.2.3 Set 'Configure Solicited Remote Assistance' to 'Disabled'	Pass: Rule passed : '0'.
7.1.2.4 Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'	Pass: Rule passed : '1'.
7.1.2.5 Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'	Pass: Rule passed : '0'.
7.1.2.6 Set 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' to 'Disabled'	Pass: Rule passed : '0'.
7.1.2.7 Set 'Network Security: Configure encryption types allowed for Kerberos' to 'RC4\AES128\AES256\Future types'	Pass: Rule passed : '2147483644'.
7.1.2.8 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'	Pass: Rule passed : '1'.
7.1.2.9 Set 'Deny access to this computer from the network'	Fail: Set 'Deny access to this computer from the network' to 'Guests' : securitypolicy (). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Guests. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network - Impact:If you configure the Deny access to this computer from the network user right for other groups, you could limit the abilities of users who are assigned t... (truncated).
7.1.2.10 Set 'Deny log on as a batch job' to include 'Guests'	Fail: Set 'Deny log on as a batch job' to 'Guests' : securitypolicy (). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Guests. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job - Impact:If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job act... (truncated).
7.1.2.11 Set 'Deny log on as a service' to include 'Guests'	Fail: Set 'Deny log on as a service' to 'Guests' : securitypolicy (). Remediation : To implement the recommended configuration state, set the following Group Policy setting to No One. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service - Impact:If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.
7.1.2.12 Set 'Deny log on locally' to include 'Guests'	Fail: Set 'Deny log on locally' to 'Guests' : securitypolicy (). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Guests. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally - Impact:If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should exp... (truncated).
7.1.2.13 Set 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	Fail: Set 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' : securitypolicy (). Remediation : To establish the recommended configuration via GP, set the following UI path to include Guests, Local account.Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services - Impact:If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users w... (truncated).

8 Implement Strong Access Control Measures: SOX Cyber Security Audit : Identify and authenticate access to system components

8.1 SOX Cyber Security Audit : Identify and authenticate access to system components: Restrict access to financial data by business need to know: 8.1 Define and implement policies and procedures to ensure proper user

8.1.1 SOX Cyber Security Audit : Identify and authenticate access to system components - Account Lockout Rules

Rule Name	Result
8.1.1.1 Set 'Account lockout threshold' to 6 or fewer invalid logon attempt(s), but not 0	Fail: Set 'Account lockout threshold' to 10 or fewer invalid logon attempt(s), but not 0 : .'10' '10'. Remediation : To establish the recommended configuration via GP, set the following UI path to 6 or fewer invalid logon attempt(s) inclusive. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold - Impact:If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate a additional help desk calls. If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.
8.1.1.2 Set 'Account lockout duration' to '30 or more minute(s)'	Pass: Rule passed : '30'.

8.1.1.3 Set 'Reset account lockout counter after' to '30 or more minute(s)'	Pass: Rule passed : '30'.
8.1.1.4 Set 'Network security: Force logoff when logon hours expire' to 'Enabled'	Pass: Rule passed : '1'.
8.1.1.5 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled'	Pass: Rule passed : '1'.
8.1.1.6 Set 'Interactive logon: Machine inactivity limit' to 15 minutes - 900 or fewer second(s), but not 0	Pass: Rule passed : '900' '900'.
8.1.1.7 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15 or fewer minute(s)'	Pass: Rule passed : '15'.
8.1.1.8 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires must be set to zero seconds	Pass: Rule passed : '0'.

8.1.2 SOX Cyber Security Audit : Identify and authenticate access to system components - Password Policy

Rule Name	Result
8.1.2.1 Set 'Enforce password history' to '24 or more password(s)'	Fail: Set 'Enforce password history' to '24 or more password(s)' : .'15'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to 24 or more password(s).Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history - Impact:The major - Impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.
8.1.2.2 Set 'Maximum password age' to 60 or fewer days, but not 0	Fail: Set 'Maximum password age' to 60 or fewer days, but not 0 : .'-1' '-1'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to 60 or fewer days, but not 0.Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age - Impact:If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.
8.1.2.3 Set 'Minimum password age' to '1 or more day(s)'	Fail: Set 'Minimum password age' to '1 or more day(s)' : .'0'. Remediation : To implement the recommended configuration state, set the following Group Policy setting to 1 or more day(s).Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age - Impact:If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.
8.1.2.4 Set 'Minimum password length' to '14 or more character(s)'	Pass: Rule passed : '14'.
8.1.2.5 Set 'Password must meet complexity requirements' to 'Enabled'	Pass: Rule passed : '1'.
8.1.2.6 Set 'Store passwords using reversible encryption' to 'Disabled'	Pass: Rule passed : '0'.

