controls-assessment-specification Documentation

Release stable

Jul 14, 2022

GENERAL

The table of contents below and in the sidebar should let you easily access the documentation for your topic of interest. You can also use the search function in the top left corner.

The main documentation for the site is organized into sections for each individual CIS Control.

The “About the CIS Controls” section provides background information about the CIS Controls.

The “About the CIS Controls Assessment Specification” provides information about the Controls Assessment Specification including its purpose, methodology, and structure.

The “Terms of Use” section provides the terms of use policy.

The “Contributing” section provides details on how you can contribute to the Controls Assessment Specification.

CHAPTER

ONE

ABOUT THE CIS CONTROLS™

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

We are at a fascinating point in the evolution of what we now call cyber defense. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life for all of us in cyberspace.

As defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. To help us understand the threat, we have seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure.

But all of this technology, information, and oversight has become a veritable "Fog of More" – competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

So how can we as a community – the community-at-large, as well as within industries, sectors, partnerships, and coalitions – band together to establish priority of action, support each other, and keep our knowledge and technology current in the face of a rapidly evolving problem and an apparently infinite number of possible solutions? What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program? Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals, and guidance to measure and improve? Which defensive steps have the greatest value?

These are the kinds of issues that led to and now drive the CIS Controls. They started as a grassroots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. And **value** here is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Led by CIS®, the CIS Controls have been matured by an international community of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;

- Share tools, working aids, and translations; and
- Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

These activities ensure that the CIS Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

1.1 Why the CIS Controls Work: Methodology and Contributors

The CIS Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to evolve the consensus list of Controls, representing the best defensive techniques to prevent or track them. This ensures that the CIS Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The CIS Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defenses identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defense, and response capability that can be maintained and improved.

The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:

Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.

Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

1.2 Getting Started

The CIS Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "What should my enterprise do?" to "What should we ALL be doing?" to improve security across a broad scale.

But this is not a one-size-fits-all solution, in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversarial actions that could impact your ability to be successful in the business or operation. Even a relatively small number of Controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.

CHAPTER

TWO

ABOUT THE CIS CONTROLS ASSESSMENT SPECIFICATION

2.1 Purpose

The CIS Controls provide essential best practices that organizations can implement to improve their cybersecurity posture. In addition to implementing the CIS Controls, it is also important that organizations measure their implementations to ensure that Safeguards are in place and working properly. The purpose of the CIS Controls Assessent Specification (CAS) is to provide a common understanding of what should be measured in order to verify that CIS Safeguards are properly implemented. The hope is that those developing related tools will then build these measures into their tools so that the CIS Controls are measured in a uniform way.

Note that the focus of CAS is on "what to measure" rather than "how to measure". With the goal of being platform agnostic, a conscious effort was made to avoid addressing the "how to measure" in writing CAS, leaving those platform specific details to specific implementations of these measures. Tool developers will determine the "hows" that are appropriate for their tools and use cases.

2.2 Methodology

The CIS Controls provide cybersecurity best practices designed to help organizations of all types secure a wide variety of systems. Because the CIS Controls cover so many security topics, and apply to such a wide variety of hardware and software that can be used in many different ways, measuring the CIS Controls is a complex challenge. Different approaches to measuring the Controls can result in multiple ways of measuring the same Sub-Control.

One useful distinction is measuring whether a Sub-Control has been implemented vs. measuring how well the Safeguard was implemented. Measuring whether a Safeguard is implemented need not be a binary yes or no; for instance, it could be a numerical score indicating how many endpoints in an environment have implemented that Safeguard. Measuring how well a Safegaurd is implemented looks more to the intended effect of the Safeguard examining whether the desired security gains are being realized. Measuring whether a Safeguard is implemented often involves checking whether something is configured in a certain way, while measuring how well often requires more involved checks including more active testing.

While both of these measurement approaches are useful and have their place, for this first version of CAS, we have focused on measuring whether a Safeguard has been implemented (which we have termed Level 1 checks). It is our hope that future versions of CAS will expand to include measurements of how well a Safeguard is implemented as well (which we have termed Level 2 checks).

Specific configuration details are not specified in CAS, as these would vary from platform to platform, and would encroach on "how to measure". When there are multiple ways to implement a Sub-Control, CAS attempts to be generic enough to cover these varying methods in its measures. Where assumptions are made, CAS attempts to explicitly state them.

2.3 Structure of a Safeguard Measurement

This section describes the standard structure of a Safeguard Measurement in CAS.

2.3.1 Basic CIS Safeguad Information

This section includes the Safeguard number, title, description, asset type, security function, and implementation group. This information matches the information in the CIS Controls v8.0 document.

2.3.2 Assumptions

Assumptions are provided inside of the section to which they are most applicable, or not in any specific section if they are general to the entire Safeguard measurement.

2.3.3 Safeguard Dependencies

This is an optional section that may not appear for all Safeguard measurements. When present, this section lists any other Safeguard that are prerequisites for measuring this Safeguard. Completion of the Safeguard specified in this section will typically generate data necessary as an Input for measuring this Safeguard.

2.3.4 Inputs

This section includes the data that is expected as an input in order to measure this Safeguard.

2.3.5 Operations

This section specifies actions to be performed on the inputs in order to generate the measures. The operations provide a linkage between the inputs and measures.

2.3.6 Measures

This section describes the information that should be measured, generally as a result of performing operations on the inputs. Measures are combined to form metrics.

2.3.7 Metrics

This section describes standard metrics that can be calculated from the measures, providing a description of the metricalong with the formula for calculating the metric. In general, CAS attempts to frame metrics in a positive light - i.e., the ratio of items that are compliant with the Safeguard (as opposed to the ratio of items that are not compliant). The provided metrics are not meant to be an exhausive list of metrics, rather it is just meant to list some examples of common metrics that are likely to be useful. The hope is that if appropriate measures have been defined, other metrics can be built from those measures to suit different use cases.

2.3.8 Procedure Review

This is an optional section that may not appear for all Safeguad measurements. When present, this section describes a manual review of a procedure that helps fulfill the Safeguard.

2.4 Versioning

CAS follows a semantic versioning approach based on semver.org and having the following format: *major.minor.point*.

- Major: Significant and material changes to * The organization of the document * Structure of sub-control measures * Inputs, measures, metrics on the whole
- Minor: Material changes to parts of sub-control measures or metrics
- Point: Immaterial changes, such as prose typos, document look and feel

CHAPTER

THREE

TERMS OF USE

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

CHAPTER

FOUR

CONTRIBUTING TO THE CIS CONTROLS ASSESSMENT SPECIFICATION

CIS welcomes contributions to the CIS Controls Assessment Specification. There are no special requirements to contribute beyond recognizing our Terms of Use (see below). If you have a suggestion for improvement to any one of the defined measures, to the content as a whole, or have other suggestions for enhancement, there are two ways to contribute:

- Create an issue in the associated GitHub repository
- Fork the associated GitHub repository and create a pull request

NOTE: To create issues or fork the repository and then submit a pull request, you will need to establish a GitHub account. The Associated GitHub repository can be reached by clicking "Edit on GitHub" in the upper right of the Read the Docs page. The Controls Assessment Specification GitHub repository is located at https://github.com/CISecurity/ControlsAssessmentSpecification

CHAPTER

FIVE

CIS CONTROL 1: INVENTORY AND CONTROL OF ENTERPRISE ASSETS

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this CIS Control Critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to enterprises' networks. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web or email-based malware; and adversaries can leverage weak security configurations for traversing the network, once they are inside.

Additional assets that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks, etc.) should be identified and/or isolated, in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex, dynamic enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" our enterprise assets at very large scale in order to support their opportunities.

Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines can be difficult to track in asset inventories when they are shut down or paused. Another benefit of complete enterprise asset management is supporting incident response. Both when investigating the origination of network traffic from an asset on the network, and to be able to identify all potentially vulnerable, or impacted, assets of similar type or location during an incident.

5.1 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

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

5.1.1 Dependencies

- None

5.1.2 Inputs

1. `GV1`: Detailed Enterprise Asset Inventory - The enterprise's list of current approved inventory to include all assests as outlined in the safeguard. This list is a mix of manual and tool-generated endpoints that includes information such as authorized, non-authorized, IP address, device type and any other information as defined by the enterprise.
2. Aggregate Enterprise Asset Inventory - The enterprise's list of all devices detected, manually or through automated scans, since the last update to `GV1`.
3. Date of last update to the Detailed Enterprise Asset Inventory

Assumptions

1. Devices belonging to the organization, but not connected to the organization's network, require manual discovery in order to be included in the aggregate inventory.

5.1.3 Operations

1. **Calculate the intersection of `GV1` and Input 2**
    1. Enumerate items in `GV1` that are not in Input 2 (M4)
    2. Enumerate items in Input 2 not in Input 1 (`GV2`: M5). These assets are considered unauthorized.
2. **Check items in Input 1 for complete or missing detailed information**
    1. Enumerate items that have complete information (M6)
    2. Enumerate items that do not have complete information or missing information (M7).
3. Calculate the time (in months) since the last update to Input 1 by using current date and Input 4 (M8).

5.1.4 Measures

- M1 = `GV1`
- M2 = Count of items in Input 2
- M3 = Count of items in the intersection of `GV1` and Input 2
- M4 = Count of items in `GV1` not found in Input 2
- M5 = `GV2`
- M6 = Count of items in `GV1` that contain all necessary detailed information
- M7 = Count of items in `GV1` that do not contain detailed information
- M8 = Months since the last update to `GV1`

5.1.5 Metrics

- If M1 is not provided or available, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M8 is greater than six months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Accuracy Score

Metric	What percentage of the aggregate endpoint inventory is accounted for in the current enterprise asset inventory?
Calculation	`M3 / M2`

Completeness Score

Metric	What percentage of the current enterprise asset inventory contains necessary detailed information?
Calculation	`M8 / M1`

Procedural Review

Manual review/rating of the inventory procedures, to include adding and removing assets, and the time allowable or expected, after acquisition or disposal of assets.

5.2 1.2: Address Unauthorized Assets

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Asset Type	Security Function	Implementation Groups
Devices	Respond	1, 2, 3

5.2.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

5.2.2 Inputs

1. `GV1`: Detailed Enterprise Asset Inventory
2. `GV2`: Unauthorized Assets
3. The enterprise defined time frame for removing unauthorized assets (weekly or more often).

Assumptions

1. If the item is not reachable, it may be reasonable to assume it has been removed from the network and therefore dealt with.

