Control Guidance

Top 10 Access Management Findings

Document Control Information

Version	1.2
Revision	2
Issued	26/11/2025
Annual Review	Q4
Process Owner (s)	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	26/11/2025	Aakash Singhal	Abhinandan Kumar	Updated for GE Vernova

Access Management – 26

Risk Rating: **High**

Control Question - Are interactive logins disabled for non-personal accounts (e.g., service accounts)?

What is the risk?
Highly Privileged accounts (Admin or root, Local Admin, Superuser) - These types of accounts are highly coveted by bad actors for their unrestricted access to file systems and system settings. Often these accounts are used to bypass or disable security setting rendering a company's network completely open to data exposure, data exfiltration, and the malicious destruction of data.

Generic User accounts - These types of accounts are shared and use a standard naming convention (e.g., Admin, Clerk, Shopfloor, etc.) meaning there is no corresponding single user associated with the account. Often this type of account is shared among multiple employees. These types of accounts are difficult to audit thus difficult to know who may have been using the credentials if the account is being used by someone with malicious intent.

Service accounts - These non-personal accounts are used by a system or multiple systems to run various automated tasks. Service accounts can require privileged access to servers, applications, and databases. By compromising a service account, attackers are potentially able to move vertically or laterally across the network to gain access to sensitive or restricted data.

What we are looking for: Statement attesting that Your organization has an established policy/procedure regarding whether your organization allows interactive logins for non-personal accounts in the production environment. If allowed, how are the accounts managed?

Acceptable Compensating Controls	Supply a statement attesting to all the following points. • Non-personal accounts are restricted from accessing GEV data. • An annual audit is conducted to find and disable non- personnel accounts that are no longer in use. • All non-personnel accounts have been catalogued under a centralized management utility. Or supply a statement attesting to the following… • Privileged Access Management PAM solution is place.

Access Management – 28

Risk Rating: **High**

Control Question - Are non-personal accounts approved (or pre-approved) for a specific timeframe after which time the password must be immediately changed?

What is the risk? Password expiration policies help mitigate the threat of Advanced Persistent Threats (APTs) by shorting's an attacker's time limits to crack passwords. The shorter the password expiration policy, the smaller the window to compromise systems and exfiltrate data

What we are looking for: Statement attesting that Your organization has an established policy/procedure regarding whether your organization has implemented a specific length of time (e.g., 120 days), after which point the password must be immediately changed for non-personal accounts?

Acceptable Compensating Controls	Supply a statement attesting to all the following points. • Non-personal accounts are restricted from accessing GEV data • An annual audit is conducted to identify and disable non- personnel accounts that are no longer in use. • All non-personnel accounts are catalogued under a centralized management utility. Or supply a statement attesting to the following… • Privileged Access Management PAM solution is place.

Access Management – 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 - Are all user accounts (including highly privileged accounts and emergency accounts) unique and traceable to a single owner? **What is the risk?** Sharing user account comes with risk. Notably… • Loss of accountability. Investigating negative user impact (Data Theft or loss, data exposer, system misconfigurations, lock outs, etc.…) becomes exponentially more difficult if an account is shared among multiple users or multiple platforms • Improve the chances of sniffing, phishing, and social engineering. **What we are looking for:** Evidence of compliance with a policy that demonstrates your organization has implemented unique user accounts for all employees irrespective of the type of account. (Normal user account, administrative accounts, highly privileged accounts, emergency accounts etc.)	
Acceptable Compensating Controls	Supply a statement attesting to all the following points. • Only unique accounts can access GEV data • Non-personal accounts are restricted from accessing GEV data

Access Management – 6

Risk Rating: **High**

Control Question - Are all user accounts deactivated within 90 days of inactivity? **What is the risk?** Inactive accounts may appear docile, but they can cause extensive damage to an organization, especially when they are not disabled or when they remain without password expiry limits. Outside intruders trying to hack into an organization can use these accounts as their activities will go unnoticed. Also, employees who quit the organization can misuse their login credentials to access network resources. **What we are looking for:** Statement attesting to Your organization has implemented technical mechanisms by which all user accounts without any activity or transaction for 90 days are de-activated automatically.	
Acceptable Compensating Controls	Supply evidence that attests to the following point. • A manual quarterly audit is conducted and documented to identify and de-activate inactive accounts.

Access Management - 7

Risk Rating: **High**

Control Question - Are all user and system/service accounts removed or stripped of all access rights within one year of inactivity?

What is the risk? A lingering inactive account can still pose a threat to your organization. Especially if the account is highly privileged or has elevated access rights. A savvy bad actor (internal or external) could reactive one of these deactivated accounts for malicious purposes.

What we are looking for: Statement attesting that your organization has implemented a technical mechanism by which all user, system and service accounts without any activity 1 year is deleted.