8.1.3 SOX Cyber Security Audit : Identify and authenticate access to system components - Windows Logon Options Rules

Rule Name	Result
8.1.3.1 Set 'Sign-in last interactive user automatically after a system-initiated restart' to 'Disabled'	Pass: Rule passed : '1'.

8.1.4 SOX Cyber Security Audit : Identify and authenticate access to system components - Windows Remote Management (WinRM)-WinRM Client Rules

Rule Name	Result
8.1.4.1 Set 'Allow Basic authentication' to 'Disabled'	Pass: Rule passed : '0'.
8.1.4.2 Set 'Allow unencrypted traffic' to 'Disabled'	Pass: Rule passed : '0'.
8.1.4.3 Set 'Disallow Digest authentication' to 'Enabled'	Pass: Rule passed : '0'.

8.1.5 SOX Cyber Security Audit : Identify and authenticate access to system components - Remote Desktop Rules

Rule Name	Result
8.1.5.1 Set 'Do not allow passwords to be saved' to 'Enabled'	Pass: Rule passed : '1'.

8.1.5.2 Set 'Do not allow drive redirection' to 'Enabled'	Pass: Rule passed : '1'.
8.1.5.3 Set 'Always prompt for password upon connection' to 'Enabled'	Pass: Rule passed : '1'.
8.1.5.4 Set 'Set client connection encryption level: Encryption Level' to 'Enabled: High Level'	Pass: Rule passed : '3'.

9 Maintain a Vulnerability Management Program: SOX Cyber Security Audit : Restrict physical access to financial data

9.1 SOX Cyber Security Audit : Restrict physical access to financial data: Physical Protection procedures and measures

9.1.1 SOX Cyber Security Audit : Restrict physical access to financial data: Physical Protection procedures and measures

Rule Name	Result
9.1.1.1 Verify SOX SOX Cyber Security Audit requirements are being operated (Rule not automatically assessed)	Pass: This rule is not automatically assessed. Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the financial data environment.

10 Regularly Monitor and Test Networks: SOX Cyber Security Audit 0: Track and monitor all access to network resources and financial data

10.1 SOX Cyber Security Audit 0: Track access to network/financial data: Retain and Review System Audit Trails

10.1.1 SOX Cyber Security Audit 0: Track access to network/financial data: Account Policies - Audit Rules

Rule Name	Result
10.1.1.1 Set 'Manage auditing and security log' to 'Administrators'	Pass: Rule passed : securitypolicy (BUILTIN\ADMINISTRATORS).
10.1.1.2 Set 'Generate security audits' to 'LOCAL SERVICE, NETWORK SERVICE'	Fail: Set 'Generate security audits' to 'Local Service, Network Service' : securitypolicy (4 items: IIS APPPOOL\NNT WEB APPLICATIONS, IIS APPPOOL\.NET V4.5, IIS APPPOOL\DEFAULTAPPPOOL, IIS APPPOOL\.NET V4.5 CLASSIC). Remediation : To implement the recommended configuration state, set the following Group Policy setting to Local Service, Network Service. Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits - Impact:None. This is the defaul... (truncated).
10.1.1.3 Set 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' to 'Enabled'	Pass: Rule passed : '1'.
10.1.1.4 Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled'	Pass: Rule passed : '0'.

