CIS Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is this CIS Control Critical?

Data is no longer only contained within an enterprise's border, it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services who might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for the protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire lifecycle. These privacy rules can be complicated for multi-national enterprises of any size. However, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

While many attacks occur on the network, others involve physical theft of portable end-user devices, attacks on service providers, or other partners holding sensitive data. Other sensitive enterprise assets may also include non-computing devices that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

The enterprise's loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost as a result of theft or espionage, the vast majority are a result of poorly understood data management rules and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise and, more importantly, is a regulatory requirement for most controlled data.

3.1: Establish and Maintain a Data Management Process

Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Data	Govern	1, 2, 3

Dependencies

- None

Inputs

1. GV10: Enterprise\'s data management process
2. Date of last update to the data management process

Operations

1. Review GV10 to determine if, at a minimum, it includes:

2. Addressing data sensitivity. If so, M1 = 1. Otherwise M1 = 0. (GV11)
3. Captures data owner. If so, M2 = 1. Otherwise M2 = 0. (GV13)
4. Handling of data. If so, M3 = 1. Otherwise, M3 = 0. (GV14)
5. Data retention limits based on the sensitivity of data. If so, M4 = 1. Otherwise, M4 = 0. (GV15)
6. Disposal requirements based on the sensitivity of data. If so, M5 = 1. Otherwise, M5 = 0. (GV16)

Measures

- M1 = Does the process address data sensitivity
- M2 = Does the process capture data owners
- M3 = Does the process include guidance for handling of data
- M4 = Does the process include data retention limits based on sensitivity of data
- M5 = Does the process include guidance on disposal requirements based on the sensitivity of the data
- M6 = GV10

Metrics

- If M6 is not available or does not exist, this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Data Management Process

Metric	**The percentage of completeness for the enterprise's data management process.**
Calculation	`(M1 + M2 + M3 + M4 + M5) / 5`

3.2: Establish and Maintain a Data Inventory

Establish and maintain a data inventory based on the enterprise’s data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

Asset Type	Security Function	Implementation Groups
Data	Identify	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. `GV11`: Portion of data management process addressing data sensitivity
2. `GV12`: Data Inventory consisting of the data set of sensitive information for which the enterprise is responsible
3. `GV1`: Enterprise asset inventory
4. Date of the last update to the sensitive data inventory

Operations

1. Use `GV11` to map Input 2 to sensitivity per the guidance in the data management process:
    1. Identify and enumerate items in the data set that have a mapping (M2)
    2. Identify and enumerate items in the data set that do not have a mapping (M3)
2. Use `GV1` and M2 from Operation 1 to map the data set to assets storing data:
    1. Identify and enumerate items that have complete and correct mapping to asset and sensitivity (M4)
    2. Identify and enumerate items that have partial mapping to sensitivity (M5)
3. Use `GV1` and M3 from Operation 2 to map the data set, without sensitivity mapping, to assets storing data:
    1. Identify and enumerate items that have partial mapping to assets (M6)
    2. Identify and enumerate items that have no mapping at all (M7)
4. Compare current date to Input 4 and capture timeframe in months (M8)

Measures

- M1 = `GV11`
- M2 = Count of sensitive data addressed in `GV11`
- M3 = Count of sensitive data not addressed in `GV11`
- M4 = Count of data with complete sensitivity and asset storage inventory
- M5 = Count of data with partial mapping to sensitivity
- M6 = Count of data with partial mapping to assets
- M7 = Count of data with no mapping to sensitivity or asset
- M8 = Timeframe since the last update to the sensitive data inventory in months
- M9 = Count of items in `GV12`

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M9 is greater than 12 months, this Safeguard is scored at zero and receives a failing score. The other metrics don't apply.