5.2.3 Operations

If the optional disposition list is provided, the checks would be tailored to those dispositions. For the following, assume no disposition list is available:

1. At the time frame specified by Input 3, for each unauthorized asset in `GV2`, check to see if the asset is present in the updated asset inventory from `GV1`.
2. **For those items in `GV2` that are not in `GV1`, scan the network to determine if the item is still reachable on the network.**
    1. Enumerate the items from `GV2` that are unreachable (M4)
    2. Enumerate the items from `GV1` that are unreachable (M5)

5.2.4 Measures

- M1 = `GV1`
- M2 = Count of `GV2`
- M3 = Timeframe in days for Input 3
- M4 = Count of items from `GV2` that are unreachable after scan
- M5 = Count of items from `GV1` that are unreachable after scan

5.2.5 Metrics

If M3 is greater than seven days, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	The ratio of unaccounted for, unauthorized assets, to the total assets in the asset inventory.
Calculation	If the value of M4 is 0, there are no unauthorized assets that remain unaccounted for. In this case, the value of the metric is 1. Otherwise, the value is :code:`(M2 - M4) / M2 `

5.3 1.3: Utilize an Active Discovery Tool

Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

5.3.1 Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

5.3.2 Inputs

1. `GV1`: Enterprise asset inventory
2. The list of active discovery tool(s) used by the enterprise
3. List consisting of the union from scan results conducted using all active asset discovery tool(s) within the enterprise (discovered assets).
4. Timeframe between two active asset discovery tool scans.
5. `GV3`: Configuration Standard

Assumptions

1. The asset discovery tools on the provided list are active asset discovery tools, as opposed to passive asset discovery tools (verification of this is not performed during the following operations).

5.3.3 Operations

1. Identify enterprise assets not discovered by the active discovery tools by comparing Input 1 and Input 3 (M2).
2. Identify the configurations for active asset discovery tools that interface with `GV1` by using `GV3`
3. **Using the configuration information in `GV3`, check the approved configurations to verify that the tools are capable of interfacing with the asset inventory to make automatic updates.**
    1. Enumerate those tools that are compliant (M3)
    2. Enumerate those that are not compliant (M4).

5.3.4 Measures

- M1 = Count of all discovered assets from Input 3
- M2 = Count of undiscovered assets
- M3 = Count of properly configured tools
- M4 = Count of improperly configured tools
- M5 = Count of Input 2
- M6 = Count of `GV1`
- M7 = Timeframe in hours for Input 4

5.3.5 Metrics

- If M7 is greater than 24 hours, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M5 is 0, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Asset Discovery Coverage

Metric	Asset Discovery Coverage
Calculation	`M1 / M6`

Tool Compliance Ratio

Metric	Tool Compliance Ratio
Calculation	`M3 / M2`

5.4 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

Asset Type	Security Function	Implementation Groups
Devices	Identify	2, 3

5.4.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

5.4.2 Inputs

1. List of DHCP servers
2. `GV41`: List of CMDB servers

Assumptions

1. CMDB servers are configured to pull from DHCP logs

5.4.3 Operations

- For each DHCP server, enumerate those where DHCP logging is enabled (M2)
- For each CMDB server, enumerate those where DHCP logs are used to update IP addresses (M4)

5.4.4 Measures

- M1 = Count of Input 1
- M2 = Count of DHCP servers with logging enabled
- M3 = Count of Input 2 `GV41`
- M4 = Count of CMDB servers configured to use DHCP logs to update IP addresses
- M5 = Count of devices in the DHCP server logs that are not included in the CMDB servers
- M6 = Count of devices in the DHCP server logs that are included in the CMDB servers

5.4.5 Metrics

- M4 > 0 indicates a non up-to-date asset inventory

DHCP Logging Quality

Metric	Ratio of appropriately configured DHCP logging enabled to known DHCP servers
Calculation	`M2 / M1`

CMDB Configuration Quality

5.5 1.5: Use a Passive Asset Discovery Tool

Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

Asset Type	Security Function	Implementation Groups
Devices	Detect	3

5.5.1 Dependencies

- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

5.5.2 Inputs

1. `GV4`: Enterprise network architecture documentation
2. List of passive asset discovery tools in use by the organization. For each, include the location of the tool's configuration information and which networks it covers.
3. `GV3`: Approved configuration(s) for each passive asset discovery tool. Configurations should include the settings necessary for the tool to be able to update the enterprise's asset inventory

5.5.3 Operations

1. Identify approved configuratons for passive asset discovery tools using `GV3`
2. **For each passive asset discovery tool provided in Input 2, check the tool's configuration against the appropriate approved configuration from `GV3`**
    1. Enumerate those tools that are properly configured (M1)
    2. Enumerate those tools that are improperly configured (M2) noting the deviations from proper configuration

3. **Identify and enumerate the enterprise's networks (M5) using Input 1, check to see if at least one properly configured passive asset discovery tool from M1 covers that network.**
    1. Create a list of the enterprise's networks that have coverage from at least one properly configured passive asset discovery tool (M3)
    2. Create a list of the enterprise's networks that do not have coverage from any properly configured passive asset discovery tools (M4)

5.5.4 Measures

- M1 = Count of properly configured passive asset discovery tools
- M2 = Count of improperly configured passive asset discovery tools
- M3 = Count of organization's networks that are covered by properly configured passive discovery tools
- M4 = Count of organization's networks that are not covered by properly configured passive discovery tools
- M5 = Count of enterprise's networks.

5.5.5 Metrics

Coverage

Metric	The ratio of the organization's networks with coverage from at least one properly configured passive asset discovery tool to the total number of networks
Calculation	`M3 / M5`

CHAPTER

SIX

CIS CONTROL 2: INVENTORY AND CONTROL OF SOFTWARE ASSETS

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why is this CIS Control Critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use "zero-day exploits", which take advantage of previously unknown vulnerabilities that have yet to have a patch released by the software vendor. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review their software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

6.1 2.1: Establish and Maintain a Software Inventory

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.

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

6.1.1 Dependencies

- None

6.1.2 Inputs

1. GV5: The authorized software inventory with detailed information including: timestamp indicating both last updated and last verified values, timestamp indicating installation date, operating system, software name, software version, software publisher, authorization status, business purpose, supported/unsupported. Where applicable, additionally include URL, app store(s), deployment mechanism, and decommission date.
2. GV6: The date of the last update to the authorized software inventory.

6.1.3 Operations

1. **Check GV5 for completeness of detailed information.**
    1. Note items that have complete detailed information (M2).
    2. Note items that having missing or incomplete information (M3).
2. Compare the current date to GV6 and note timeframe in months (M4).

6.1.4 Measures

- M1 = Count of GV5
- M2 = Count of items in GV5 with complete information
- M3 = Count of items in GV5 with incomplete or missing information
- M4 = Timeframe in months since last update GV6

6.1.5 Metrics

- If M1 is not provided or available, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M4 is greater than six months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Accuracy Score

Metric	What percentage of the current enterprise asset inventory contains necessary detailed information?
Calculation	M2 / M1

6.2 2.2: Ensure Authorized Software is Currently Supported

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

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

6.2.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

6.2.2 Inputs

1. `GV5`: The authorized software inventory with detailed information. deployment mechanism, and decommission date.
2. Authoritative source of information indicating supported/unsupported details by product.
3. Exception documentation for unsupported software that is necessary for the fulfillment of the enterprise's mission.
4. `GV6`: Date of last update to the authorized software inventory

6.2.3 Assumptions

1. Authorized software inventory with detailed information exists for the enterprise.

6.2.4 Operations

1. **For each item in `GV5`, perform a lookup in Input 2 to verify supported/unsupported status.**
    1. Enumerate each item labeled "unsupported" but "supported based on Input 2 (M2)
    2. Enumerate each item labeled "supported" but is "unsupported" based on Input 2 (M3).
2. Identify and note truly "unsupported" items from Input 1 after conducting Operation 1 (M4).
3. **For each unsupported item identifed in Operation 2, conduct a check using Input 3.**
    1. Note items that do not have appropriate exception documentation (M5).
    2. Note items that do have appropriate exception documentation (M6).
4. Compare date of `GV6` to the current date and note timeframe in weeks (M7).

6.2.5 Measures

- M1 = Count of Input 1
- M2 = Count of items in Input 1 that are mislabeled as unsupported
- M3 = Count of items in Input 1 that are mislabeled as supported
- M4 = Count of unsupported items
- M5 = Count of items in Input 1 with that are no longer supported but exception documentation exists
- M6 = Count of items in Input 1 with that are no longer supported and exception documentation does not exist
- M7 = Timeframe in weeks of last update to the authorized software inventory

6.2.6 Metrics

- If M7 is greater than four, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Percentage of Unsupported Software in Use

Metric	What percentage of authorized software inventory in use is unsupported?
Calculation	`M4 / M1`

Rate of False Positives

Metric	What percentage of software listed as supported is actually not supported?
Calculation	`M3 / M1`

Rate of False Negatives

Metric	What percentage of software listed as unsupported is actually supported?
Calculation	`M2 / M1`

Percentage of unsupported software with exception documentation

Metric	What percentage of software listed as unsupported but appropriate exception documentation exists?
Calculation	`M5 / M4`

6.3 2.3: Address Unauthorized Software

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently..

Asset Type	Security Function	Implementation Groups
Applications	Respond	1, 2, 3

6.3.1 Dependencies

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

6.3.2 Inputs

1. `GV5`: Authorized software inventory
2. `GV1`: Enterprise asset Invetory
3. Enterprise defined timeframe for scanning of enterprise assets.
4. Enterprise defined allowable timeframe for resolution of discovered unauthorized software (recommend at least monthly)

6.3.3 Assumptions

1. The scanning schedule timeframe is greater than the enterprise defined allowable timeframe for resolution of discovered unauthorized software.

6.3.4 Operations

1. Identify the software capable enterprise assets in `GV1` (`GV7`)
2. Scan the assets identified in Operation 1 and note software present on each asset (M1)
3. **Compare the scan results to the authorized software list in `GV5`**
    1. Enumerate unauthorized software identified on assets (M2)
4. **Conduct subsquent scan of assets identified in Operation 1 as dictated by timeframe in Input 3**
    1. Compare to list generated in Operation 3 (M2)

5. **For each software still present in Operation 4, check the authorized software list in `GV5`**
    1. Software that remains installed and is not listed in `GV5` is placed on the unaddressed software list (M3) for that asset.

6.3.5 Measures

- M1 = The count of software installed on a given asset
- M2 = The count of unauthorized software installed on a given asset
- M3 = The count of unaddressed software installed on a given asset, identified by follow-up scan.
- M4 = Timeframe for resolution of discovered unauthorized software in weeks

6.3.6 Metrics

- If M4 is greater than four weeks, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Unauthorized software Per Asset

Metric	Ensure unauthorized software installations are addressed
Calculation	`(M2-M3) / M3`

Unauthorized software for the enterprise

- The enterprise metric is calculated through averaging the results calculated above per asset.

