Control Guidance

Top 10 Network Security Findings

Document Control Information

Version	1.2
Revision	2
Issued	26/11/2025
Annual Review	Q4
Process Owner	Abhinandan Kumar
Program Owner	Abhinandan Kumar
Approved by	Abhinandan Kumar
Functional Team	GE Vernova Third Party Security
Document Classification	GE Vernova Public

Version Control

The Process owner(s) are responsible for maintaining the master copy of the document and keeping the document updated annually to incorporate any changes in the process.

Revision Number	Date of Issue	Author(s)	Reviewer(s) /Approver(s)	Brief Description of Changes
1	7/5/2022	Aaron Kunec	David Prescott	Final Draft
2	26/112025	Aakash Singhal	Abhinandan Kumar	Updated for GE Vernova

Network Security - 2b

Risk Rating: **High**

Control Question - Do firewall ruleset terms include "ANY" or similar terms that allow all possible combinations of Internet Protocol (IP) addresses, TCP/UDP port numbers, or protocols? Note: If "Yes", please include comments for the scenarios where "Any" is used. **What is the risk?** In general, an "any" rule could allow ANY traffic from the source the rule is applied too (IP address, MAC address, or Port). This is bad practice when it comes to applying a firewall rule set. The conventional approach is to block everything and add exceptions for what you need to allow. **What we are looking for:** Statement attesting that Your organization has implemented firewall rules without " ANY " in all the 3 fields i.e. Source, Destination and Service/Ports/Protocols. If there are rules matching this criterion, please provide documentation on the business justification to have such rules.	
Acceptable Compensating Controls	Statement attesting to the following points • Internal approval by upper management for all rule sets that include the term 'Any' • Which ports are open with the term 'ANY' applied. • Which specific IP sources and destinations are allowed over open with the term 'ANY' applied.

Network Security - 2c

Risk Rating: **High**

Control Question - Are high risk protocols (e.g., NetBIOS, Telnet, FTP, etc.) and high-risk ports (20, 21, 23, 25, etc.) blocked on your organization's perimeter firewall? **What is the risk?** Protocols such as NETBOIS, Telnet and FTP are inherently insecure. For example, with NetBIOS, an attacker computer could make contact to any host on your LAN and claim that they are a particular service the host regularly connects with, such as a file server. This could result in a middleperson attack against listening hosts, and the compromise of credentials. With the use of telnet credential information (usernames and passwords) submitted through the protocol are not encrypted and is therefore vulnerable to identity theft. Finally, FTP does not offer data encryption. When files are sent using this protocol, data, usernames, and passwords are all shared in plain text, a bad actor can access this information with little to no effort. **What we are looking for:** Statement attesting that Your organization has implemented firewall rules without any high-risk protocols or ports such NetBIOS, Telnet, FTP, SSL etc. on the perimeter firewall.	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Network Security - 2d

Risk Rating: **High**

Control Question - Are network level firewall rulesets reviewed semi-annually (at a minimum)? **What is the risk?** Firewalls are not a set and forget network appliance. They require regular maintenance and reconfiguration. Due to the level of administrative involvement, misconfigurations are common. Not performing a periodic firewall ruleset review can leave your organization open to undiscovered configuration gaps that could render the appliance ineffective. **What we are looking for:** Statement attesting that your organization has established a semi - annual process to periodically review the firewall rules to validate whether they are still needed or if there are any redundant firewall rules.	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Network Security – 3

Risk Rating: **High**

Control Question - Is network level authentication used to limit and control which devices can be connected to your organization's network? **What is the risk?** A network that does not have network level authentication (NLA) enabled is more vulnerable to Denial of Service (DOS) and Man-in-the- Middle (MiTM) attacks. Network level authentication (NLA) creates an additional layer that helps prevents attackers from reaching internal systems and bogging down critical services, or intercepting communications between clients and servicer. **What we are looking for:** Statement attesting to the use of network level authentication	
Acceptable Compensating Controls	Statement attesting to the following points. • GEV data is segregated from the general network with limited user account access. • An annual audit is conducted to identify and disable any unnecessary devices connectivity. • All network level devices are catalogued under a centralized management utility. • External IPs are blocked or filtered from a direct connect to LAN devices • Any unauthorized devices should trigger an alert to IT or Cyber team

Network Security – 4

Risk Rating: **Critical**

Note: A statement alone is not sufficient for Control Questions with a Risk Rating of Critical. Attaching evidence is required to meet the control standards

Control Question - Are firewalls (physical or virtual) used to segment your organization's network into untrusted and trusted zones (internet, demilitarized zone (DMZ), internal network)? **What is the risk?** If network segmentation has not been implemented, a bad actor can easily move across your network. For instance, movement can be made from a summer intern's workstation directly to the workstation of a system administrator in charge of a server holding social security numbers. Even though there is no business reason for the intern to access the

sysadmin's workstation, without proper network segmentation, there is nothing stopping those hosts from communicating – and from the intern being able to pull other employee's information.