Completeness of Sensitive Data Inventory

Metric	Percentage of data with complete information
Calculation	`M4 / M9`

Partial Completeness of Sensitive Data Inventory

Metric	Percentage of data with partial inventory
Calculation	`(M5 + M6) / M9`

3.3: Configure Data Access Control Lists

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

Dependencies

- Safeguard 3.2: Establish and Maintain a Data Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Inputs

1. `GV12`: Sensitive Data Inventory
2. `GV1`: Enterprise asset inventory
3. `GV3`: Configuration Standards
4. `GV13`: Portion of data management process addressing data owners
5. `GV14`: Portion of data management process addressing data handling
6. `GV22`: Inventory of Accounts

Assumptions

Operations

1. Use the data management process, specifically `GV13` and `GV14`, as guidelines to map user accounts to sensitive data in `GV12`:

    1. Identify and enumerate sensitive data correctly mapped to user accounts (M1)
    2. Identify and enumerate sensitive data not correctly mapped to user accounts (M2)

2. For each enterprise asset storing sensitive data, as outlined by `GV12`:

    1. Identify and enumerate all assets storing sensitive data (M3)
    2. Use `GV3` to check and enumerate assets that are properly configured to only allow users as identified in Operation 1 (M4)
    3. Use `GV3` to check and enumerate assets that are improperly configured to only allow users as identified in Operation 1 (M5)

Measures

- M1 = Count of sensitive data correctly mapped to user accounts per the data management process
- M2 = Count of sensitive data not correctly mapped to user accounts per the data management process
- M3 = Count of assets storing sensitive data
- M4 = Count of properly configured assets to support data access control
- M5 = Count of improperly configured assets to support data access control
- M6 = `GV17`
- M7 = `GV13`
- M8 = `GV14`

Metrics

- If either M7 or M8 is 0, this Safeguard receives a failing score. The other metrics don't apply.

Completeness of User Access Control

Metric	**Percentage of user accounts properly mapped to sensitive data**
Calculation	`M1 / M6`

Properly Configured Assets

Metric	**Percentage of assets properly configured to control access of sensitive data**
Calculation	`M4 / M3`

3.4: Enforce Data Retention

Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.

Asset Type	**Security Function**	**Implementation Groups**
Data	Protect	1, 2, 3

Dependencies

- Safeguard 3.1: Establish and Maintain a Data Management Process
- Safeguard 3.2: Establish and Maintain a Data Inventory

Inputs

1. `GV15`: Data Retention Limits outlined in the data management process
2. `GV11`: Portion of data management process addressing data sensitivity
3. `GV12`: Sensitive Data Inventory

Operations

1. For each sensitive data type covered in `GV11`:

    1. Enumerate the number of types of sensitivity (`GV17`: M1), at a minimum one to differentiate sensitive data from other data
    2. Identify and enumerate if each type has a minimum retention time (M2) as defined by `GV15`
    3. Identify and enumerate if each type has a maximum retention time (M3) as defined by `GV15`

2. Using the output of Operation 1.1 and 1.2, check the data inventory `GV12` for enforcement of data retention:

    1. Identify and enumerate items in the inventory that comply with retention timelines (M4)
    2. Identify and enumerate items in the inventory that do not comply with retention timelines (M5)

Measures

- M1 = Count of sensitivity types that require retention timelines
- M2 = Count of sensitivity types that include minimum retention times
- M3 = Count of sensitivity types that include maximum retention times
- M4 = Count of data in inventory that comply with retention policy
- M5 = Count of data in inventory that do not comply with retention policy
- M6 = Count of `GV12`

Metrics

- If `GV15` is 0, this Safeguard receives a failing score. The other metrics don't apply.

Completeness of Policy

Metric	**The percentage of sensitivity types that include minimum retention timelines**
Calculation	`M2 / M1`

Metric	**The percentage of sensitivity types that include maximum retention timelines**
Calculation	`M3 / M1`

Enforcement of Retention Policy

Metric	**The percentage of sensitivity data that complies with retention policy**
Calculation	`M4 / M6`

3.5: Securely Dispose of Data

Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

Dependencies

- Safeguard 3.1: Establish and Maintain a Data Management Process
- Safeguard 3.2: Establish and Maintain a Data Inventory

Inputs

1. `GV16`: Data disposal requirement portion of data management process
2. `GV11`: Portion of data management process addressing data sensitivity
3. `GV17`: Count of Sensitive data types
4. `GV12`: Sensitive Data Inventory