6.4 2.4: Utilize Automated Software Inventory Tools

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Asset Type	Security Function	Implementation Groups
Applications	Detect	2, 3

6.4.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.3: Address Unauthorized Software

6.4.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV7`: Software capable assets
3. List of software inventory tools

6.4.3 Operations

1. Use `GV1` and `GV7` to identify and enumrate assets unable to support sofware (M2).
2. **For each software capable asset `GV7`**
    1. Identify and enumerate if the asset is covered by at least one software inventory tool (M3)
    2. Identify and enumerate if the asset is not covered by at least one software inventory tool (M4)

6.4.4 Measures

- M1 = Count of `GV7`
- M2 = Count of assets unable to to support software
- M3 = Count of assets covered by software inventory tools
- M4 = Count of assets not covered by software inventory tools
- M5 = Count of Input 2

6.4.5 Metrics

- If M5 is 0 or unavailable, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Inventory Tool Coverage

6.5 2.5: Allowlist Authorized Software

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

6.5.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 2.3: Address Unauthorized Software
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

6.5.2 Inputs

1. `GV7`: Software capable assets
2. `GV5`: Authorized software inventory
3. `GV3`: Approved configuration Standards
4. Date of last assessment of this safeguard

6.5.3 Operations

1. Using `GV7` identify and enumerate assets capable of supporting allowlisting software (some assets may not enable third-party software installation or otherwise have constrained environments precluding the use of allowlisting software) (M1).
2. Using `GV5` identify all authorized allowlisting software within the enterprise (`GV8`)
3. **Using the output from Operation 1 and authorized allowlisting software `GV8`**
    1. Identify and enumerate allowlisting capable assets with allowlisting software installed (M2)
    2. Identify and enumerate allowlisting capable assets without allowlisting software installed (M3)
4. Use `GV3` to identify allowlisting software configurations (`GV9`)
5. **For each asset with allowlisting software installed (M2) from Operation 2 use the output from Operation 3 to**
    1. Identify and enumerate properly configured software (M4)
    2. Identify and enumerate improperly configured software (M5)
6. Compare Input 4 to current date and note timeframe in months (M6)

6.5.4 Measures

- M1 = Count of enterprise assets capable of supporting allowlisting software
- M2 = Count of enterprise assets capable of supporting allowlisting software and have the software installed
- M3 = Count of enterprise assets capable of supporting allowlisting software and do not have the software installed
- M4 = Count of enterprise assets with allowlisting software that is properly configured
- M5 = Count of enterprise assets with allowlisting software that is properly configured
- M6 = Timeframe since last assessment of this safeguard

6.5.5 Metrics

- If M6 is greater than six months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Allowlisting Installation Coverage

Metric	The percentage of enterprise assets capable of supporting allowlisting with allowlisting installed
Calculation	`M2 / M1`

Allowlisting Configuration Coverage

Metric	The percentage of enterprise assets with properly configured allowlisting installed
Calculation	`M4 / M2`

6.6 2.6: Allowlist Authorized Libraries

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc. files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

6.6.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 2.5: Allowlist Authorized Software
- Safegaurd 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

6.6.2 Inputs

1. `GV8`: Authorized allowlisting software
2. The list of authorized software libraries
3. `GV9`: Approved configuration (s) for allowlisting software
4. Date of last assessement of this safeguard

6.6.3 Operations

1. **For each item identified in `GV8`, use the approved configurations from :code:`GV9` and authorized library list from Input 2**
    1. Identify and enumerate allowlisting software properly configured to allow process loading of authorized libraries (M2)
    2. Identify and enumerate allowlisting software improperly configured to allow process loading of authorized libraries (M3)
2. Compare the date from Input 4 to current date and note timeframe in months (M4).

6.6.4 Measures

- M1 = Count :code:`GV8
- M2 = Count of properly configured allowlisting software
- M3 = Count of improperly configured allowlisting software
- M4 = Timeframe since last assessment of this safeguard

6.6.5 Metrics

- If M4 is greater than six months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of appropriately configured allowlisting software instances within the enterprise.
Calculation	`M2 / M1`

6.7 2.7: Allowlist Authorized Scripts

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc. files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

6.7.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

6.7.2 Inputs

1. `GV5`: Authorized allowlisting software
2. The list of authorized scripts
3. `GV3`: Approved configuration Standards
4. Date of last assessement of this safeguard

6.7.3 Operations

1. Use `GV5` to identify and enumerate all enterprise authorized software capable of executing scripts, including allowlisting software, email client applications, and web client applications (M1)
2. Use `GV3` to identify approved configurations for all software identified in Operation 1
3. **For each item in identified in Operation 1, use the approved configurations from Operation 2**
    1. Identify and enumerate software properly configured to allow execution of authorized and signed scripts from Input 2 (M2)
    2. Identify and enumerate software improperly configured to allow execution of authorized and signed scripts from Input 2(M3)
4. Compare the date from Input 4 to current date and note timeframe in months (M4).

6.7.4 Measures

- M1 = Count of authorized software capable of executing scripts
- M2 = Count of properly configured software
- M3 = Count of improperly configured software
- M4 = Timeframe since last assessment of this safeguard

6.7.5 Metrics

- If M4 is greater than six months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of appropriately configured allowlisting software instances within the enterprise.
Calculation	`M2 / M1`

CHAPTER

SEVEN

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 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.

7.1 3.1: Establish and Maintain a Data Management Process

Establish and maintain a 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	Identify	1, 2, 3

7.1.1 Dependencies

- None

7.1.2 Inputs

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

7.1.3 Operations

1. **Review `GV10` to determine if, at a minimum, it includes:**
    1. Addressing data sensitivity. If so, M1 = 1. Otherwise M1 = 0. (`GV11`)
    2. Captures data owner. If so, M2 = 1. Otherwise M2 = 0. (`GV13`)
    3. Handling of data. If so, M3 = 1. Otherwise M3 = 0. (`GV14`)
    4. Data retention limits based on sensitivity of data. If so, M4 = 1. Otherwise M4 = 0. (`GV15`)
    5. Disposal requirements based on sensitivity of data. If so, M5 = 1. Otherwise M5 = 0. (`GV16`)

7.1.4 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 rentention limits based on sensitivity of data
- M5 = Does the process include guidance on disposal requirements based on sensitivity of data
- M6 = `GV10`

7.1.5 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 perecentage of completeness for the enterprise's data management process.
Calculation	`(M1 + M2 + M3 + M4 + M5) / 5`

7.2 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

7.2.1 Dependencies

- Sub-control 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

7.2.2 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 last update to the sensitive data inventory

7.2.3 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: code:*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)

7.2.4 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 last update to sensitive data inventory in months
- M9 = Count of items in `GV12`

7.2.5 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`

7.3 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

7.3.1 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

7.3.2 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

7.3.3 Assumptions

7.3.4 Operations

1. **Use the data managemet process, specifically GV13 and GV14, as guidelines to map user account to sensitive data in GV12.**
    1. Identify and enumerate sensitive data correctly mapped to user accounts (M1)
    2. Idenitfy and enumerate sensitive data not correctly mapped to user accounts (M2)
2. **For each enterprise asset storing sensitive data, as outlined by :code:`GV12,**
    1. Identify and enumerate all assets storing sensitive data (3)
    2. Use GV3 to check and enumerate assets that are properly configured to only allow users as identified in Operation 1 (M3)
    3. Use GV3 to check and enumerate assets that are improperly configured to only allow users as identified in Operation 1 (M4)

7.3.5 Measures

- M1 = Count of sensitive data correctly mapped to user accounts per the data management process
- M2 = Count of sensitive data 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 = Count of GV17
- M7 = :code:'GV13`
- M8 = GV14

7.3.6 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 acess of sensitive data
Calculation	`M4 / M3`

7.4 3.4: Enforce Data Retention

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

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

7.4.1 Dependencies

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

7.4.2 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

7.4.3 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 deferrentiate 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 :code:`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)

7.4.4 Measures

- M1 = Count of sensitivity types that require retention timelines
- M2 = Count of sensitivity types that ainclude minimum retention times
- M3 = Count of sensitivity types that ainclude 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

7.4.5 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	:code: *M2 / M1*
Metric	The percentage of sensitivity types that include maximum retention timelines
Calculation	:code: *M3 / M1*

Enforcement of Retention Policy

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

7.5 3.5: Securely Dispose of Data

Securely dispose of data as outlined in the enterprise's 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

7.5.1 Dependencies

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

7.5.2 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

7.5.3 Operations

1. **For each sensitive data type covered in `GV17`**
    1. Identify and enumerate each type 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 :code:`GV16`(M3)
2. **For each item in `GV12`determine wether they data complies with the disposal requirements outlined in :code:`GV17`**
    1. Enumerate data that does not comply with disposal requirements (M4)
    2. Enumerate data that complies with disposal requirements (M5)

7.5.4 Measures

- M1 = GV17
- M2 = Count of sensitive data types with an outlined disposal method
- M3 = Count of sensitive data types witouth 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

7.5.5 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

7.6 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
Devices	Protect	1, 2, 3

7.6.1 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

7.6.2 Inputs

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

7.6.3 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)

7.6.4 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

7.6.5 Metrics

Installed Software Coverage

Appropriately Configured Devices

7.7 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

7.7.1 Dependencies

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

7.7.2 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

7.7.3 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 :code:`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 classsification or contains an innaccurate classification per the classification scheme (M5)
4. Compare the current date to that provided in Input 4. Note the timeframe in months. (M8)

7.7.4 Measures

- M1 = Output of Operation 1
- M2 = Sensitivity addressed by the classification scheme
- M3 = Sensitivity not addressed by the classification scheme
- M4 = Data properly catergorized 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 last review of the classification scheme

7.7.5 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

Implementation of the Classification Scheme

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

7.8 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

7.8.1 Dependencies

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

7.8.2 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

7.8.3 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 :code:`GV12`and 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)

7.8.4 Measures

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

7.8.5 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

7.9 3.9: Encrypt Data on Removable Media

Encrypt data on removable media.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

7.9.1 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

7.9.2 Inputs

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

7.9.3 Assumptions

1. Enterprise asset inventory includes removable media

7.9.4 Operations

1. Use `GV1` to identify and enumerate assets authorized to support removeable 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)

7.9.5 Measures

- M1 = Count of assets authorized to support removeable 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

7.9.6 Metrics

Coverage

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

7.10 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

7.10.1 Dependencies

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

7.10.2 Inputs

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

7.10.3 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)

