NNT
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

NNT ISO27K Microsoft Windows Server 2012 R2 Benchmark
27/07/2017 15:14
GEN7-IP18 (169.254.251.115,192.168.1.18)

Compliance Score : 44.23%

161 of 364 rules passed
0 of 364 rules partially passed
203 of 364 rules failed

1 A.10 Communications and operations management

1.1 ISO27001 A-10-4 Protection malicious and mobile code - Hardened Server Configuration Settings

1.1.1 A-10-4-1 Controls against malicious code - User Account Control Rules

Rule Name	Score	Pass / Fail
1.1.1.1 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'	0	Fail
1.1.1.2 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'	1	Pass
1.1.1.3 Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent on the secure desktop'	0	Fail
1.1.1.4 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	0	Fail
1.1.1.5 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'	1	Pass
1.1.1.6 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'	1	Pass
1.1.1.7 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	1	Pass
1.1.1.8 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	1	Pass
1.1.1.9 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	1	Pass

1.1.2 A-10-4-1 Controls against malicious code - Administrative Templates (Computer) Rules

Rule Name	Score	Pass / Fail
1.1.2.1 Set 'Apply UAC restrictions to local accounts on network logons' to 'Enabled'	0	Fail
1.1.2.2 Set 'WDigest Authentication' to 'Disabled'	0	Fail

1.1.3 A-10-4-1 Controls against malicious code - Attachment Manager Rules

Rule Name	Score	Pass / Fail
1.1.3.1 Set 'Do not preserve zone information in file attachments' to 'Disabled'	0	Fail
1.1.3.2 Set 'Notify antivirus programs when opening attachments' to 'Enabled'	0	Fail

1.1.4 A-10-4-1 Controls against malicious code - Windows Installer Rules

Rule Name	Score	Pass / Fail
1.1.4.1 Set 'Always install with elevated privileges' to 'Disabled'	0	Fail

1.1.5 A-10-4-1 Controls against malicious code - EMET Rules

Rule Name	Score	Pass / Fail
1.1.5.1 Ensure EMET is installed	0	Fail
1.1.5.2 Set 'Default Protections for Internet Explorer' to 'Enabled'	0	Fail
1.1.5.3 Set 'Default Protections for Popular Software' to 'Enabled'	0	Fail
1.1.5.4 Set 'Default Protections for Recommended Software' to 'Enabled'	0	Fail
1.1.5.5 Set 'System ASLR' to 'Enabled:Application Opt-In'	0	Fail
1.1.5.6 Set 'System DEP' to 'Enabled:Application Opt-Out'	0	Fail
1.1.5.7 Set 'System SEHOP' to 'Enabled:Application Opt-Out'	0	Fail

1.1.6 A-10-4-1 Controls against malicious code - Early Launch Antimalware Rules

Rule Name	Score	Pass / Fail
1.1.6.1 Set 'Boot-Start Driver Initialization Policy' to 'Enabled:Good, unknown and bad but critical'	0	Fail

1.1.7 A-10-4-1 Controls against malicious code - Internet Communication settings Rules

Rule Name	Score	Pass / Fail
1.1.7.1 Set 'Turn off downloading of print drivers over HTTP' to 'Enabled'	0	Fail
1.1.7.2 Set 'Turn off Internet download for Web publishing and online ordering wizards' to 'Enabled'	0	Fail
1.1.7.3 Set 'Turn off printing over HTTP' to 'Enabled'	0	Fail
1.1.7.4 Set 'Turn off Search Companion content file updates' to 'Enabled'	0	Fail
1.1.7.5 Set 'Turn off the "Publish to Web" task for files and folders' to 'Enabled'	0	Fail
1.1.7.6 Set 'Turn off the Windows Messenger Customer Experience Improvement Program' to 'Enabled'	0	Fail

1.1.8 A-10-4-1 Controls against malicious code - App runtime Rules

Rule Name	Score	Pass / Fail
1.1.8.1 Set 'Allow Microsoft accounts to be optional' to 'Enabled'	0	Fail

1.1.9 A-10-4-1 Controls against malicious code - AutoPlay Policies Rules

Rule Name	Score	Pass / Fail
1.1.9.1 Set 'Turn off Autoplay' to 'Enabled:All drives'	0	Fail

1.2 ISO27001 A-10-4 Protection malicious and mobile code - Approved Non-Default Services List

If any services are present that are not included in either the Default or Optional Services lists, these will be reported here. If any services are identified, their Business Justification should be reviewed and if deemed necessary, added to the Approved Non-Default Services list.