Operations

1. For each sensitive data type covered in `GV17`:
    1. Identify and enumerate each type that has a disposal method and process as defined by `GV16` (M2)
    2. Identify and enumerate each type that does not have a disposal method and process as defined by `GV16` (M3)
2. For each item in `GV12`, determine whether the data complies with the disposal requirements outlined in `GV17`:
    1. Enumerate data that does not comply with disposal requirements (M4)
    2. Enumerate data that complies with disposal requirements (M5)

Measures

- M1 = `GV17`
- M2 = Count of sensitive data types with an outlined disposal method
- M3 = Count of sensitive data types without an outlined disposal method
- M4 = Count of data in inventory that does not comply with disposal requirement
- M5 = Count of data in inventory that complies with disposal requirement
- M6 = Count of items in `GV12`

Metrics

- If `GV16` is 0, this Safeguard receives a failing score. The other metrics don't apply.

Completeness of Disposal Process

Metric	**The percentage of data sensitivity types that contain a disposal method and process**
Calculation	`M2 / M1`

Compliance to Disposal Process

Metric	**The percentage of compliance to the data disposal process**
Calculation	`M5 / M6`

3.6: Encrypt Data on End-User Devices

Encrypt data on end-user devices containing sensitive data. Example implementations can include, Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Asset Type	**Security Function**	**Implementation Groups**
Data	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration Standards

Operations

1. For each asset in GV1, identify end-user devices:
    1. Enumerate the end-user devices (M1)
    2. Use GV5 to identify and enumerate the assets that have encryption software installed (M2)
    3. Use GV5 to identify and enumerate the assets without encryption software (M3)
2. For each encryption software installed on assets (M2), use GV3 to determine whether the software is properly configured:
    1. Enumerate the encryption software that is properly configured (M4)
    2. Enumerate the encryption software that is improperly configured (M5)

Measures

- M1 = Count of approved end-user devices
- M2 = Count of approved end-user devices with encryption software installed
- M3 = Count of approved end-user devices without encryption software
- M4 = Count of properly configured end-user devices
- M5 = Count of improperly configured end-user devices

Metrics

- Installed Software Coverage

Metric	**The percentage of approved mobile devices that are equipped with approved encryption software.**
Calculation	`M2 / M1`

- Appropriately Configured Devices

Metric	**The percentage of approved mobile devices equipped with approved encryption software that meet or exceed the approved configuration policy.**
Calculation	`M3 / M1`

3.7: Establish and Maintain a Data Classification Scheme

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as “Sensitive”, “Confidential,” and “Public”, and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Data	Identify	2, 3

Dependencies

- Safeguard 3.1: Establish and Maintain a Data Management Process
- Safeguard 3.2: Establish and Maintain a Data Inventory

Inputs

1. Enterprise's data classification scheme
2. `GV17`: Sensitive Data types
3. `GV12`: Sensitive Data Inventory
4. Date of last review of the data classification scheme

Operations

1. Check if the enterprise has a data classification scheme (Input 1):
    1. If Input 1 exists, M = 1
    2. Otherwise M1 = 0
2. Using `GV17`, determine if the enterprise has a way to categorize the type of data within the classification scheme:
    1. Enumerate the sensitivity types that are included in the classification scheme (M2)
    2. Enumerate the sensitivity types that are not included in the classification scheme (M3)
3. Compare `GV12` and Input 1:
    1. Identify and enumerate data that contains an accurate classification per the classification scheme (M4)
    2. Identify and enumerate data that does not contain a classification or contains an inaccurate classification per the classification scheme (M5)
4. Compare the current date to that provided in Input 4. Note the timeframe in months (M8)

Measures

- M1 = Output of Operation 1
- M2 = Sensitivity addressed by the classification scheme
- M3 = Sensitivity not addressed by the classification scheme
- M4 = Data properly categorized per the classification scheme
- M5 = Data lacking or improperly categorized per the classification scheme
- M6 = Count of items in `GV17`
- M7 = Count of `GV12`
- M8 = Count of months since the last review of the classification scheme

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M8 is greater than twelve, this Safeguard receives a failing score. The other metrics don't apply.