7.10.4 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

7.10.5 Metrics

Coverage

7.11 3.11: Encrypt Sensitive Data At Rest

Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. 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. .. list-table:

```
:header-rows: 1

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

7.11.1 Dependencies

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

7.11.2 Inputs

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

7.11.3 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)

7.11.4 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

7.11.5 Metrics

Coverage

7.12 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
Network	Protect	2, 3

7.12.1 Dependencies

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

7.12.2 Inputs

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

7.12.3 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.

7.12.4 Operations

1. For each item in `GV12` identify the assets that store, process, or transmit sensitive data (:code:`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 seperated assets from less sensitive networks (M2)
    2. Identify and enumerate any instances of improperly seperated assets from less sensitive networks (M3)

7.12.5 Measures

- M1 = Count of assets storing, processing, or transmitting sensitive data
- M2 = Count of sensitive assets properly seperated from less sensitive networks
- M3 = Count of sensitive assets improperly seperated from less sensitive networks

7.12.6 Metrics

Coverage

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

7.13 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 sensitive data inventory.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

7.13.1 Dependencies

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

7.13.2 Inputs

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

7.13.3 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 lass prevention software (M4)
    2. Identify and enumerate assets with improperly configured data lass prevention software (M5)

7.13.4 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

7.13.5 Metrics

Coverage

7.14 3.14: Log Sensitive Data Access

Log sensitive data access, including modification and disposal.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

7.14.1 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

7.14.2 Inputs

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

7.14.3 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)

7.14.4 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 imporperly configured logging

7.14.5 Metrics

Coverage

CHAPTER

EIGHT

CIS CONTROL 4: SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why is this CIS Control Critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software, rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked," to allow the installation of new software or to support new operational requirements.

8.1 4.1: Establish and Maintain a Secure Configuration Process

Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

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

8.1.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

8.1.2 Inputs

1. `GV2`: Authorized software inventory
2. `GV1`: Enterprise asse inventory
3. `GV3`: Configuration Standard: this should include any enterprise approved deviations from industry standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
4. Date of last review and updat of configuration standard

8.1.3 Operations

1. **Identify whether Input 2 exists**
    1. If it exists M1 = 1
    2. If it does not exist M1 = 0
2. Identify and enumerate end-user devices, including portable and mobile, non-computing/IoT devices, and servers in `GV1` (M2)
3. Using the output of Operation 2 (M2), identify and enumerate the software installed on the assets using `GV2` (M3)
4. **For each software identified in Operation 3 (M3)**
    1. Enumerate software that is listed in the configuration standard :code:`GV3`(M4)
    2. Enumerate software that is not listed in the configuration standard :code:`GV3`(M5)
5. Compare current date to date provided in Input 4. Note the timeframe in months (M6)

8.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of applicable enterprise assets
- M3 = Count of software insalled on applicable enterprise assets
- M4 = Count of software that is listed in the configuration standard
- M5 = Count of software that is not listed in the configuration standard
- M6 = Timeframe since last review and update in months

8.1.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M6 is greater than twelve, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Standard Configuration Coverage

8.2 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

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

8.2.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

8.2.2 Inputs

1. `GV2`: Authorized software inventory
2. `GV1`: Enterprise asse inventory
3. `GV3`: Configuration Standard: this should include any enterprise approved deviations from industry standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
4. Date of last review and updat of configuration standard

8.2.3 Operations

1. **Identify whether Input 2 exists**
    1. If it exists M1 = 1
    2. If it does not exist M1 = 0
2. Identify and enumerate network infrastructure assets in `GV1` (M2)
3. Using the output of Operation 2 (M2), identify and enumerate the software installed on the assets using `GV2` (M3)
4. **For each software identified in Operation 3 (M3)**
    1. Enumerate software that is listed in the configuration standard :code:`GV3`(M4)
    2. Enumerate software that is not listed in the configuration standard :code:`GV3`(M5)
5. Compare current date to date provided in Input 4. Note the timeframe in months (M6)

8.2.4 Measures

- M1 = Output of Operation 1
- M2 = Count of applicable enterprise assets
- M3 = Count of software insalled on applicable enterprise assets
- M4 = Count of software that is listed in the configuration standard
- M5 = Count of software that is not listed in the configuration standard
- M6 = Timeframe since last review and update in months

8.2.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M6 is greater than twelve, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Standard Configuration Coverage

8.3 4.3: Configure Automatic Session Locking on Enterprise Assets

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

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

8.3.1 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

8.3.2 Inputs

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

8.3.3 Operations

1. Identify and enumerate assets within `GV1` that support automatic locking due to inactivity (M1)
2. Use `GV5` to identify and enumerate assets from Operation 1 with authorized software installed (M2)
3. **Check the configurations for the software using `GV3`**
    1. For general computing assets, enumerate those assets with properly configured automatic locking (15 minutes or less) (M3)
    2. For general computing assets, enumerate those assets with improperly configured automatic locking (greater than 15 minutes) (M4)
    3. For mobile assets, enumerate those assets with properly configured automatic locking (2 minutes or less) (M5)
    4. For mobile assets, enumerate those assets with improperly configured automatic locking (greater than 2 minutes) (M6)

8.3.4 Measures

- M1 = Count of assets capable of supporting automatic lockout
- M2 = Count of assets with authorized software installed to allow lockout
- M3 = Count of general computing assets with properly configured lockout
- M4 = Count of general computing assets with improperly configured lockout
- M5 = Count of mobile assets with properly configured lockout
- M6 = Count of mobile assets with improperly configured lockout

8.3.5 Metrics

Properly Configured Assets

Metric	The percentage of assets properly configured for automatic lockout.
Calculation	`(M3 + M5) / M1`

8.4 4.4: Implement and Manage a Firewall on Servers

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

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

8.4.1 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

8.4.2 Inputs

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

8.4.3 Operations

1. Identify and enumerate servers capable of hosting a firewall using `GV1` (M1)
2. Identify and enumerate applications capable of hosting a firewall using `GV5` (M2)
3. **Using configuration standards to check if firewalls are properly configured**
    1. Enumerate servers from Operation 1 with properly configured firewalls (M3)
    2. Enumerate servers from Operation 1 with improperly configured firewalls (M4)
    3. Enumerate applications from Operation 2 with properly configured firewalls (M3)
    4. Enumerate application from Operation 2 with improperly configured firewalls (M4)

8.4.4 Measures

- M1 = Count of servers enterprise assets capable of hosting a firewall
- M2 = Count of applications software capable of hosting a firewall
- M3 = Count of servers with properly configured firewalls
- M4 = Count of servers with improperly configured firewalls
- M5 = Count of applications with properly configured firewalls
- M6 = Count of applications with improperly configured firewalls

8.4.5 Metrics

Implementation of firewalls

Metric	The percentage of properly configured firewalls within the enterprise
Calculation	`(M3 + M5) / (M1 + M2)`

8.5 4.5: Implement and Manage a Firewall on End-User Devices

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

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

8.5.1 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

8.5.2 Inputs

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

8.5.3 Operations

1. Identify and enumerate end-user devices capable of hosting a firewall or a deny rule using `GV1` (M1)
2. **Using configuration standards `GV3` to check if firewalls or deny rules are properly configured on end-user devices**
    1. Enumerate assets from Operation 1 with properly configured firewalls or a configured default deny rule (M3)
    2. Enumerate assets from Operation 1 with improperly configured firewalls and lacking a configured default deny rule(M4)

8.5.4 Measures

- M1 = Count of end-user devices capable of hosting a firewall
- M2 = Count of end-user devices with a properly configured firewall or default deny rule
- M3 = Count of end-user devices with an improperly configured firewall and lacking a configured default deny rule

8.5.5 Metrics

Coverage

Metric	The percentage of properly configured firewalls or deny rule on end-user devices
Calculation	`M2 / M1`

8.6 4.6: Securely Manage Enterprise Assets and Software

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

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

8.6.1 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

8.6.2 Inputs

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

8.6.3 Operations

1. Using `GV5` identify and enumerate authorized management software (M1)
2. Using `GV1` identify and enumerate assets capable of supporting management software (M2)
3. Using the output of Operations 1 and 2, identify and enumerate assets with authorized management software installed (M3)
4. **Using configuration standards `GV3` to check if management software is configured properly**
    1. Enumerate assets from Operation 3 with properly configured management software (M4)
    2. Enumerate assets from Operation 1 with improperly configured mangement software (M5)

8.6.4 Measures

- M1 = Count of authorized management software
- M2 = Count of enterprise assets capable of supporting management software
- M3 = Count of assets with authorized management software installed
- M4 = Count of assets with properly configured management software
- M5 = Count of assets with improperly configured management software

8.6.5 Metrics

Coverage

Metric	The percentage of assets with properly configured authorized management software
Calculation	`M4 / M2`

8.7 4.7: Manage Default Accounts on Enterprise Assets and Software

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

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

8.7.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 5.2: Use Unique Passwords

8.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV20`: Unique password policy

8.7.3 Operations

1. Use `GV5` to identify and enumerate authorized operating software, applications, and third-party software that contain default accounts (M1)
2. Use `GV1` to identify and enumerate assets with software, from Operation 1, installed (M2)
3. For each identified in Operation 2, enumerate default accounts (M3)
4. **Check if default accounts can be disabled**
    1. Enumerate accounts that are disabled (M4)
    2. Enumerate accounts that are enabled (M5)
5. **If account cannot be disabled, ensure to change default passwords according to the `GV20`: enterprise's unique password policy**
    1. Enumerate accounts with changed passwords (M6)

8.7.4 Measures

- M1 = Count of software that uses default accounts
- M2 = Count of assets with software installed that uses default accounts
- M3 = Count of default accounts identified
- M4 = Count of default accounts that have been disabled
- M5 = Count of default accounts that are enabled
- M6 = Count of enabled default accounts with changed passwords

8.7.5 Metrics

Unusable Default Accounts

Metric	The percentage of default accounts that have been rendered unusable
Calculation	`(M4 + M6) / M3`

8.8 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

8.8.1 Dependencies

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

8.8.2 Inputs

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

8.8.3 Operations

1. Use `GV5` to identify and enumerate authorized services (M1)
2. Use `GV1` to identify and enumerate services on enterprise assets (M2)
3. **Compare outputs from Operations 1 and 2**
    1. Identify and enumerate authorized services on assets (M3)
    2. Identify and enumerate unauthorized services on assets (M4)