The standard requires 'enable only necessary services' and 'remove all unnecessary functionality'. There are typically more than 100 standard Windows Services installed and enabled on a Default Build system. The majority of these will not be required for the Server Role and are therefore unnecessary. These Services should be disabled and stopped to prevent any chance that malware or a hacker could exploit vulnerabilities provided by the Service. This checklist is derived from Microsoft's Knowledgebase Threats and Countermeasures Guide and Microsoft's Security Configuration Wizard

1.2.1 Approved Non-Default Services List: Services deeemed necessary for Business Services

Rule Name	Score	Pass / Fail
1.2.1.1 Check for any Non-Default Services (see Result Details report for list of exceptions)	0	Fail

1.3 ISO27001 A-10-4 Protection malicious and mobile code - Default Services List

If any Default Services are missing the rule will still pass, however any default services present must be in the correct state and startmode.

The standard requires 'enable only necessary services' and 'remove all unnecessary functionality'. There are typically more than 100 standard Windows Services installed and enabled on a Default Build system. The majority of these will not be required for the Server Role and are therefore unnecessary. These Services should be disabled and stopped to prevent any chance that malware or a hacker could exploit vulnerabilities provided by the Service. This checklist is derived from Microsoft's Knowledgebase Threats and Countermeasures Guide and Microsoft's Security Configuration Wizard

1.3.1 Mandatory Services List: Review all Mandatory Services and disable/stop all unnecessary services.

Rule Name	Score	Pass / Fail
1.3.1.1 App Readiness Service	1	Pass
1.3.1.2 Application Experience Service	1	Pass
1.3.1.3 Application Host Helper Service	1	Pass
1.3.1.4 Application Identity Service	1	Pass
1.3.1.5 Application Information Service	1	Pass
1.3.1.6 Application Layer Gateway Service	0	Fail
1.3.1.7 Application Management Service	0	Fail
1.3.1.8 AppX Deployment Service (AppXSVC) Service	0	Fail
1.3.1.9 ASP.NET State Service (aspnet_state) Service	0	Fail
1.3.1.10 Background Intelligent Transfer Service	1	Pass
1.3.1.11 Background Tasks Infrastructure (BrokerInfrastructure) Service	1	Pass

1.3.1.12 Base Filtering Engine Service	1	Pass
1.3.1.13 Certificate Propagation Service	0	Fail
1.3.1.14 CNG Key Isolation Service	1	Pass
1.3.1.15 COM+ Event System Service	1	Pass
1.3.1.16 COM+ System Application Service	0	Fail
1.3.1.17 Computer Browser Service	1	Pass
1.3.1.18 Credential Manager Service	1	Pass
1.3.1.19 Cryptographic Services Service	1	Pass
1.3.1.20 DCOM Server Process Launcher Service	1	Pass
1.3.1.21 Device Association (deviceassociationservice) Service	0	Fail
1.3.1.22 Device Install (deviceinstall) Service	0	Fail
1.3.1.23 Device Setup (dsmsvc) Service	0	Fail
1.3.1.24 DHCP Client Service	0	Fail
1.3.1.25 Diagnostic Policy Service	0	Fail
1.3.1.26 Diagnostic Service Host Service	0	Fail
1.3.1.27 Diagnostic System Host Service	0	Fail
1.3.1.28 Distributed Link Tracking Client Service	0	Fail
1.3.1.29 Distributed Transaction Coordinator Service	0	Fail
1.3.1.30 DNS Client Service	1	Pass
1.3.1.31 The Enhanced Mitigation Experience Toolkit (EMET) Service	0	Fail
1.3.1.32 Encrypting File System (EFS) Service	1	Pass
1.3.1.33 Extensible Authentication Protocol Service	1	Pass
1.3.1.34 Function Discovery Provider Host Service	0	Fail
1.3.1.35 Function Discovery Resource Publication Service	0	Fail
1.3.1.36 Group Policy Client Service	1	Pass
1.3.1.37 Health Key and Certificate Management Service	1	Pass
1.3.1.38 Human Interface Device Access Service	0	Fail
1.3.1.39 Hyper-V Data Exchange Service (vmickvpexchange) Service	0	Fail
1.3.1.40 Hyper-V Guest Service Interface (vmicguestinterface) Service	0	Fail
1.3.1.41 Hyper-V Guest Shutdown Service (vmicshutdown) Service	0	Fail
1.3.1.42 Hyper-V Heartbeat Service (vmicheartbeat) Service	0	Fail
1.3.1.43 Hyper-V Remote Desktop Virtualization Service (vmicrdv) Service	0	Fail
1.3.1.44 Hyper-V Time Synchronization Service (vmictimesync) Service	0	Fail
1.3.1.45 Hyper-V Volume Shadow Copy Requestor (vmicvss) Service	0	Fail
1.3.1.46 IKE and AuthIP IPsec Keying Modules Service	0	Fail
1.3.1.47 Interactive Services Detection Service	0	Fail
1.3.1.48 Internet Connection Sharing (ICS) Service	0	Fail
1.3.1.49 Internet Explorer ETW Collector Service	1	Pass
1.3.1.50 IP Helper Service	1	Pass
1.3.1.51 IPsec Policy Agent Service	0	Fail
1.3.1.52 KDC Proxy Server service (kpssvc) Service	0	Fail
1.3.1.53 KtmRm for Distributed Transaction Coordinator Service	0	Fail
1.3.1.54 Link-Layer Topology Discovery Mapper Service	0	Fail
1.3.1.55 Microsoft iSCSI Initiator Service	1	Pass
1.3.1.56 Microsoft Software Shadow Copy Provider Service	1	Pass
1.3.1.57 Microsoft Storage Spaces SMP (smphost) Service	1	Pass
1.3.1.58 Multimedia Class Scheduler Service	1	Pass
1.3.1.59 Net.Tcp Port Sharing Service	1	Pass
1.3.1.60 Netlogon Service	0	Fail
1.3.1.61 Network Access Protection Agent Service	1	Pass
1.3.1.62 Network Connections Service	1	Pass

