Third Party Risk Management

Control Guidance

Top 8 Encryption 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

Encryption – 3

Risk Rating: **High**

Control Question - Are cryptographic keys used for a single purpose (e.g., encryption, authentication, digital signatures)? **What is the risk?** If a key is over-used (e.g., used to encrypt too much data), then it makes the key more vulnerable to cracking, especially when using older symmetric algorithms; it also means that a high volume of data could be exposed in the event of key compromise. **What we are looking for:** Statement attesting that your organization is not using the same cryptographic keys for multiple purposes (e.g.: encryption, authentication, digital signatures).	
Acceptable Compensating Controls	Supply a statement attesting to the following points • GEV data is stored and processed in a cloud environment (provide name of cloud service). • GEV data does not leave the cloud environment. • GEV data is not saved on premises or locally.

Encryption – 4

Risk Rating: **High**

Control Question - Are cryptographic keys rotated/changed on a periodic basis based on NIST 800-57 guidelines or other industry best practices? **What is the risk?** If a key is used for too long, then it makes the key more vulnerable to cracking, especially when using older symmetric algorithms; this is especially true when dealing with advanced persistent threats. **What we are looking for:** Statement attesting that your organization has implemented a process to ensure that cryptographic keys are periodically changed or rotated to reduce the probability of brute force attacks on encryption keys.	
Acceptable Compensating Controls	Supply a statement attesting to the following points • GEV data is stored and processed in a cloud environment (provide name of cloud service). • GEV data does not leave the cloud environment. • GEV data is not saved on premises or locally.

Encryption - 5

Risk Rating: **High**

Control Question - Are cryptographic keys stored in a protected key vault? Note: If cryptographic keys are not stored in a protected key vault, please explain how the keys are protected from unauthorized access. **What is the risk?** The unauthorized disclosure of a private cryptographic keys means that the integrity and non-repudiation qualities of all data signed by that key are suspect. An unauthorized party in possession of the private key could sign false information and make it seem valid. If attackers can steal a private key, they can impersonate the device and decrypt /read data and authenticate to a network." **What we are looking for:** Statement attesting that your organization has implemented a technical solution, such as key vault, for protecting encryption keys from unauthorized access and securely storing them.	
Acceptable Compensating Controls	Supply a statement attesting to the following points • GEV data is stored and processed in a cloud environment (provide name of cloud service). • GEV data does not leave the cloud environment. • GEV data is not saved on premises or locally.

Encryption – 6

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 GEV data stored in an encrypted form using an encryption algorithm equivalent to AES 128, 192, or 256? Examples: If storing GEV data on a server on in a network share drive, the drive, or the folder where the data resides should be encrypted. If storing data in a database, sensitive data should be encrypted within the database. If storing GEV data on laptops, the laptops should have full disk encryption installed. If storing GEV data on a mobile device, the device should be encrypted. **What is the risk?** Without encryption, any security hole that grants an attacker access to an organization's system can also grant them access to the company's sensitive data. Properly applied encryption will ensure that only those who need to view sensitive data will have the rights to do so. Additionally, if data is stolen, a properly applied encryption algorithm can render the information useless to data thief. **What we are looking for**: Evidence of compliance with an encryption key management policy (KMP). Please provide one of the following: • Screenshots which show all systems hosting GEV Data have encryption enabled • Policy documentation that shows client data is required to be encrypted at rest on your systems which includes endpoints, server, and databases	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.

Encryption – 7

Risk Rating: **High**

Control Question - If confidential GEV data is sent via email, is the email (including any attachments) encrypted using TLS 1.2 or TLS 1.3? Example: Transport Layer Security (TLS) versions 1.2 or 1.3 are widely used to encrypt email traffic. Note: If your organization uses TLS 1.0 or 1.1, select "No". These versions of TLS are not secure. **What is the risk?** Not implementing a current version of TLS can leave your organizations email messaging susceptible to man-in-the-middle attacks, jeopardizing the integrity, confidentiality and authenticity of information transmitted between multiple parties. **What we are looking for:** Statement attesting to a policy or documentation that the company email solution has TLS v 1.2 or 1.3 is enabled	
Acceptable Compensating Controls	Supply a statement attesting to the following points • Your company outsources email to an encrypted email business solution (e.g., Gmail, Proton mail, apple mail for business, etc.)

Encryption – 8

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 - If GEV data is sent over public networks such as the internet, is all web traffic encrypted using secure protocols? Note: Protocols to encrypt internet traffic include, but are not limited to TLS, Hyper Text Transfer Protocol Secure (HTTPS), and Internet Protocol Security (IPsec). **What is the risk?** Encrypting data over public network is especially important for sites where sensitive data is passed across the connection, such as eCommerce sites that accept online card payments, or login areas that require users to enter their credentials. It is not difficult for bad actors to capture data that is being transmitted from site to site over the internet, SO encrypting that data is crucial. **What we are looking for**: Evidence of implementation of secure protocols (such as, HTTPS, IPSEC, etc.) to protect and prevent unauthorized access to GEV data if there is a need to transmit/share GEV data over public networks.	
Acceptable Compensating Controls	Compensating Controls are not permitted for this Control Question.