10.1.2 SOX Cyber Security Audit 0: Track access to network/financial data: Windows Components - Event Log Rules

Rule Name	Result
10.1.2.1 Set 'Maximum Log Size (KB)' to 'Enabled:32768'	Pass: Application Event Log Max Size is set to: 32768.
10.1.2.2 Set 'Retain old events' to 'Disabled'	Pass: Configured Setting is 0.
10.1.2.3 Set 'Retain old events' to 'Disabled'	Pass: Configured Setting is 0.
10.1.2.4 Set 'Maximum Log Size (KB)' to 'Enabled:81920'	Pass: Security Event Log Max Size is set to: 81920.
10.1.2.5 Set 'Maximum Log Size (KB)' to 'Enabled:32768'	Pass: System Event Log Max Size is set to: 32768.
10.1.2.6 Set 'Retain old events' to 'Disabled'	Pass: Configured Setting is 0.

10.1.3 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - System Rules

Rule Name	Result
10.1.3.1 Set 'Audit Policy: System: System Integrity' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: System Integrity - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.3.2 Set 'Audit Policy: System: Security System Extension' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security System Extension - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.3.3 Set 'Audit Policy: System: Security State Change' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security State Change - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

10.1.3.4 Set 'Audit Policy: System: IPsec Driver' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: IPsec Driver - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.3.5 Set 'Audit Policy: System: Other System Events' to 'No Auditing'	Pass: Rule passed :.

10.1.4 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Object Access Rules

Rule Name	**Result**
10.1.4.1 Set 'Audit Policy: Object Access: Handle Manipulation' to 'No Auditing'	Pass: Rule passed :.
10.1.4.2 Set 'Audit Policy: Object Access: Other Object Access Events' to 'No Auditing'	Pass: Rule passed :.
10.1.4.3 Set 'Audit Policy: Object Access: File Share' to 'No Auditing'	Pass: Rule passed :.
10.1.4.4 Set 'Audit Policy: Object Access: File System' to 'No Auditing'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to No Auditing. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Policy: Object Access: File System - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.4.5 Set 'Audit Policy: Object Access: SAM' to 'No Auditing'	Pass: Rule passed :.
10.1.4.6 Set 'Audit Policy: Object Access: Kernel Object' to 'No Auditing'	Pass: Rule passed :.
10.1.4.7 Set 'Audit Policy: Object Access: Filtering Platform Packet Drop' to 'No Auditing'	Pass: Rule passed :.
10.1.4.8 Set 'Audit Policy: Object Access: Registry' to 'No Auditing'	Pass: Rule passed :.
10.1.4.9 Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing'	Pass: Rule passed :.
10.1.4.10 Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing'	Pass: Rule passed :.
10.1.4.11 Set 'Audit Policy: Object Access: Detailed File Share' to 'No Auditing'	Pass: Rule passed :.
10.1.4.12 Set 'Audit Policy: Object Access: Filtering Platform Connection' to 'No Auditing'	Pass: Rule passed :.

10.1.5 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Logon-Logoff Rules

Rule Name	**Result**
10.1.5.1 Set 'Audit Policy: Logon-Logoff: Other Logon/Logoff Events' to 'No Auditing'	Pass: Rule passed :.
10.1.5.2 Set 'Audit Policy: Logon-Logoff: Special Logon' to 'Success'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Special Logon - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.5.3 Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing'	Pass: Rule passed :.
10.1.5.4 Set 'Audit Policy: Logon-Logoff: Account Lockout' to 'No Auditing'	Pass: Rule passed :.
10.1.5.5 Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing'	Pass: Rule passed :.

10.1.5.6 Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing'	Pass: Rule passed :.
10.1.5.7 Set 'Audit Policy: Logon-Logoff: Logoff' to 'Success'	Pass: Rule passed :.
10.1.5.8 Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing'	Pass: Rule passed :.
10.1.5.9 Set 'Audit Policy: Logon-Logoff: Logon' to 'Success and Failure'	Pass: Rule passed :.

10.1.6 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - DS Access Rules

Rule Name	**Result**
10.1.6.1 Set 'Audit Policy: DS Access: Directory Service Replication' to 'No Auditing'	Pass: Rule passed :.
10.1.6.2 Set 'Audit Policy: DS Access: Detailed Directory Service Replication' to 'No Auditing'	Pass: Rule passed :.
10.1.6.3 Set 'Audit Policy: DS Access: Directory Service Changes' to 'No Auditing'	Pass: Rule passed :.
10.1.6.4 Set 'Audit Policy: DS Access: Directory Service Access' to 'No Auditing'	Pass: Rule passed :.