What we are looking for: Evidence that your organization that has segmented your network into various zones through firewalls. At a minimum, you should segment the network into zones such as – Untrusted network (Internet or any foreign network), Trusted network zone (internal network, Demilitarized zone DMZ).

Your organization should also consider capturing the network segmentation through a network architecture or topology diagram.

Network Security – 5

Risk Rating: **Critical**

Note: A statement alone is not sufficient for Control Questions with a Risk Rating of Critical. Attaching evidence is required to meet the control standards

Control Question - Is a network level intrusion detection or prevention system implemented to monitor the network where GEV data will be stored? **What is the risk?** Not having a NIDS or NIPS in place can delay event response time. A well-tuned NIDS or NIPS will alert your IT security staff of potential malicious activity in real-time. Common malicious activity includes Denial-of-Service (DoS), port-scans, and ping sweeps. **What we are looking for:** Evidence that your organization has implemented a network intrusion detection or prevention system to monitor the network where GEV data will be stored or processed. Your organization should consider configuring the network intrusion detection or prevention system ruleset to identify and detect/prevent all malicious activity, intrusion attempts or any anomalies in the network.	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Network Security - 5a

Risk Rating: **High**

Control Question - Is the network level intrusion detection or prevention system monitor on a 24x7x365 basis for "Critical" and "High" alerts? **What is the risk?** Bad actors understand most originations do not have 24x7x365 security monitoring. Often, malicious activity is more prevent after hours, during the weekends, or over a holiday break. **What we are looking for:** Statement attesting that Your organization has implemented a process to monitor all critical and high alerts from network intrusion detection or prevention systems on a 24x7x365 basis. The process should include actions taken by your organization to address critical or high alerts identified.	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Network Security - 6a

Risk Rating: **High**

Control Question – Do your wireless access points require users to authenticate with a unique username and password? **What is the risk?** failure to secure your wireless network could open your internet connection to unintended usage. These users may be able to use your WIFI to conduct illegal activity, monitor and capture your web traffic, steal personal files, or clone your hotspot to conduct malicious activity on unsuspecting victims. **What we are looking for:** Statement attesting that Your organization has configured all the wireless access points/wireless LAN controllers with authentication settings (e.g.: username, password, certificate-based authentication etc.) for all end users

Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Network Security – 7

Risk Rating: **Critical**

Note: A statement alone is not sufficient for Control Questions with a Risk Rating of Critical. Attaching evidence is required to meet the control standards

Control Question - Is multi-factor authentication required to access your organization's network remotely? Note: Two factor authentication requires at least two of the following: 1. Something you have (e.g., RSA Pin), 2. Something you know (e.g., Password), and/or 3. Something you are (e.g., Fingerprint scan) **What is the risk?** Once the username and password are acquired, every transaction will be treated as valid, and basic security measures cannot prevent it. This is what makes Phishing attacks a favourite among bad actors. Adding an additional layer of authentication at the network level decreases the chances of success for an attacker using stolen credentials to traverse your organizations network. **What we are looking for:** Evidence of compliance with a Multi-Factor Authentication (MFA) policy. Please provide one of the following: • Written Policy approved by company management listing additional authentication factor other than Passwords • Screen shot of enabled second factor authentication management console • Screenshot of a user login requiring while connecting remotely to your network	
Acceptable Compensating Controls	Supply evidence that attests to the following points. • all remote access users are catalogued under a centralized management role-based access control (RBAC) structure. • An annual audit is in place to identify and disable any unnecessary access or privileges that have been granted to remote users. • An attribute-based access control (ABAC) model has been implemented • Statement attesting to remote users are governed by Just-in-Time Privileged Access Management (JIT PAM) via a Privileged Access Management (PAM) systems

Network Security – 8

Risk Rating: **Moderate**

Control Question - Does your organization perform checks on a periodic basis to detect and deactivate unauthorized (i.e. rouge) access points from your network? **What is the risk?** One of the most common WIFI based attacks is known as an Evil Twin attack. In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate the access point. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it is easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. **What we are looking for:** Statement attesting that your organization has implemented a formalized process (i.e. asset management) to periodically scan and remove unauthorized or rogue wireless access points from your network.

Acceptable Compensating Controls	Supply evidence that attests to the following points. • WIFI network should be segregated by guest and employee • Guest WIFI should not allow access to internal systems • Regular alerts when unauthorised devices are connected to network • WPA2 (Wi-Fi Protected Access 2) mechanism is in place.