1.3.1.63 Network Connectivity Assistant (ncasvc) Service	0	Fail
1.3.1.64 Network List Service	0	Fail
1.3.1.65 Network Location Awareness Service	1	Pass
1.3.1.66 Network Store Interface Service	1	Pass
1.3.1.67 Optimize Drives (defragsvc) Service	1	Pass
1.3.1.68 Performance Counter DLL Host (perfhost) Service	0	Fail
1.3.1.69 Performance Logs and Alerts Service	1	Pass
1.3.1.70 Plug and Play Service	1	Pass
1.3.1.71 Portable Device Enumerator Service	0	Fail
1.3.1.72 Power Service	1	Pass
1.3.1.73 Print Spooler Service	0	Fail
1.3.1.74 Printer Extensions and Notifications Service	0	Fail
1.3.1.75 Problem Reports and Solutions Control Panel Support Service	0	Fail
1.3.1.76 Remote Access Auto Connection Manager Service	0	Fail
1.3.1.77 Remote Access Connection Manager Service	0	Fail
1.3.1.78 Remote Desktop Configuration Service	0	Fail
1.3.1.79 Remote Desktop Services Service	0	Fail
1.3.1.80 Remote Desktop Services UserMode Port Redirector	0	Fail
1.3.1.81 Remote Procedure Call (RPC) Service	1	Pass
1.3.1.82 Remote Procedure Call (RPC) Locator Service	0	Fail
1.3.1.83 Remote Registry Service	0	Fail
1.3.1.84 Resultant Set of Policy Provider Service	0	Fail
1.3.1.85 Routing and Remote Access Service	1	Pass
1.3.1.86 RPC Endpoint Mapper Service	1	Pass
1.3.1.87 Secondary Logon Service	0	Fail
1.3.1.88 Secure Socket Tunneling Protocol Service	0	Fail
1.3.1.89 Security Accounts Manager Service	0	Fail
1.3.1.90 Server Service	0	Fail
1.3.1.91 Shell Hardware Detection Service	1	Pass
1.3.1.92 Smart Card Service	0	Fail
1.3.1.93 Smart Card Device Enumeration Service	1	Pass
1.3.1.94 Smart Card Removal Policy Service	1	Pass
1.3.1.95 SNMP Trap Service	0	Fail
1.3.1.96 Software Protection Service	1	Pass
1.3.1.97 Special Administration Console Helper Service	0	Fail
1.3.1.98 Spot Verifier Service	1	Pass
1.3.1.99 SSDP Discovery Service	0	Fail
1.3.1.100 Storage Tiers Management Service	1	Pass
1.3.1.101 Superfetch Service	1	Pass
1.3.1.102 System Event Notification Service	0	Fail
1.3.1.103 System Events Broker Service	1	Pass
1.3.1.104 Task Scheduler Service	1	Pass
1.3.1.105 TCP/IP NetBIOS Helper Service	0	Fail
1.3.1.106 Telephony Service	0	Fail
1.3.1.107 Themes Service	0	Fail
1.3.1.108 Thread Ordering Server Service	1	Pass
1.3.1.109 UPnP Device Host Service	0	Fail
1.3.1.110 User Access Logging Service	1	Pass
1.3.1.111 User Profile Service	1	Pass
1.3.1.112 Virtual Disk Service	1	Pass
1.3.1.113 Volume Shadow Copy Service	1	Pass