4. **For authorized services in Operation 3.2, use `GV3` to check configurations**
    1. Identify and enumerate services that are configured correctly (disabled) (M5)
    2. Identify and enumerate services that are configured improperly (enabled) (M6)

8.8.4 Measures

- M1 = Count of authorized services
- M2 = Count of services on enterprise assets
- M3 = Count of authorized services on assets
- M4 = Count of unauthorized services on assets
- M5 = Count of unauthorized services that are disabled
- M6 = Count of unauthorized serivces that are enabled

8.8.5 Metrics

Compliant Services

Metric	The percentage of services installed/running that are enterprise essential
Calculation	`(M3 + M5) / M2`

Non-compliant Services

- – **Metric**
  - – The percentage of services installed/running that are not enteprise essential
- – **Calculation**
  - – `M6 / M2`

8.9 4.9: Configure Trusted DNS Servers on Enterprise Assets

Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

8.9.1 Dependencies

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

8.9.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standard

8.9.3 Operations

1. Use `GV1` to identify and enumerate authorizsed DNS servers (M1)
2. Use `GV1` to identify and enumerate assets configured for authorized DNS servers (M2)
3. **Use `GV3` to check configuration of DNS servers identified on assets in Operation 2**
    1. Identify and enumerate assets with DNS servers that are properly configured (M3)
    2. Identify and enumerate assets with DNS servers that are improperly configured (M4)

8.9.4 Measures

- M1 = Count of authorized DNS servers
- M2 = Count of enterprise assets configured for DNS servers
- M3 = Count of assets with properly configured DNS servers
- M4 = Count of assets with improperly configured DNS servers

8.9.5 Metrics

Coverage

Metric	The percentage of assets with properlyn configured DNS servers
Calculation	`M3 / M2`

8.10 4.10: Enforce Automatic Device Lockout on Portable End-User Devices

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft? InTune Device Lock and Apple? Configuration Profile maxFailedAttempts.

Asset Type	Security Function	Implementation Groups
Devices	Respond	2, 3

8.10.1 Dependencies

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

8.10.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

8.10.3 Operations

1. Use `GV1` to identify and enumerate all portable devices (M1)
2. **Use `GV3` to check failed authentication configuration for all portable devices**
    1. Identify and enumerate failed authentication on laptops that is properly configured (20 failed attempts or less) (M2)
    2. Identify and enumerate failed authentication on laptops that is not properly configured (greater than 20 failed attempts) (M3)
    3. Identify and enumerate failed authentication on mobile devices that is properly configured (10 failed attempts or less) (M4)
    4. Identify and enumerate failed authentication on mobile devices that is not properly configured (greater than 10 failed attempts) (M5)

8.10.4 Measures

- M1 = Count of portable devices
- M2 = Count of properly configured laptops
- M3 = Count of improperly configured laptops
- M4 = Count of properly configured mobile devices
- M5 = Count of improperly configured mobile devices

8.10.5 Metrics

Compliance of Default Lockout

Metric	The percentage of portable devices with properly configured failed authentication.
Calculation	`(M2 + M4) / M1`

8.11 4.11: Enforce Remote Wipe Capability on Portable End-User Devices

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

8.11.1 Dependencies

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

8.11.2 Inputs

1. :code:`GV21: Portable end-user devices
2. `GV3`: Configuration standards

8.11.3 Operations

1. Use `GV21` to identify and enumerate portable end-user devices that support remote wipe (M1)
2. **Use `GV3` to check configuration for remote wipe on portable devices capable of supporting as identified in Operation 1**
    1. Identify and enumerate portable devices with properly configured remote wipe (M2)
    2. Identify and enumerate portable devices with improperly configured remote wipe (M3)

8.11.4 Measures

- M1 = Count of portable devices capable of supporting remote wipe
- M2 = Count of properly configured portable devices
- M3 = Count of improperly configured portable devices

8.11.5 Metrics

Compliance of Remote Wipe

Metric	The percentage of portable devices with properly configured remote wipe.
Calculation	`M2 / M1`

8.12 4.12: Separate Enterprise Workspaces on Mobile End-User Devices

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple? Configuration Profile or Android? Work Profile to separate enterprise applications and data from personal applications and data.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

8.12.1 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

8.12.2 Inputs

1. `GV21`: Portable end-user devices
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standards

8.12.3 Operations

1. Use `GV5` to identify and enumerate authorized mobile device management software (M1)
2. Use `GV21` to identify mobile devices capable of supporting mobile device management software (M2)
3. **Compare the output of Operations 1 and 2**
    1. Identify and enumerate mobile devices with authorized mobile device management software (M3)
    2. Identify and enumerate mobile devices without authorized mobile device management software (M4)
4. **Use `GV3` to check configurations of mobile devices with mobile device management software**
    1. Identify and enumerate mobile devices with properly configured mobile device management software to seperate enterprise workspace (M5)
    2. Identify and enumerate mobile devices with improperly configured mobile device management sotware (M6)

8.12.4 Measures

- M1 = Count of authorized mobile device management software
- M2 = Count of mobile devices capable of supporting mobile device management software
- M3 = Count of mobile devices with mobile device management software
- M4 = Count of mobile devices without mobile device management software
- M5 = Count of asssets with properly configured mobile device management software
- M6 = Count of asssets with improperly configured mobile device management software

8.12.5 Metrics

Compliance of Seperation of Enterprise Workspace

CHAPTER

NINE

CIS CONTROL 5: ACCOUNT MANAGEMENT

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why is this CIS Control Critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in CIS Control 8 (Audit Log Management), it is important in the development of a comprehensive Identity and Access Management (IAM) program.

9.1 5.1: Establish and Maintain an Inventory of Accounts

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

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

9.1.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

9.1.2 Inputs

1. `GV5`: Authorized software inventory
2. `GV22`: Inventory of accounts
3. Date of last review of the inventory of accounts

9.1.3 Operations

1. **Check if the enterprise maintains an inventory of user and administrative accounts (Input 2)**
    1. If the inventory exists M1 = 1
    2. If the inventory does not exist M1 = 0
2. **Using the inventory of accounts `GV22`, determine if the inventory captures the following elements: person's name, username, start/stop dates, and department**
    1. Each element is assigned a value of 1 if it exists and 0 if it does not. Total the number of elements that exist. (M3)
3. **Using `GV22` check each account for elements: person's name, username, start/stop dates, and department**
    1. Identify and enumerate accounts with all elements (M4)
    2. Identify and enumerate accounts missing or with incomplete elements (M5)
4. Use `GV5` to identify authentication systems or other software that manages accounts `GV23`.
5. Using the output of Operation 4, enumerate all current user and administrative accounts throughout the enterprise (M6)
6. **Compare the output of Operation 5 with `GV22`**
    1. Identify and enumerate accounts that are supposed to be active/enabled (M7)
    2. Identify and enumerate accounts that are supposed to be disabled/removed (M8)
7. Compare the current date to the date provided in Input 3 and enumerate the timeframe in months (M9)

9.1.4 Measures

- M1 = Does the account inventory exist (Output of Operation 1)
- M2 = Count of accounts in `GV22`
- M3 = Count of elements provided in inventory
- M4 = Count of accounts in inventory with complete information
- M5 = Count of accounts in inventory with missing or incomplete information
- M6 = Count of current accounts identified through Operation 5
- M7 = Count of authorized accounts
- M8 = Count of unauthorized accounts

- M9 = Timeframe of last update in months

9.1.5 Metrics

If M1 is 0, this safeguard receives a failing score and other metrics don't apply. If M9 is greater than three, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	The percentage of minimum elements included in the inventory.
Calculation	`M3 / 4`
Metric	The percentage of accounts with complete information.
Calculation	`M4 / 2`

Accuracy of Inventory

Metric	The percentage of accurately listed accounts in the inventory.
Calculation	`M8 / M6`

9.2 5.2: Use Unique Passwords

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

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

9.2.1 Dependencies

- None

9.2.2 Inputs

1. `GV20`: Unique password policy for the enterprise

9.2.3 Operations

1. **Check if the enterprise has a unique password policy**
    1. If policy is available M1 = 1
    2. Otherwise M1 = 0
2. **Review the policy and determine whether it includes password guidance for accounts without MFA**
    1. **If guidance is included M2 = 1**
        1. **Does guidance, at a minimum, require a fourteen character password**
            1. If password guidance is fourteen characters or longer M3 = 1
            2. Otherwise M3 = 0
    2. Otherwise M2 = 0
3. **Review the policy and determine whether it includes password guidance for accounts with MFA**
    1. **If guidance is included M4 = 1**

        # Does guidance, at a minimu, require an eight character password
        1. If password guidance is eight characters or longer M5 = 1
        2. Otherwise M5 = 0
    2. Otherwise M3 = 0

9.2.4 Measures

- M1 = Does a password policy exist
- M2 = Does guidance exist for accounts without MFA
- M3 = Does guidance for accounts without MFA meet minimum guidance
- M4 = Does guidance exist for accounts with MFA
- M5 = Does guidance for accounts with MFA meet minimum guidance

9.2.5 Metrics

If M1 is 0, the safeguard recieves a failing score. Other metrics don't apply

Completeness of Password Policy

Metric	The percentage of completeness of the unique password policy
Calculation	`(M2 + M4) / 2`

Strength of Policy

Metric	The percentage of password guidance that meets minimum character length standards
Calculation	`(M3 + M5) / 2`

9.3 5.3: Disable Dormant Accounts

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported

Asset Type	Security Function	Implementation Groups
Users	Respond	1, 2, 3

9.3.1 Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

9.3.2 Inputs

1. `GV22`: Inventory of accounts
2. Enterprise defined policy for dormant threshold

9.3.3 Assumptions

1. The list of accounts for the enterprise includes OS-level, database, internal and external application accounts.
2. A query interface is assumed to enable collection of a "last activity" timestamp, such as last logon, as well as a status indicating if the account is enabled or disabled.

9.3.4 Operations

1. Review Input 2 and note the dormant threshold in terms of days (M2)
2. **For each account in GV22, query the interface and collect**
    1. The date of last activity for each account
    2. Whether the account is disabled or not
3. **Using the output of Operation 2.1 and Input 2**
    1. Identify and enumerate accounts that have exceeded the dormant threshold (M3)
    2. Identify and enumerate accounts that are still within the dormant threshold (M4)
4. **Use the output of Operation 2.2 and 3.1 (M3)**
    1. Identify and enumerate accounts that are disabled (M5)
    2. Identify and enumerate accounts that are still enabled (M6)

9.3.5 Measures

- M1 = Count of accounts in GV22
- M2 = Timeframe of dormant threshold in days
- M3 = Count of dormant accounts
- M4 = Count of active accounts
- M5 = Count of dormant accounts that have been disabled
- M6 = Count of dormant accounts still enabled

9.3.6 Metrics

Dormant Accounts

Enabled Dormant Accounts

Metric	The percentage of dormant accounts still enabled
Calculation	M6 / M3

9.4 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

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

9.4.1 Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

9.4.2 Inputs

1. `GV22`: Inventory of accounts
2. List of users identified as administrators

9.4.3 Assumptions

1. For the purpose of this control, it is assumed that users identified as administrators that have an active administrative and non-administrative account have properly dedicated accounts for administrative privileges.

9.4.4 Operations

1. **Using `GV22` and Input 2**
    1. Identify and enumerate users identified as administrators with active administrator accounts (M1)
    2. Identify and enumerate users identified as administrators without active administrator accounts (M2)
    3. Identify and enumerate users not identified as administrators with active administrator accounts (M3)
2. **Using `GV22` and output of Operation 1.1**
    1. Identify and enumerate users identified as administrators that have an active non-administrative user account (M4)
    2. Identify and enumerate users identified as administrators that do not have an active non-administrative user account (M5)

9.4.5 Measures

- M1 = Count of authorized administrative users with active administrator accounts
- M2 = Count of authorized administrative users without active administrator accounts
- M3 = Count of non-administrative users with active administrator accounts