10.1.7 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Detailed Tracking Rules

Rule Name	Result
10.1.7.1 Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing'	Pass: Rule passed :.
10.1.7.2 Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No Auditing'	Pass: Rule passed :.
10.1.7.3 Set 'Audit Policy: Detailed Tracking: Process Creation' to 'Success'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: Process Creation - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.7.4 Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing'	Pass: Rule passed :.

10.1.8 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Policy Change Rules

Rule Name	Result
10.1.8.1 Set 'Audit Policy: Policy Change: MPSSVC Rule-Level Policy Change' to 'No Auditing'	Pass: Rule passed :.
10.1.8.2 Set 'Audit Policy: Policy Change: Filtering Platform Policy Change' to 'No Auditing'	Pass: Rule passed :.
10.1.8.3 Set 'Audit Policy: Policy Change: Authorization Policy Change' to 'No Auditing'	Pass: Rule passed :.
10.1.8.4 Set 'Audit Policy: Policy Change: Audit Policy Change' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Audit Policy Change - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.8.5 Set 'Audit Policy: Policy Change: Other Policy Change Events' to 'No Auditing'	Pass: Rule passed :.
10.1.8.6 Set 'Audit Policy: Policy Change: Authentication Policy Change' to 'Success'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authentication Policy Change - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

10.1.9 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Account Management Rules

Rule Name	Result
10.1.9.1 Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing'	Pass: Rule passed :.
10.1.9.2 Set 'Audit Policy: Account Management: Computer Account Management' to 'Success'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Computer Account Management - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

10.1.9.3 Set 'Audit Policy: Account Management: User Account Management' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User Account Management - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.9.4 Set 'Audit Policy: Account Management: Security Group Management' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.9.5 Set 'Audit Policy: Account Management: Other Account Management Events' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Other Account Management Events - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.
10.1.9.6 Set 'Audit Policy: Account Management: Application Group Management' to 'No Auditing'	Pass: Rule passed :.

10.1.10 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Account Logon Rules

Rule Name	Result
10.1.10.1 Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to 'No Auditing'	Pass: Rule passed :.
10.1.10.2 Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing'	Pass: Rule passed :.
10.1.10.3 Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations' to 'No Auditing'	Pass: Rule passed :.
10.1.10.4 Set 'Audit Policy: Account Logon: Credential Validation' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential Validation - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

10.1.11 SOX Cyber Security Audit 0: Track access to network/financial data: Advanced Audit Policy Configuration - Privilege Use Rules

Rule Name	Result
10.1.11.1 Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No Auditing'	Pass: Rule passed :.
10.1.11.2 Set 'Audit Policy: Privilege Use: Non Sensitive Privilege Use' to 'No Auditing'	Pass: Rule passed :.

10.1.11.3 Set 'Audit Policy: Privilege Use: Sensitive Privilege Use' to 'Success and Failure'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to Success and Failure. Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Sensitive Privilege Use - Impact:If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

11 Regularly Monitor and Test Networks: SOX Cyber Security Audit 1: Regularly test security systems and processes

11.1 SOX Cyber Security Audit 1: Regularly test security systems and processes

11.1.1 SOX Cyber Security Audit 1: Regularly test security systems and processes: 11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized

Rule Name	Result
11.1.1.1 Implement File Integrity Monitoring: Verify the use of a change-detection mechanism within the financial data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities.	Pass: This rule is not automatically assessed. Use Change Tracker Gen 7 to detect all system integrity changes and implement procedures for reviewing and acknowledging Device Events as Planned Changes.

12 Maintain an Information Security Policy: SOX Cyber Security Audit 2: Maintain a policy that addresses information security for all personnel

12.1 SOX Cyber Security Audit 2: Maintain a policy that addresses information security for all personnel

12.1.1 SOX Cyber Security Audit 2: Maintain a policy that addresses information security for all personnel: Policy and Procedure Documentation

Rule Name	Result
12.1.1.1 Verify SOX SOX Cyber Security Audit 2 requirements are being operated	Pass: This rule is not automatically assessed. Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).