1.3.1.114 Windows Audio Service	1	Pass
1.3.1.115 Windows Audio Endpoint Builder Service	0	Fail
1.3.1.116 Windows Color System Service	1	Pass
1.3.1.117 Windows Connection Manager (wcmsvc) Service	1	Pass
1.3.1.118 Windows Driver Foundation - User-mode Driver Framework Service	0	Fail
1.3.1.119 Windows Encryption Provider Host Service	0	Fail
1.3.1.120 Windows Error Reporting Service	0	Fail
1.3.1.121 Windows Event Collector Service	0	Fail
1.3.1.122 Windows Event Log Service	1	Pass
1.3.1.123 Windows Firewall Service	1	Pass
1.3.1.124 Windows Font Cache (fontcache) Service	0	Fail
1.3.1.125 Windows Installer Service	1	Pass
1.3.1.126 Windows Management Instrumentation Service	1	Pass
1.3.1.127 Windows Modules Installer Service	1	Pass
1.3.1.128 Windows Presentation Foundation Font Cache (fontcache3.0.0.0) Service	0	Fail
1.3.1.129 Windows Process Activation Service Service	0	Fail
1.3.1.130 Windows Remote Management (WS-Management) Service	0	Fail
1.3.1.131 Windows Store Service (WSService)	0	Fail
1.3.1.132 Windows Time Service	1	Pass
1.3.1.133 Windows Update Service	0	Fail
1.3.1.134 WinHTTP Web Proxy Auto-Discovery Service	0	Fail
1.3.1.135 Wired AutoConfig Service	0	Fail
1.3.1.136 WMI Performance Adapter Service	1	Pass
1.3.1.137 Workstation Service	1	Pass

1.4 ISO27001 A-10-4 Protection malicious and mobile code - Optional Services List

If these services are not installed then the audit will still pass, however, if the services checked are installed they must be set to the correct Start Mode and Running state for the audit to pass.

1.4.1 Optional Services List: The following services, if installed, must be set to the correct Start Mode and Running state for the audit to pass.

Rule Name	Score	Pass / Fail
1.4.1.1 Optional Services List: NNT Agent Service (NNTAgentService)	0	Fail
1.4.1.2 Optional Services List: NNT Proxy Agent Service (NNTAgentProxyService)	1	Pass
1.4.1.3 Optional Services List: NNT Change Tracker Gen 7 MongoDB Service	1	Pass
1.4.1.4 Optional Services List: NNT Change Tracker Gen 7 Redis Service	0	Fail
1.4.1.5 Optional Services List: ASP.NET State Service (aspnet_state) Service	0	Fail
1.4.1.6 Optional Services List: World Wide Web Publishing Service	0	Fail
1.4.1.7 Optional Services List: W3C Logging Service	0	Fail

1.5 ISO27001 A-10-8 Exchange of information

1.5.1 A-10-8 Exchange of information - Network security Rules

Rule Name	Score	Pass / Fail
1.5.1.1 Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'	0	Fail
1.5.1.2 Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'	0	Fail
1.5.1.3 Set 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' to 'Disabled'	0	Fail
1.5.1.4 Set 'Network Security: Configure encryption types allowed for Kerberos' to 'RC4\AES128\AES256\Future types'	0	Fail
1.5.1.5 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'	1	Pass
1.5.1.6 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	0	Fail
1.5.1.7 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher	1	Pass
1.5.1.8 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	0	Fail
1.5.1.9 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'	0	Fail

2 A.11 Access control

2.1 ISO27001 A-11-1 Business requirement for access control

2.1.1 A-11-1-1 Access control policy - Account Lockout Policy

Rule Name	Score	Pass / Fail
2.1.1.1 Set 'Account lockout duration' to '15 or more minute(s)'	1	Pass
2.1.1.2 Set 'Account lockout threshold' to 10 or fewer invalid logon attempt(s), but not 0	1	Pass
2.1.1.3 Set 'Reset account lockout counter after' to '15 or more minute(s)'	1	Pass