- M4 = Count of authorized administrative users with an active administrative and non-administrative account
- M5 = Count of authorized administrative users without an active administrative and non-administrative account
- M6 = Count of Input 2

9.4.6 Metrics

Administrative User Accounts

Metric	The perecentage of administrative users with both an administrative account and non-administrative acount.
Calculation	`M4/ M6`

Unauthorized Administrative Accounts

Metric	The percentage of unauthorized administrative accounts
Calculation	`M3 / (M1 + M3)`

9.5 5.5: Establish and Maintain an Inventory of Service Accounts

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Asset Type	Security Function	Implementation Groups
Users	Identify	2, 3

9.5.1 Dependencies

- Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

9.5.2 Inputs

1. `GV23`: Authentication and Authorizaion System Inventory
2. Inventory of service accounts
3. Date of last review of the inventory of service accounts

9.5.3 Operations

1. **Check if the enterprise maintains an inventory of service accounts (Input 2)**
    1. If the inventory exists M1 = 1
    2. If the inventory does not exist M1 = 0
2. **Using the inventory of accounts Input 2, determine if the inventory captures the following elements: department owner, review date, and purpose**
    1. Each element is assigned a value of 1 if it exists and 0 if it does not. Total the number of elements that exist. (M3)
3. **Using Input 2 check each account for elements: department owner, review date, and purpose**
    1. Identify and enumerate accounts with all elements (M4)
    2. Identify and enumerate accounts missing or with incomplete elements (M5)
4. Use `GV23` to identify authentication systems or other software that manages service accounts.
5. Using the output of Operation 4, enumerate all current service accounts throughout the enterprise (M6)
6. **Compare the output of Operation 5 with Input 2**
    1. Identify and enumerate accounts that are supposed to be active/enabled (M7)
    2. Identify and enumerate accounts that are supposed to be disabled/removed (M8)
7. Compare the current date to the date provided in Input 3 and enumerate the timeframe in months (M9)

9.5.4 Measures

- M1 = Does the account inventory exist (Output of Operation 1)
- M2 = Count of accounts in Input 2
- M3 = Count of elements provided in inventory
- M4 = Count of accounts in inventory with complete information
- M5 = Count of accounts in inventory with missing or incomplete information
- M6 = Count of current service accounts identified through Operation 5
- M7 = Count of authorized accounts
- M8 = Count of unauthorized accounts
- M9 = Timeframe of last update in months

9.5.5 Metrics

If M1 is 0, this safeguard receives a failing score and other metrics don't apply. If M9 is greater than three, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	The percentage of minimum elements included in the inventory.
Calculation	`M3 / 4`
Metric	The percentage of accounts with complete information.
Calculation	`M4 / 2`

Accuracy of Inventory

Metric	The percentage of accurately listed accounts in the inventory.
Calculation	`M8 / M6`

9.6 5.6: Centralize Account Management

Centralize account management through a directory or identity service.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

9.6.1 Dependencies

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

9.6.2 Inputs

1. `GV1`: Enterprise asset inventory

9.6.3 Operations

1. Using `GV1` identify and enumerate centralized auhtentication points (M1)
2. **For each centralized authentication point indentifed in Operation 1, determine whether it is necessary or can be consolidated**
    1. Identify and enumerate authentication points that are unnecesary or can be consolidated (M2)
    2. Identify and enumerate authentication points that are necesary and cannot be consolidated (M3)

9.6.4 Measures

- M1 = Count of cetralized authentication points in the enterprise
- M2 = Count of unnecessary centralized authentication points
- M3 = Count of necessary centralized authentication points

9.6.5 Metrics

Coverage

Metric	Percentage of properly centralized aunthentication points
Calculation	`M3 / M1`

CHAPTER

TEN

CIS CONTROL 6: ACCESS CONTROL MANAGEMENT

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why is this CIS Control Critical?

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

There are some user activities that pose greater risk to an enterprise, either because they are accessed from untrusted networks, or performing administrator functions that allow the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them less secure. This also enforces the importance of using MFA and Privileged Access Management (PAM) tools.

Some users have access to enterprise assets or data they do not need for their role; this might be due to an immature process that gives all users all access, or lingering access as users change roles within the enterprise over time. Local administrator privileges to users' laptops is also an issue, as any malicious code installed or downloaded by the user can have greater impact on the enterprise asset running as administrator. User, administrator, and service account access should be based on enterprise role and need.

10.1 6.1: Establish an Access Granting Process

Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

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

10.1.1 Dependencies

- None

10.1.2 Inputs

1. Enterprise process for granting access to enterprise assets

10.1.3 Operations

1. **Check to see if Input 1 exists**
    1. If the enterprise has an access granting process, M1 = 1
    2. If the enterprise does not have an access granting process, M1 = 0
2. **Using Input 1, check to see if the process, includes at a minimum, a way to grant access upon new hire, rights grat, and role change of a user.**
    1. For each element that is include, assign a value of 1. Sum the value of the elemnts included. (M2)

10.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of elements included in the access granting process

10.1.5 Metrics

If M1 is 0, the safeguard receives a failing score. The other metric don't apply.

Completeness of Process

Metric	The percentage of elements included in the access granting process
Calculation	`M2 / 3`

10.2 6.2: Establish an Access Revoking Process

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

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

10.2.1 Dependencies

- None

10.2.2 Inputs

1. Enterprise process for revoking access to enterprise assets

10.2.3 Operations

1. **Check to see if Input 1 exists**
    1. If the enterprise has an access revoking process, M1 = 1
    2. If the enterprise does not have an access revoking process, M1 = 0
2. **Using Input 1, check to see if the process, includes at a minimum, a way to revoke access upon termination, rights revocation, and role change of a user.**
    1. For each element that is include, assign a value of 1. Sum the value of the elemnts included. (M2)

10.2.4 Measures

- M1 = Output of Operation 1
- M2 = Count of elements included in the access revoking process

10.2.5 Metrics

If M1 is 0, the safeguard receives a failing score. The other metric don't apply.

Completeness of Process

Metric	The percentage of elements included in the access granting process
Calculation	`M2 / 3`

10.3 6.3: Require MFA for Externally-Exposed Applications

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

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

10.3.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

10.3.2 Inputs

1. `GV5`: Authorized Software Inventory
2. `GV22`: Inventory of Accounts
3. `GV3`: Configuration Standard

10.3.3 Operations

1. Use Input 1 to identify and enumerate externally exposed and third party applications
2. Using the output of Operation 1 and `GV22` identify and enumerate all user accounts associated with the applications (M1)
3. **For each account identified in Operation 2 use `GV3` to**
    1. Identify and enumerate accounts properly configured to require MFA (M2)
    2. Identify and enumerate accounts not properly configured to require MFA (M3)

10.3.4 Measures

- M1 = Count of accounts associated with externally exposed and third party applications
- M2 = Count of accounts properly configured to require MFA
- M3 = Count of accounts not properly configured to require MFA

10.3.5 Metrics

Coverage

10.4 6.4: Require MFA for Remote Network Access

Require MFA for remote network access.

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

10.4.1 Dependencies

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

10.4.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

10.4.3 Operations

1. Using `GV1` as a guide, identify and enumerate all authorized remote assets (M1)
2. **For each asset identified in Operation 1, check configurations `GV3`**
    1. Identify and enumerate assets properly configured to require MFA (M2)
    2. Identify and enumerate assets not properly configured to require MFA (M3)

10.4.4 Measures

- M1 = Count of remote assets
- M2 = Count of remote assets properly configured to require MFA
- M3 = Count of remote assets not properly configured to require MFA

10.4.5 Metrics

Coverage

Metric	The percentage of remote assets poperly configured to require MFA	`M2 / M1`

10.5 6.5: Require MFA for Administrative Access

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

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

10.5.1 Dependencies

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

10.5.2 Inputs

1. `GV22`: Inventory of accounts
2. `GV3`: Configuration Standard

10.5.3 Operations

1. Using `GV22` identify and enumerate all administrative accounts (M1)
2. **For each administrative account identified in Operation 1 check configurations in `GV3`**
    1. Identify and enumerate administrative accounts properly configured to require MFA (M2)
    2. Identify and enumerate administrative accounts not properly configure to require MFA (M3)

10.5.4 Measures

- M1 = Count of administrative accounts
- M2 = Count of administrative accounts properly configured to require MFA
- M3 = Count of administrative accounts not properly configured to require MFA

10.5.5 Metrics

Coverage

10.6 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Users	Identify	2, 3

10.6.1 Dependencies

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

10.6.2 Inputs

1. `GV23`: Authentication and Authorization System Inventory
2. `GV5`: Authorized software inventory
3. Date of last update to the authentication and authorization system inventory

10.6.3 Operations

1. **Check if enterprise maintains an `GV23` Authentication and Authorization System Inventory of all on-site and remote service providers**
    1. If the inventory exists, M1 = 1
    2. If the inventory does not exist or is not provided, M1 = 0
2. Use `GV5` identify and enumerate authorized authentication and authorization systems within the enterprise
3. **Use the output of Operation 2 to compare to the existing inventory `GV23`**
    1. Identify and enumerate systems that are authorized and currently in the inventory (M2)
    2. Identify and enumerate systems that are authorized and not currently in the inventory (M3)
    3. Identify and enumarate systems that are not authorized but listed in the current inventory (M4)
4. Compare the date of Input 3 to the current date and capture timeframe in months (M6)

10.6.4 Measures

- M1 = Ouptut of Operation 1
- M2 = Count of authorized and properly inventoried systems
- M3 = Count of authorized but not properly inventoried systems
- M4 = Count of unauthorized but inventoried systems
- M5 = Count of systems in the current inventory `GV23`
- M6 = Timeframe since last update of inventory

10.6.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M6 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Accuracy Score

10.7 6.7: Centralize Access Control

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

10.7.1 Dependencies

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

10.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

10.7.3 Operations

1. Use `GV5` to identify all directory and SSO services
2. Use `GV1` to identify and enumerate assets that support directory and SSO services (M1)
3. **Check the output of Operations 1 and 2 to ensure each asset is covered by at least one directory or SSO service**
    1. Identify and enumerate assets that are covered by at least one directory or SSO services (M2)
    2. Identify and enumerate assets that are not covered by at least one directory or SSO service (M3)

10.7.4 Measures

- M1 = Count of assets capable of supporing directory and/or SSO services
- M2 = Count of assets covered by at least one directory or SSO service
- M3 = Count of assets not covered by at least one directory or SSO service

10.7.5 Metrics

Coverage

10.8 6.8: Define and Maintain Role-Based Access Control

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

10.8.1 Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

10.8.2 Inputs

1. Enterprise documented process for assigning role-based access control
2. `GV22`: Inventory of accounts
3. Date of last validation of role-based access control

10.8.3 Operations

1. **Determine whether the enterprise has a process for assigning role-based access control**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 1
2. **Use `GV22` and check if each account is assigned a role or group as outlined by the role-based access control process**
    1. Identify and enumerate accounts that are assigned a role or group (M3)
    2. Identify and enumerate accounts that are not assigned a role or group (M4)
3. Compare the date in Input 3 to the current date and capture timeframe in months (M5)

10.8.4 Measures

- M1 = Does a role-based access control process exist as defined by the Output of Operation 1
- M2 = Count of `GV22`
- M3 = Count of accounts found in the inventory with assigned role or group
- M4 = Count of accounts found in the inventory not assigned a role or group