Acceptable Compensating Controls	Supply a statement attesting to the following point. • A manual annual audit is conducted and documented to identify and remove deactivated accounts.

Access Management - 13

Risk Rating: **High**

Control Question - Are the following password requirements enforced for access to networks, systems, and applications that process and/or store GEV data:

1. Minimum password length of eight characters
2. Maximum of ten incorrect login attempts

Note: If all aspects above are not met, please answer "No" and indicate which aspects are not implemented or please include the current password length and the number of incorrect login attempts.

What is the risk? Shorter non-complex passwords are easy to guess or crack using password cracking tools. Additionally, networks, systems, and applications are vulnerable to brute force attacks if accounts do not lock after a defined number of incorrect authentication attempts.

What we are looking for: Statement attesting to that your organization has implemented a password policy for all networks, systems, and applications that process and/or store GEV data.

Example of such password policies includes, but not limited to:
1. Minimum password length of eight characters
2. Maximum of ten incorrect login attempts

Acceptable Compensating Controls	Supply a statement attesting to the following points. • Password policy is enforcing the use of uppercase, lowercase, number, and special characters • Password policy is enforcing maximu006D of ten incorrect login attempts

Access Management - 16

Risk Rating: **High**

Control Question - Is privileged account access managed by a centralized server(s) (e.g., RSA, RADIUS, TACACS, or LDAP)?

Note: If local accounts on servers exist, please answer "No" and provide a business justification for the use of local privileged accounts. Highly Privileged Accounts include, but are not limited to server administrators, network administrators, domain administrations, and database administrators.

What is the risk? A decentralized system can lead to inconsistent policy enforcement across the enterprises, which can be just as bad as having no policies at all. Further, even the best IT team will have trouble scaling appropriately and managing a growing company's accounts, permissions, credentials, and assets. A decentralized or manual privileged access management process inevitably leaves security gaps that bad actors can exploit.

What we are looking for: Statement attesting that your organization has implemented a centralized access management solution for managing and controlling privileged accounts. Examples of such solutions - RADIUS, TACACS, LDAP etc.

Acceptable Compensating Controls	Supply a statement attesting to the following points. • Privileged accounts are restricted to specific personnel • Password policy is enforcing the use of uppercase, lowercase, number, and special characters • Password policy is enforcing maximum of ten incorrect login attempts • password resets are enforced every 90 days for all user and highly privileged accounts.

Access Management - 23

Risk Rating: **High**

Control Question - For systems, computers, devices, and applications that access, process, and/or store GEV sensitive data, are sessions set to timeout after 30 minutes of inactivity?

What is the risk? The lack of proper session expiration creates a domino effect that may increase the success of session hacking or brute force attacks. A long expiration time increases an attacker's chance of successfully guessing a valid session ID or password. The longer the expiration time, the more concurrent open sessions will exist at any given time. The larger the pool of sessions, the more likely an attacker will guess a session ID or password at random.

What we are looking for: Statement attesting that your organization has established a formalized process (i.e., system hardening) to programmatically set and enforce session timeouts after 30 minutes of user inactivity prior to being allowed on the production network.

Acceptable Compensating Controls	Supply a statement attesting to the following points. • Computers or systems that do not have a session timeout enabled are set to 'Kiosk mode' and are not permitted to access the internet.

Access Management - 33

Risk Rating: **High**

Control Question - Are all domain controllers running on the latest operation system version? **What is the risk?** Domain Controllers running a legacy operating system hinders your organizations from taking advantage of the latest security features that come standard with current operating system versions. **What we are looking for**: Statement attesting that your organizations domain controllers are running the most recent operating system version. Or your current domain controller is on a patch management schedule that that will update your domain controllers to the latest version within 90 days from when this control reviewed.	
Acceptable Compensating Controls	Supply a statement attesting to the following points. • You are using a combination of AppLocker configuration, "black hole" proxy configuration, and WFAS configuration to prevent domain controllers from accessing the Internet • Perimeter firewalls have been configured to block outbound connections from domain controllers to the Internet. • Domain Controllers are being monitored via a SIEM utility for susception activity

Access Management - 34

Risk Rating: **High**

Control Question - Do all administrators use a dedicated computers to perform administrative tasks? **What is the risk?** Having a dedicated administrative host that is extensively hardened (e.g., Internet access is blocked on the host) creates a layer of complexity that limits eternal bad actors chances of successfully compromising highly privileged accounts. **What we are looking for:** Statement attesting that your organization has established a formalized process requiring administrators to use dedicated workstations for tasks requiring elevated administrative access and a separate workstation for normal user account activities.	
Acceptable Compensating Controls	Supply a statement attesting to the following points. • A TOTP (Time-based One-Time Passwords) or HOTP (Host-based One-Time Passwords) password token solution is in place and limited to personnel who perform administrative duties