2.1.2 A-11-1-1 Access control policy - Local Policies Rules

Rule Name	Score	Pass / Fail
2.1.2.1 Set 'Access Credential Manager as a trusted caller' to 'No One'	1	Pass
2.1.2.2 Set 'Access this computer from the network'	0	Fail
2.1.2.3 Set 'Act as part of the operating system' to 'No One'	1	Pass
2.1.2.4 Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	0	Fail
2.1.2.5 Set 'Allow log on locally' to 'Administrators'	0	Fail
2.1.2.6 Configure 'Allow log on through Remote Desktop Services'	1	Pass
2.1.2.7 Set 'Back up files and directories' to 'Administrators'	0	Fail
2.1.2.8 Set 'Change the system time' to 'Administrators, LOCAL SERVICE'	1	Pass
2.1.2.9 Set 'Change the time zone' to 'Administrators, LOCAL SERVICE'	1	Pass
2.1.2.10 Set 'Create a pagefile' to 'Administrators'	1	Pass
2.1.2.11 Set 'Create a token object' to 'No One'	1	Pass
2.1.2.12 Set 'Create global objects' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	1	Pass
2.1.2.13 Set 'Create permanent shared objects' to 'No One'	1	Pass
2.1.2.14 Set 'Create symbolic links' to 'Administrators'	1	Pass
2.1.2.15 Set 'Debug programs' to 'Administrators'	1	Pass
2.1.2.16 Set 'Deny access to this computer from the network'	0	Fail
2.1.2.17 Set 'Deny log on as a batch job' to include 'Guests'	0	Fail
2.1.2.18 Set 'Deny log on as a service' to include 'Guests'	0	Fail
2.1.2.19 Set 'Deny log on locally' to include 'Guests'	0	Fail
2.1.2.20 Set 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	0	Fail
2.1.2.21 Set 'Enable computer and user accounts to be trusted for delegation'	1	Pass
2.1.2.22 Set 'Force shutdown from a remote system' to 'Administrators'	1	Pass
2.1.2.23 Set 'Generate security audits' to 'LOCAL SERVICE, NETWORK SERVICE'	0	Fail
2.1.2.24 Set 'Impersonate a client after authentication' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	0	Fail
2.1.2.25 Set 'Increase scheduling priority' to 'Administrators'	1	Pass
2.1.2.26 Set 'Load and unload device drivers' to 'Administrators'	1	Pass
2.1.2.27 Set 'Lock pages in memory' to 'No One'	1	Pass
2.1.2.28 Set 'Manage auditing and security log' to 'Administrators'	1	Pass
2.1.2.29 Set 'Modify an object label' to 'No One'	1	Pass
2.1.2.30 Set 'Modify firmware environment values' to 'Administrators'	1	Pass
2.1.2.31 Set 'Perform volume maintenance tasks' to 'Administrators'	1	Pass
2.1.2.32 Set 'Profile single process' to 'Administrators'	1	Pass
2.1.2.33 Set 'Profile system performance' to 'Administrators, NT SERVICE\WdiServiceHost'	1	Pass
2.1.2.34 Set 'Replace a process level token' to 'LOCAL SERVICE, NETWORK SERVICE'	0	Fail
2.1.2.35 Set 'Restore files and directories' to 'Administrators'	0	Fail
2.1.2.36 Set 'Shut down the system' to 'Administrators'	0	Fail
2.1.2.37 Set 'Take ownership of files or other objects' to 'Administrators'	1	Pass

2.1.3 A-11-1-1 Access control policy - Domain member Rules

Rule Name	Score	Pass / Fail
2.1.3.1 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'	1	Pass
2.1.3.2 Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'	1	Pass
2.1.3.3 Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled'	1	Pass
2.1.3.4 Set 'Domain member: Disable machine account password changes' to 'Disabled'	1	Pass
2.1.3.5 Set 'Domain member: Maximum machine account password age' to 30 or fewer days, but not 0	1	Pass
2.1.3.6 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled'	1	Pass

2.1.4 A-11-1-1 Access control policy - Interactive logon Rules

Rule Name	Score	Pass / Fail
2.1.4.1 Set 'Interactive logon: Do not display last user name' to 'Enabled'	0	Fail
2.1.4.2 Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'	1	Pass
2.1.4.3 Set 'Interactive logon: Machine inactivity limit' to 900 or fewer second(s), but not 0	0	Fail
2.1.4.4 Configure 'Interactive logon: Message text for users attempting to log on'	0	Fail
2.1.4.5 Configure 'Interactive logon: Message title for users attempting to log on'	0	Fail
2.1.4.6 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'	0	Fail
2.1.4.7 Set 'Interactive logon: Prompt user to change password before expiration' to 'between 5 and 14 days'	1	Pass
2.1.4.8 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation'	0	Fail

2.1.5 A-11-1-1 Access control policy - Microsoft network client Rules

Rule Name	Score	Pass / Fail
2.1.5.1 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	0	Fail
2.1.5.2 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'	1	Pass
2.1.5.3 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'	1	Pass

2.1.6 A-11-1-1 Access control policy - Devices Rules

Rule Name	Score	Pass / Fail
2.1.6.1 Set 'Devices: Allowed to format and eject removable media' to 'Administrators'	0	Fail
2.1.6.2 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled'	1	Pass

2.1.7 A-11-1-1 Access control policy - Remote Assistance Rules

Rule Name	Score	Pass / Fail
2.1.7.1 Set 'Configure Offer Remote Assistance' to 'Disabled'	0	Fail
2.1.7.2 Set 'Configure Solicited Remote Assistance' to 'Disabled'	0	Fail

2.1.8 A-11-1-1 Access control policy - Remote Procedure Call Rules

Rule Name	Score	Pass / Fail
2.1.8.1 Set 'Enable RPC Endpoint Mapper Client Authentication' to 'Enabled'	0	Fail