Completeness of Classification Scheme

Metric	**The percentage of sensitive data types covered within the classification scheme.**
Calculation	`M2 / M6`

Implementation of the Classification Scheme

Metric	**The percentage of data categorized using the classification scheme.**
Calculation	`M4 / M7`

3.8: Document Data Flows

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise’s data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	**Security Function**	**Implementation Groups**
Data	Identify	2, 3

Dependencies

- Safeguard 3.1: Establish and Maintain a Data Management Process
- Safeguard 3.2: Establish and Maintain a Data Inventory

Inputs

1. Documentation outlining data flow for enterprise-owned data. Documentation should include, at a minimum, data flows to external enterprises.
2. `GV12`: Sensitive Data Inventory
3. Date of last review of the data flow documentation

Operations

1. Check if the enterprise has data flow documentation (Input 1):
    1. If Input 1 exists, M = 1
    2. Otherwise M1 = 0
2. Using `GV12`, identify data that flows to external enterprises:
    1. Enumerate the data that flows to external enterprises (M2)
3. Compare Input 1 and the output of Operation 2:
    1. Enumerate data flows from Operation 2 that are included in Input 1 (M3)
    2. Enumerate data flows from Operation 2 that are not included in Input 1 (M4)
4. Compare the current date to that provided in Input 3. Note the timeframe in months (M5)

Measures

- M1 = Output of Operation 1
- M2 = Count of data flows to external enterprises
- M3 = Count of data flows included in the data flow documentation
- M4 = Count of data flows not included in the data flow documentation
- M5 = Count of months since last review of the data flow documentation

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M5 is greater than twelve, this Safeguard receives a failing score. The other metrics don't apply.

Coverage of Data Flow Documentation

Metric	**The percentage of existing data flows in the enterprise's data flow documentation.**
Calculation	`M3 / M2`

3.9: Encrypt Data on Removable Media

Encrypt data on removable media.

Asset Type	**Security Function**	**Implementation Groups**
Data	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration Standards

Assumptions

- Enterprise asset inventory includes removable media

Operations

1. Use `GV1` to identify and enumerate assets authorized to support removable media (M1)

2. Use `GV5` to identify encryption software installed on assets identified in Operation 1 (M1):

    1. Enumerate the number of assets with encryption software installed (M2)
    2. Enumerate the number of assets without encryption software installed (M3)

3. For assets identified in Operation 2.1, use `GV3` to check configurations of encryption software:

    1. Enumerate assets that have properly configured encryption software (M4)
    2. Enumerate assets that have improperly configured encryption software (M5)

Measures

- M1 = Count of assets authorized to support removable media
- M2 = Count of authorized assets with encryption software installed
- M3 = Count of authorized assets without encryption software installed
- M4 = Count of authorized assets with properly configured encryption software
- M5 = Count of authorized assets with improperly configured encryption software

Metrics

Coverage

Metric	**The percentage of appropriately configured assets to support removable media.**
Calculation	`M4 / M1`

3.10: Encrypt Sensitive Data in Transit

Encrypt sensitive data in transit. Example implementations can include, Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 3.2: Establish and Maintain a Data Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV12`: Sensitive Data Inventory
2. `GV5`: Configuration Information

Operations

1. For each item in `GV12`, identify the means and components for encrypting data in transit.

2. Compare the output of Operation 1 with `GV5` to check appropriate approved configurations:

    1. Enumerate the data items in `GV12` that are properly configured (M2)
    2. Enumerate the data items in `GV12` that are improperly configured (M3)

Measures

- M1 = Count of items in `GV12`
- M2 = Count of data with properly configured encryption components
- M3 = Count of data with improperly configured encryption components

Metrics

Coverage

Metric	**The percentage of sensitive data properly configured to be encrypted in transit.**
Calculation	`M2 / M1`

3.11: Encrypt Sensitive Data At Rest

Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV12`: Sensitive data inventory
2. `GV4`: Enterprise Network Architecture Documentation
3. `GV18`: Enterprise assets storing sensitive data