- M5 = Timeframe in months of last review of role-bases access control process

10.8.5 Metrics

If M1 is 0, this safeguard receives a failing score. The other metrics don't apply. If M5 is greater than twelve months, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

CHAPTER

ELEVEN

CIS CONTROL 7: CONTINUOUS VULNERABILITY MANAGEMENT

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is this CIS Control Critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches , and install the patch.

There is never perfection in this process. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability referred to as a "zero-day" exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders must keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g., vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate, and therefore need to use other controls to mitigate.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, while not impacting the enterprise's business or mission.

11.1 7.1: Establish and Maintain a Vulnerability Management Process

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

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

11.1.1 Dependencies

- None

11.1.2 Inputs

1. Enterprise vulnerability management process
2. Date of last update to the vulnerability management process

11.1.3 Operations

1. **Determine wether the enterprise maintains a vulnerability management process**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Compare the date from Input 1 to the curren date and enumerate timeframe in months (M2)

11.1.4 Measures

- M1 = Output of Operation 1
- M2 = Timeframe since last update to vulnerability management process

11.1.5 Metrics

If M1 is 0, this safeguard receives a failing score. The other metrics don't apply. If M2 is greater than twelve, this safeguard receives a failing score. The other metrics don't apply.

11.2 7.2: Establish and Maintain a Remediation Process

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Asset Type	Security Function	Implementation Groups
Applications	Respond	1, 2, 3

11.2.1 Dependencies

- None

11.2.2 Inputs

1. Enterprise remediation strategy process
2. Date of last review of the process
3. GV18: Enterprise assets storing, processing, and transmitting sensitive data

11.2.3 Operations

1. **Determine whether the enterprise maintains a documented remediation process**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. **Check the documented remediation process to identify whether it includes a risk based process based on the following elements: Sensitive assets GV18 and criticality of vulnerability**
    1. Each element, if included, gets a value of 1. Sum all elements (M2)
3. Compare the date from Input 2 and current date. Enumerate the timeframe in terms of days (M3)

11.2.4 Measures

- M1 = Output of Operation 1
- M2 = Sum of elements included in the remediation process
- M3 = Timeframe since last review of process in days

11.2.5 Metrics

If M1 is 0, the safeguard receives a failing score. The other metrics don't apply. If M3 is greater than thirty, the safeguard receives a failing score. The other metrics don't apply.

Completenes

Metric	The percentage of elements included in the process
Calculation	`M2 / 2`

11.3 7.3: Perform Automated Operating System Patch Management

Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

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

11.3.1 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

11.3.2 Inputs

1. `GV5`: Authorized software inventory
2. `GV1`: Enterprise asset inventory
3. Authoritative source of information indicating version details by product
4. `GV3`: Configuration standards

11.3.3 Operations

1. Use `GV5` to identify authorized operating systems within the enterprise
2. Use `GV1` and the output of Operation 1 to identify the operating system currently running on each asset (M1)
3. **For each asset, compare the version of the operating system to that listed in Input 4**
    1. Identify and enumerate operating systems that are up to date (M2)
    2. Identify and enumerate operating systems that are not up to date (M3)
4. **For each operating system idetified in Operation 2.2, determine whether there is a documented exception**
    1. Identify and enumerate operating systems with a documented exception (M4)
    2. Identify and enumerate operating systems without a documented exception (M5)
5. Use `GV5` to identify authorized automated patch management software (M6)
6. **Compare output of Operation 5 and Operation 1**
    1. Identify and enumerate operating systems covered by at least one automated patch management software (M7)
    2. Identify and enumerate operating systems not covered by at least one automated patch management software (M8)
7. **Check configurations of automated patch mangement software identified in Operation 5 using `GV3`**
    1. Identify and enumerate those configured to run every 30 days or less (M9)
    2. Identify and enumerate those not configured to run every 30 days or less (M10)

11.3.4 Measures

- M1 = Count of authorized operating sytem installed on an asset
- M2 = Count of up to date operating system installed on an asset
- M3 = Count of operating system installed on an asset that is not up to date
- M4 = Count of not up to date operating system with a documented exception
- M5 = Count of not up to date operating system without a documented exception
- M6 = Count of authorized automated patch management software
- M7 = Count of operating systems covered by at least one automated patch management software
- M8 = Count of operating systems not covered by at least one automated patch management software
- M9 = Count of automated patch management software properly configured to run every 30 days or less
- M10 = Count of automated patch management software not properly configured to run every 30 days

11.3.5 Metrics

Update Effectiveness (Per Asset)

Metric	The percent of operating system on an asset that are up to date
Calculation	`(M2 + M4) / M1`

Update Effectiveness (Organizational)

Calculate the organizational metric by averaging the asset scores

Coverage of Automation

Scan Compliance

11.4 7.4: Perform Automated Application Patch Management

Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

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

11.4.1 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

11.4.2 Inputs

1. `GV5`: Authorized software inventory
2. `GV1`: Enterprise asset inventory
3. Authoritative source of information indicating version details by product
4. `GV3`: Configuration standards
5. `GV24`: Authorized automated patch management software

11.4.3 Operations

1. Use `GV5` to identify authorized applications within the enterprise
2. Use `GV1` and the output of Operation 1 to identify the applications currently running on each asset (M1)
3. **For each asset, compare the version of the application to that listed in Input 4**
    1. Identify and enumerate applications that are up to date (M2)
    2. Identify and enumerate applications that are not up to date (M3)
4. **For each application idetified in Operation 2.2, determine whether there is a documented exception**
    1. Identify and enumerate applications with a documented exception (M4)
    2. Identify and enumerate applications without a documented exception (M5)
5. **Compare `GV24` and Operation 1**
    1. Identify and enumerate applications covered by at least one automated patch management software (M7)
    2. Identify and enumerate applications not covered by at least one automated patch management software (M8)
6. **Check configurations of automated patch mangement software `GV24` using `GV3`**
    1. Identify and enumerate those configured to run every 30 days or less (M9)
    2. Identify and enumerate those not configured to run every 30 days or less (M10)

11.4.4 Measures

- M1 = Count of authorized applications installed on an asset
- M2 = Count of up to date applications installed on an asset
- M3 = Count of applications installed on an asset that is not up to date
- M4 = Count of not up to date applications with a documented exception
- M5 = Count of not up to date applications without a documented exception
- M6 = Count of `GV24` authorized automated patch management software
- M7 = Count of applications covered by at least one automated patch management software
- M8 = Count of applications not covered by at least one automated patch management software
- M9 = Count of automated patch management software properly configured to run every 30 days or less
- M10 = Count of automated patch management software not properly configured to run every 30 days

11.4.5 Metrics

If M4 is greater than thirty, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Update Effectiveness (Per Asset)

Metric	The percent of applications on an asset that are up to date
Calculation	`(M2 + M4) / M1`

Update Effectiveness (Organizational)

Calculate the organizational metric by averaging the asset scores

Coverage of Automation

Scan Compliance

11.5 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

Asset Type	Security Function	Implementation Groups
Applications	Identify	2, 3

11.5.1 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

11.5.2 Inputs

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

11.5.3 Operations

1. **Use the :code:`GV5`authorized software inventory to**
    1. Identify and enumerate `GV25` vulnerability scanning software (M1)
    2. Identify and enumerate authenticated vulnerability scanning software (M2)
2. Use the `GV1` enterprise asset inventory to identify and enumerate all internal assets (M3)
3. **Use the output of Operation 2 and Operation 1.1**
    1. Identify and enumerate internal assets covered by at least one vulnerability scanning software (M4)
    2. Identify and enumerate internal assets not covered by at least one vulnerability scanning software (M5)
4. **Use the output of Operation 2 and Operation 1.2**
    1. Identify and enumerate internal assets covered by at least one authenticated vulnerability scanner (M6)
    2. Identify and enumerate internal assets not covered by at least one authenticated vulnerability scanner (M7)
5. **Use the output of Operation 1.1 and `GV3`**
    1. Identify and enumerate vulnerability scanners properly configured to scan every 3 months or less (M8)
    2. Identify and enumerate vulnerability scanners not properly configured to scan every 3 months or less (M9)
6. **Use the output of Operation 1.2 and `GV3`**
    1. Identify and enumerate authenticated vulnerability scanners properly configured to scan every 3 months or less (M10)
    2. Identify and enumerate authenticated vulnerability scanners not properly configured to scan every 3 months or less (M11)

11.5.4 Measures

- M1 = Count of authorized vulnerability scanning software
- M2 = Count of authorized authenticated vulnerability scanning software
- M3 = Count of internal enterprise assets
- M4 = Count of internal assets covered by a vulnerability scanner
- M5 = Count of internal assets not covered by a vulnerability scanner
- M6 = Count of internal assets covered by an authenticated vulnerability scanner
- M7 = Count of internal assets not covered by an authenticated vulnerability scanner
- M8 = Count of vulnerability scanners properly configured to run every 3 months or less
- M9 = Count of vulnerability scanners not properly configured to run every 3 months or less
- M10 = Count of authenticated vulnerability scanners properly configured to run every 3 months or less
- M11 = Count of authenticated vulnerability scanners not properly configured to run every 3 months or less

11.5.5 Metrics

Coverage of Vulnerability Scans

Metric	The percentage of internal assets covered by a vulnerability scanner
Calculation	`M4 / M3`

Coverage of Authenticated Scans

Compliance of Vulnerability Scans

Compliance of Authenticated Scans

11.6 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.

Asset Type	Security Function	Implementation Groups
Applications	Identify	2, 3

11.6.1 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

11.6.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV25`: Vulnerability scanning software
3. `GV3`: Configuration standard

11.6.3 Operations

1. Use the `GV1` enterprise asset inventory to identify and enumerate all external assets (M2)
2. **Use the output of Operation 1 and `GV25` to**
    1. Identify and enumerate external assets covered by at least one vulnerability scanning software (M3)
    2. Identify and enumerate external assets not covered by at least one vulnerability scanning software (M4)
3. **Use the `GV25` and `GV3`**
    1. Identify and enumerate vulnerability scanners properly configured to scan every 30 days or less (M5)
    2. Identify and enumerate vulnerability scanners not properly configured to scan every 30 days or less (M6)

11.6.4 Measures

- M1 = Count of authorized `GV25` vulnerability scanning software
- M2 = Count of external enterprise assets
- M3 = Count of external assets covered by a vulnerability scanner
- M4 = Count of external assets not covered by a vulnerability scanner
- M5 = Count of vulnerability scanners properly configured to run every 30 days or less
- M6 = Count of vulnerability scanners not properly configured to run every 30 days or less

11.6.5 Metrics

Coverage of Vulnerability Scans

Metric	The percentage of external assets covered by a vulnerability scanner
Calculation	`M3 / M2`

Compliance of Vulnerability Scans

11.7 7.7: Remediate Detected Vulnerabilities

Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Asset Type	Security Function	Implementation Groups
Applications	Respond	2, 3

11.7.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

11.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. Current vulnerability scan
3. Previous vulnerability scan
4. Date of current vulnerability scan
5. Date of previous vulnerability scan

11.7.3 Assumptions

1. Asset-Vulnerability combinations not found in most recent scan is indicative of remediation of that vulnerability on that asset.

11.7.4 Operations