2.1.9 A-11-1-1 Access control policy - MSS Rules

Rule Name	Score	Pass / Fail
2.1.9.1 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled'	1	Pass
2.1.9.2 Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	0	Fail
2.1.9.3 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'	0	Fail
2.1.9.4 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled'	0	Fail
2.1.9.5 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' to '5 or fewer seconds'	0	Fail
2.1.9.6 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90% or less'	0	Fail

2.1.10 A-11-1-1 Access control policy - Recovery console Rules

Rule Name	Score	Pass / Fail
2.1.10.1 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'	1	Pass
2.1.10.2 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled'	1	Pass

2.1.11 A-11-1-1 Access control policy - Shutdown Rules

Rule Name	Score	Pass / Fail
2.1.11.1 Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'	1	Pass

2.1.12 A-11-1-1 Access control policy - System objects Rules

Rule Name	Score	Pass / Fail
2.1.12.1 Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled'	1	Pass
2.1.12.2 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled'	1	Pass

2.1.13 A-11-1-1 Access control policy - Logon Rules

Rule Name	Score	Pass / Fail
2.1.13.1 Set 'Do not display network selection UI' to 'Enabled'	0	Fail

2.2 ISO27001 A-11-2 User access management

2.2.1 A-11-2-3 User access management - User password management

Rule Name	Score	Pass / Fail
2.2.1.1 Set 'Enforce password history' to '24 or more password(s)'	0	Fail
2.2.1.2 Set 'Maximum password age' to 60 or fewer days, but not 0	0	Fail
2.2.1.3 Set 'Minimum password age' to '1 or more day(s)'	0	Fail
2.2.1.4 Set 'Minimum password length' to '14 or more character(s)'	1	Pass
2.2.1.5 Set 'Password must meet complexity requirements' to 'Enabled'	1	Pass
2.2.1.6 Set 'Store passwords using reversible encryption' to 'Disabled'	1	Pass

2.3 ISO27001 A-11-4 Network access control

2.3.1 A-11-4-6 Network connection control: Windows Firewall With Advanced Security - Domain

Rule Name	Score	Pass / Fail
2.3.1.1 Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)'	1	Pass
2.3.1.2 Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)'	1	Pass
2.3.1.3 Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)'	1	Pass
2.3.1.4 Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)'	0	Fail
2.3.1.5 Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	1	Pass
2.3.1.6 Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)'	1	Pass
2.3.1.7 Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)'	1	Pass
2.3.1.8 Set 'Windows Firewall: Domain: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	1	Pass
2.3.1.9 Set 'Windows Firewall: Domain: Logging: Size limit (KB)' to '16,384 KB or greater '	1	Pass
2.3.1.10 Set 'Windows Firewall: Domain: Logging: Log dropped packets' to 'Yes'	1	Pass
2.3.1.11 Set 'Windows Firewall: Domain: Logging: Log successful connections' to 'Yes'	1	Pass

2.3.2 A-11-4-6 Network connection control: Windows Firewall With Advanced Security - Private Profile

Rule Name	Score	Pass / Fail
2.3.2.1 Set 'Windows Firewall: Private: Firewall state' to 'On (recommended)'	1	Pass
2.3.2.2 Set 'Windows Firewall: Private: Inbound connections' to 'Block (default)'	1	Pass
2.3.2.3 Set 'Windows Firewall: Private: Outbound connections' to 'Allow (default)'	1	Pass
2.3.2.4 Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)'	0	Fail
2.3.2.5 Set 'Windows Firewall: Private: Allow unicast response' to 'No'	1	Pass
2.3.2.6 Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'	1	Pass
2.3.2.7 Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)'	1	Pass
2.3.2.8 Set 'Windows Firewall: Private: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	1	Pass
2.3.2.9 Set 'Windows Firewall: Private: Logging: Size limit (KB)' to '16,384 KB or greater'	1	Pass

2.3.2.10 Set 'Windows Firewall: Private: Logging: Log dropped packets' to 'Yes'	1	Pass
2.3.2.11 Set 'Windows Firewall: Private: Logging: Log successful connections' to 'Yes'	1	Pass

2.3.3 A-11-4-6 Network connection control: Windows Firewall With Advanced Security - Public Profile

Rule Name	Score	Pass / Fail
2.3.3.1 Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)'	0	Fail
2.3.3.2 Set 'Windows Firewall: Public: Inbound connections' to 'Block (default)'	0	Fail
2.3.3.3 Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)'	0	Fail
2.3.3.4 Set 'Windows Firewall: Public: Display a notification' to 'Yes'	1	Pass
2.3.3.5 Set 'Windows Firewall: Public: Allow unicast response' to 'No'	1	Pass
2.3.3.6 Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)'	0	Fail
2.3.3.7 Set 'Windows Firewall: Public: Apply local connection security rules' to 'No'	1	Pass
2.3.3.8 Set 'Windows Firewall: Public: Logging: Name' to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	1	Pass
2.3.3.9 Set 'Windows Firewall: Public: Logging: Size limit (KB)' to '16,384 KB or greater'	1	Pass
2.3.3.10 Set 'Windows Firewall: Public: Logging: Log dropped packets' to 'Yes'	1	Pass
2.3.3.11 Set 'Windows Firewall: Public: Logging: Log successful connections' to 'Yes'	1	Pass