Operations

1. Use `GV5` to identify and enumerate all encryption tools requiring secondary authentication systems (M1)

2. Use `GV12` and `GV1` to identify and enumerate all enterprise assets storing sensitive data (`GV19`: M2)

3. Compare the output of Operation 1 and Operation 2:

    1. Identify and enumerate assets with at least one encryption tool from M1 installed (M4)
    2. Identify and enumerate assets without at least one encryption tool from M1 installed (M5)

Measures

- M1 = Count of authorized encryption tools requiring secondary authentication systems
- M2 = Count of enterprise assets storing sensitive data
- M3 = Count of assets with at least one encryption tool installed
- M4 = Count of assets without at least one encryption tool installed

Metrics

Coverage

Metric	The percentage of assets storing sensitive data covered by an encryption tool.
Calculation	`M3 / M2`

3.12: Segment Data Processing and Storage Based on Sensitivity

Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 3.2: Establish and Maintain a Data Inventory
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Inputs

1. `GV12`: Sensitive Data Inventory
2. `GV4`: Enterprise Network Architecture Documentation

Assumptions

1. An asset's overall sensitivity level should be the highest sensitivity level of the data it stores/processes/transmits. If a system contains any sensitive information, that asset should be treated accordingly and should be properly separated from networks or network segments that don't have a need to access that type of sensitive information.

Operations

1. For each item in `GV12` identify the assets that store, process, or transmit sensitive data (`GV18`: M1)

2. Use the output of Operation 1 and `GV4` to identify networks/VLANs connected to the assets:

    1. Identify and enumerate any instances of properly separated assets from less sensitive networks (M2)
    2. Identify and enumerate any instances of improperly separated assets from less sensitive networks (M3)

Measures

- M1 = Count of assets storing, processing, or transmitting sensitive data

- M2 = Count of sensitive assets properly separated from less sensitive networks
- M3 = Count of sensitive assets improperly separated from less sensitive networks

Metrics

Coverage

Metric	**The percentage of properly separated sensitive assets.**
Calculation	`M2 / M1`

3.13: Deploy a Data Loss Prevention Solution

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 3.2: Establish and Maintain a Data Inventory

Inputs

1. `GV18`: Enterprise assets storing, processing, or transmitting sensitive data
2. `GV5`: Authorized Software inventory
3. `GV3`: Configuration Standards

Operations

1. Use `GV5` to identify and enumerate all data loss prevention software.

2. Compare `GV18` and the output of Operation 1:

    1. Identify and enumerate each asset in `GV18` with data loss prevention software installed (M2)
    2. Identify and enumerate each asset in `GV18` without data loss prevention software installed (M3)

3. For assets with data loss prevention installed from Operation 2.1, check `GV3` for configuration information:

    1. Identify and enumerate assets with properly configured data loss prevention software (M4)

2. Identify and enumerate assets with improperly configured data loss prevention software (M5)

Measures

- M1 = Count of GV18
- M2 = Count of assets with data loss prevention software
- M3 = Count of assets without data loss prevention software
- M4 = Count of assets with properly configured data loss prevention software
- M5 = Count of assets with improperly configured data loss prevention software

Metrics

Coverage

Metric	**The percentage of assets covered by at least one properly configured data loss prevention software instance.**
Calculation	M4 / M1

3.14: Log Sensitive Data Access

Log sensitive data access, including modification and disposal.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV5: Authorized software inventory
2. GV19: Enterprise assets storing sensitive data
3. GV3: Configuration Standards

Operations

1. Using GV3, identify authorized logging software.

2. For each asset in GV19, use the output from Operation 1:

    1. Identify and enumerate assets with logging software installed (M2)

2. Identify and enumerate assets that do not have logging software installed (M3)

3. For logging software installed, check configuration using `GV3`:

    1. Identify and enumerate software that is properly configured (M4)
    2. Identify and enumerate software that is improperly configured (M5)

Measures

- M1 = Count of `GV19`
- M2 = Count of assets storing sensitive data with logging software
- M3 = Count of assets storing sensitive data without logging software
- M4 = Count of assets with properly configured logging
- M5 = Count of assets with improperly configured logging

Metrics

Coverage

Metric	**The percentage of properly configured logging on assets storing sensitive data.**
Calculation	`M4 / M1`