2.3.4 A-11-4-6 Network connection control: Remote Desktop Services (formerly Terminal Services)-Remote Desktop Connection Client Rules

Rule Name	Score	Pass / Fail
2.3.4.1 Set 'Do not allow passwords to be saved' to 'Enabled'	0	Fail

2.3.5 A-11-4-6 Network connection control: Remote Desktop Services (formerly Terminal Services)-Remote Desktop Session Host-Device and Resource Redirection Rules

Rule Name	Score	Pass / Fail
2.3.5.1 Set 'Do not allow drive redirection' to 'Enabled'	0	Fail

2.3.6 A-11-4-6 Network connection control: Remote Desktop Services (formerly Terminal Services)-Remote Desktop Session Host-Security Rules

Rule Name	Score	Pass / Fail
2.3.6.1 Set 'Always prompt for password upon connection' to 'Enabled'	0	Fail
2.3.6.2 Set 'Set client connection encryption level: Encryption Level' to 'Enabled: High Level'	0	Fail

2.4 ISO27001 A-11-5 Operating system access control

2.4.1 A-11-5-1 Operating system access control: Secure log-on procedures - Network access Rules

Rule Name	Score	Pass / Fail
2.4.1.1 Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'	1	Pass
2.4.1.2 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'	1	Pass
2.4.1.3 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'	0	Fail
2.4.1.4 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'	1	Pass
2.4.1.5 Configure 'Network Access: Named Pipes that can be accessed anonymously'	1	Pass
2.4.1.6 Set 'Network access: Remotely accessible registry paths'	1	Pass
2.4.1.7 Set 'Network access: Remotely accessible registry paths and sub-paths'	1	Pass
2.4.1.8 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'	1	Pass
2.4.1.9 Set 'Network access: Shares that can be accessed anonymously' to 'None'	1	Pass
2.4.1.10 Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves'	1	Pass

2.4.2 A-11-5-1 Operating system access control: Windows Logon Options Rules

Rule Name	Score	Pass / Fail
2.4.2.1 Set 'Sign-in last interactive user automatically after a system-initiated restart' to 'Disabled'	1	Pass

2.4.3 A-11-5-1 Operating system access control: Windows Remote Management (WinRM)-WinRM Client Rules

Rule Name	Score	Pass / Fail
2.4.3.1 Set 'Allow Basic authentication' to 'Disabled'	0	Fail

2.4.3.2 Set 'Allow unencrypted traffic' to 'Disabled'	0	Fail
2.4.3.3 Set 'Disallow Digest authentication' to 'Enabled'	0	Fail

2.4.4 A-11-5-2 User identification and authentication- Accounts Rules

Rule Name	Score	Pass / Fail
2.4.4.1 Set 'Accounts: Block Microsoft accounts' to 'Users can't add or log on with Microsoft accounts'	0	Fail
2.4.4.2 Set 'Accounts: Guest account status' to 'Disabled'	1	Pass
2.4.4.3 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'	1	Pass
2.4.4.4 Configure 'Accounts: Rename administrator account'	0	Fail
2.4.4.5 Configure 'Accounts: Rename guest account'	0	Fail

2.4.5 A-11-5-4 Use of system utilities: Group Policy Rules

Rule Name	Score	Pass / Fail
2.4.5.1 Set 'Configure registry policy processing: Do not apply during periodic background processing' to 'False'	0	Fail
2.4.5.2 Set 'Configure registry policy processing: Process even if the Group Policy objects have not changed' to 'True'	0	Fail

2.4.6 A-11-5-5 Session time-out: Personalization Rules

Rule Name	Score	Pass / Fail
2.4.6.1 Set 'Enable screen saver' to 'Enabled'	0	Fail
2.4.6.2 Set 'Force specific screen saver: Screen saver executable name' to 'Enabled:scrnsave.scr'	0	Fail
2.4.6.3 Set 'Password protect the screen saver' to 'Enabled'	0	Fail

2.4.7 A-11-5-6 Limitation of connection time: Microsoft network server Rules

Rule Name	Score	Pass / Fail
2.4.7.1 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15 or fewer minute(s)'	1	Pass
2.4.7.2 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'	0	Fail
2.4.7.3 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'	0	Fail
2.4.7.4 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled'	1	Pass
2.4.7.5 Set 'Microsoft network server: Server SPN target name validation level' to 'Accept if provided by client'	0	Fail

3 A.12 Information systems acquisition, development and maintenance

3.1 ISO27001 A-12-6 Technical Vulnerability Management

3.1.1 A-12-6-1 Control of technical vulnerabilities

Rule Name	Score	Pass / Fail
3.1.1.1 Set 'Configure Automatic Updates' to 'Enabled'	0	Fail
3.1.1.2 Set 'Configure Automatic Updates: Scheduled install day' to '0 - Every day'	0	Fail
3.1.1.3 Set 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' to 'Disabled'	0	Fail
3.1.1.4 Set 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' to 'Disabled'	0	Fail
3.1.1.5 Set 'No auto-restart with logged on users for scheduled automatic updates installations' to 'Disabled'	0	Fail
3.1.1.6 Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled:1 minute'	0	Fail

4 A.15 Compliance

4.1 ISO27001 A-15-2 Compliance security policies - Advanced Audit Policy Configuration Rules

4.1.1 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - Account Logon

Rule Name	Score	Pass / Fail
4.1.1.1 Set 'Audit Credential Validation' to 'Success and Failure'	0	Fail

4.1.2 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - Account Management

Rule Name	Score	Pass / Fail
4.1.2.1 Set 'Audit Computer Account Management' to 'Success and Failure'	0	Fail
4.1.2.2 Set 'Audit Other Account Management Events' to 'Success and Failure'	0	Fail
4.1.2.3 Set 'Audit Security Group Management' to 'Success and Failure'	0	Fail
4.1.2.4 Set 'Audit User Account Management' to 'Success and Failure'	0	Fail

4.1.3 A-15-2 Compliance security policies - Advanced Audit Policy Configuration Rules - Detailed Tracking

Rule Name	Score	Pass / Fail
4.1.3.1 Set 'Audit Process Creation' to 'Success'	0	Fail

4.1.4 A-15-2 Compliance security policies - Advanced Audit Policy Configuration Rules - Logoff Rules

Rule Name	Score	Pass / Fail
4.1.4.1 Set 'Audit Account Lockout' to 'Success'	0	Fail
4.1.4.2 Set 'Audit Logoff' to 'Success'	1	Pass
4.1.4.3 Set 'Audit Logon' to 'Success and Failure'	1	Pass
4.1.4.4 Set 'Audit Other Logon/Logoff Events' to 'Success and Failure'	0	Fail
4.1.4.5 Set 'Audit Special Logon' to 'Success'	0	Fail

4.1.5 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - Object Access

Rule Name	Score	Pass / Fail
4.1.5.1 Set 'Audit Removable Storage' to 'Success and Failure'	0	Fail

4.1.6 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - Policy Change

Rule Name	Score	Pass / Fail
4.1.6.1 Set 'Audit Audit Policy Change' to 'Success and Failure'	0	Fail
4.1.6.2 Set 'Audit Authentication Policy Change' to 'Success'	0	Fail

4.1.7 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - Privilege Use

Rule Name	Score	Pass / Fail
4.1.7.1 Set 'Audit Sensitive Privilege Use' to 'Success and Failure'	0	Fail

4.1.8 A-15-2 Compliance security policies: Advanced Audit Policy Configuration Rules - System

Rule Name	Score	Pass / Fail
4.1.8.1 Set 'Audit IPsec Driver' to 'Success and Failure'	0	Fail
4.1.8.2 Set 'Audit Other System Events' to 'Success and Failure'	0	Fail
4.1.8.3 Set 'Audit Security State Change' to 'Success and Failure'	0	Fail
4.1.8.4 Set 'Audit Security System Extension' to 'Success and Failure'	0	Fail
4.1.8.5 Set 'Audit System Integrity' to 'Success and Failure'	0	Fail

4.1.9 A-15-2 Compliance security policies: Event Log Service-Application Rules

Rule Name	Score	Pass / Fail
4.1.9.1 Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'	0	Fail
4.1.9.2 Set 'Application: Maximum Log Size (KB)' to 'Enabled:32,768 or greater'	0	Fail

4.1.10 A-15-2 Compliance security policies: Event Log Service-Security Rules

Rule Name	Score	Pass / Fail
4.1.10.1 Set 'Security: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'	0	Fail
4.1.10.2 Set 'Security: Maximum Log Size (KB)' to 'Enabled:196,608 or greater'	0	Fail

4.1.11 A-15-2 Compliance security policies: Event Log Service-Setup Rules

Rule Name	Score	Pass / Fail
4.1.11.1 Set 'Setup: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'	0	Fail
4.1.11.2 Set 'Setup: Maximum Log Size (KB)' to 'Enabled:32,768 or greater'	0	Fail

4.1.12 A-15-2 Compliance security policies: Event Log Service-System Rules

Rule Name	Score	Pass / Fail
4.1.12.1 Set 'System: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'	0	Fail
4.1.12.2 Set 'System: Maximum Log Size (KB)' to 'Enabled:32,768 or greater'	0	Fail