1. **For each asset in `GV1`, compare Inputs 2 and 3**
    1. Identify and enumerate assets listed with the same vulnerability on both scans (M2)
    2. Identify and enumerate assets previously found in Input 3 that are no longer listed in Input 2 with the same vulnerability (M3)
2. Compare Inputs 4 and 5 and capture timeframe between scans in days (M4)

11.7.5 Measures

- M1 = Count of vulnerabilities identified in Input 3
- M2 = Count of unremediated vulnerabilities
- M3 = Count of remediated vulnerabilities
- M4 = Timeframe in between scans

11.7.6 Metrics

If M4 is greater than thirty, this safeguard receives a failing score. The other metrics don't apply.

Remediation

Metric	The percentage of remediated vulnerabilities
Calculation	`M3 / M1`

CHAPTER

TWELVE

CIS CONTROL 8: AUDIT LOG MANAGEMENT

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why is this CIS Control Critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems, and take less configuration to turn on. Audit logs typically include user-level events – when a user logged in, accessed a file, etc. – and take more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

12.1 8.1: Establish and Maintain an Audit Log Management Process

Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

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

12.1.1 Dependencies

- None

12.1.2 Inputs

1. `GV26`: Enterprise's audit log management process
2. Date of last review of the audit log management process

12.1.3 Operations

1. **Check if :code:`GV26`the audit log management process exists**
    1. If it exists, M1 = 1
    2. If it does not exist, M1 = 0
2. **Review `GV26` for elements of the process, at a minimum, address the collection, review, and retention of audit logs for enterprise assets.**
    1. For each element that exists, assign a value of 1. Sum the values of existing elements. (M2)
3. Compare the date from Input 2 and the current date. Capture the timeframe in terms of months. (M3)

12.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of elements included in the audit log management process
- M3 = Timeframe since last review of the autid log management process

12.1.5 Metrics

If M1 is 0, this safeguard receives a failing a score. The other metrics don't apply. If M3 is greater than twelve, this safeguard is measured at a 0 and receives a failing score. THe other metrics don't apply.

Completeness

12.2 8.2: Collect Audit Logs

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Asset Type	Security Function	Implementation Groups
Network	Detect	1, 2, 3

12.2.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 8.1: Establish and Maintain an Audit Log Management Process

12.2.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards
3. `GV26`: Enterprise's audit log management process

12.2.3 Operations

1. Use `GV1` to identify and enumerate assets capable of supporting logging `GV27` (M1)
2. **Use `GV26` and `GV3` as guides to determine, for each asset identifed in Operation 1 is configured to log events as outlined by the enterprise's process**
    1. Identify and enumerate assets properly configured to log events per the process (M2)
    2. Identify and enumerate assets not properly configured to log events per the process (M3)

12.2.4 Measures

- M1 = Count of assets capable of supporting logging
- M2 = Count of properly configured assets to log events per the audit log management process
- M3 = Count of assets not properly configured to log events per the audit log management process

12.2.5 Metrics

Coverage

Metric	The ratio of logging capable assets properly configured per the audit log management process.
Calculation	`M2 / M1`

12.3 8.3: Ensure Adequate Audit Log Storage

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

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

12.3.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

12.3.2 Inputs

1. `GV27`: Assets capable of supporting logging
2. `GV26`: Enterprise's audit log management process

12.3.3 Assumptions

1. It is assumed that if the an asset is properly configured to meet the retention policy, that would include log rotation, maximum storage size, etc.

12.3.4 Operations

1. For each asset in `GV27` collect the asset's logging configuration
2. **Compare the output of Operation 1 and the retention portion of `G26`**
    1. Identify and enumerate assets configured to comply with the retention portion of the process (M2)
    2. Identify and enumerate assets not configured to comply with the retention portion of the process (M3)

12.3.5 Measures

- M1 = Count of `GV27` assets capable of supporting logging
- M2 = Count of assets properly configured to meet retention requirements
- M3 = Count of assets not properly configured to meet retention requirements

12.3.6 Metrics

Logging Storage Coverage

12.4 8.4: Standardize Time Synchronization

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

12.4.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

12.4.2 Inputs

1. `GV27`: Assets capable of supporting logging
2. List of approved network time sources/NTP servers

12.4.3 Operations

1. Using :code:'GV27`, identify and enumerate assets capable of supporting time synchronization (M1)
2. **Check the configurations of the assets identified in Operation 1**
    1. Identify and enumerate the assets configured using at least two approved time sources from Input 2 (M2)
    2. Identify and enumerate the assets configured using time sources not on the approved list (M3)
    3. Identify and enumerate the assets not configured using time sources (M4)

12.4.4 Measures

- M1 = Count of logging capable assets that support time synchronization
- M2 = Count of properly configured assets using at least two approve time sources
- M3 = Count of assets configured using non-approved time sources
- M4 = Count of assets not configured to use time sources

12.4.5 Metrics

NTP Compliance Coverage

Metric	The percentage of assets propery configured to with at least two approved synchronized time sources.
Calculation	`M2 / M1`

12.5 8.5: Collect Detailed Audit Logs

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.5.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

12.5.2 Inputs

1. `GV18`: Enterprise assets storing, processing, and transmitting sensitive data
2. `GV26`: Enterprise's audit log management process
3. `GV3`: Configuration standards

12.5.3 Operations

1. **Review `GV26` for detailed logging requirements such as event source, date, username, timestamp, source addresses, and destination addresses.**
    1. For each detailed logging requirement included, assign a value of 1. Sum all requirements included. (M2)
2. **For each asset in `GV18` check configuraions using `GV3` as a guide**
    1. Identify and enumerate assets properly configured to collect detailed logging requirements (M3)
    2. Identify and enumerate assets not properly configured to collect detailed logging requirements (M4)

12.5.4 Measures

- M1 = Count of assets capable of supporting logging GV27
- M2 = Count of detailed logging requirements included in log management process
- M3 = Count of assets properly configured to collect detailed logs
- M4 = Count of assets not properly configured to collect detailed logs

12.5.5 Metrics

Completeness of Process

Logging Coverage

12.6 8.6: Collect DNS Query Audit Logs

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.6.1 Dependencies

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

12.6.2 Inputs

1. GV1: Enterprise asset inventory
2. GV3: Configuration standards

12.6.3 Assumptions

1. The enterprise maintains their own internal DNS Servers.

12.6.4 Operations

1. Use Input 1 GV1 to identify and enumerate internal DNS Servers (M1)
2. **Check the configurations GV3 of each DNS Server identified in Operation 1**
    1. Identify and enumerate DNS servers properly configured to collect logs (M2)
    2. Identify and enumerate DNS servers not properly configured to collect logs (M3)

12.6.5 Measures

- M1 = Count of internal DNS servers
- M2 = Count of properly configured DNS servers
- M3 = Count of DNS servers not properly configured DNS servers

12.6.6 Metrics

DNS Configuration Coverage

Metric	The percentage of properly configured DNS servers to meet logging requirements.
Calculation	`M2 / M1`

12.7 8.7: Collect URL Request Audit Logs

Collect URL request audit logs on enterprise assets, where appropriate and supported.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.7.1 Dependencies

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

12.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

12.7.3 Operations

1. Use `GV1` to identify and enumerate assets that support URL logging (M1)
2. **For each asset identified in Operation 1, use `GV3` to check configurations for URL logging**
    1. Identify and enumerate assets properly configured for logging (M2)
    2. Identify and enumerate assets not properly configured for logging (M3)

12.7.4 Measures

- M1 = Count of assets capable of supporting URL logging
- M2 = Count of assets properly configured for URL logging
- M3 = Count of assets not properly configured for URL logging

12.7.5 Metrics

Configuration Coverage

Metric	The percentage of assets properly cofigured for URL logging
Calculation	`M2 / M1`

12.8 8.8: Collect Command-Line Audit Logs

Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals..

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

12.8.1 Dependencies

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

12.8.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

12.8.3 Operations

1. Use `GV1` to identify and enumerate assets that support command line auditing of command shells (M1)
2. **For each asset identified in Operation 1, use `GV3` to check configurations for command line auditing of command shells**
    1. Identify and enumerate assets properly configured (M2)
    2. Identify and enumerate assets not properly configured (M3)

12.8.4 Measures

- M1 = Count of assets capable of supporting command line auditing of command shells
- M2 = Count of assets properly configured for command line auditing of command shells
- M3 = Count of assets not properly configured for command line auditing of command shells

12.8.5 Metrics

Configuration Coverage

Metric	The percentage of assets properly cofigured for command line auditing of command shells.
Calculation	`M2 / M1`

12.9 8.9: Centralize Audit Logs

Centralize, to the extent possible, audit log collection and retention across enterprise assets.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.9.1 Dependencies

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

12.9.2 Inputs

1. `GV27`: Assets capable of supporting logging
2. `GV5`: Authorized software inventory

12.9.3 Operations

1. Use the software inventory `GV5` to identify and enumerate log aggregating software `GV28`
2. **For each asset capable of supporting logging, check if asset is covered by at least one log aggregating software**
    1. Identify and enumerate assets covered by at least one aggregating software (M2)
    2. Identify and enumerate assets not covered by at least one aggregating software (M3)

12.9.4 Measures

- M1 = Count of GV27
- M2 = Count of assets covered by at least one aggregating software
- M3 = Count of assets not covered by at least one aggregating software

12.9.5 Metrics

Log Aggregating

Metric	The percentage of log producing assets covered by aggregating software.
Calculation	M2 / M1

12.10 8.10: Retain Audit Logs

Retain audit logs across enterprise assets for a minimum of 90 days.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

12.10.1 Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 8.9: Centralize Audit Logs

12.10.2 Inputs

1. GV28: Log aggregating software
2. GV3: Configuration standards

12.10.3 Operations

1. **For each log aggregating software GV28 use GV3 to check configuration standards**
    1. Identify and enumerate aggregating software configured to retain logs for 90 days or more (M2)
    2. Identify and enumerate aggregating software configured to retain logs for less than 90 days (M3)

12.10.4 Measures

- M1 = Count of log aggregating software `GV28`
- M2 = Count of aggregating software properly configured to retain logs for 90 days or more
- M3 = Count of aggregating software configured to retainlogs for less than 90 days

12.10.5 Metrics

Compliance

Metric	The percentage of aggregating software properly configured to retain logs for 90 days or more.
Calculation	`M2 / M1`

12.11 8.11: Conduct Audit Log Reviews

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis..

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

12.11.1 Dependencies

- None

12.11.2 Inputs

1. Timestamp for two consecutive log reviews

12.11.3 Assumptions

1. Log reviews are conducted at regular and consistent intervals

12.11.4 Operations

1. Compare each timestamp to determine timeframe between log reviews in days (M1)

12.11.5 Measures

- M1 = Timeframe between log reviews

12.11.6 Metrics

If M1 is greater than seven, this safeguard is measured at a 0 and receives a failing score.

12.12 8.12: Collect Service Provider Logs

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events

Asset Type	Security Function	Implementation Groups
Data	Detect	3

12.12.1 Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

12.12.2 Inputs

1. `GV29`: Inventory of service providers
2. `GV3`: Configuration standard

12.12.3 Operations

1. For each service provided in `GV29` identify and enumerate service providers that supports logging (M1)
2. **Use service provider identified in Operation 1, use `GV3` to check configurations**
    1. Identify and enumerate service providers properly configured to collect logs (M2)
    2. Identify and enumerate service providers not properly configured to collect logs (M3)

12.12.4 Measures

- M1 = Count of service providers that support logging
- M2 = Count of service providers configured to collect logs
- M3 = Count of service providers not configured to collect logs

12.12.5 Metrics

Coverage

Metric	The percentage of service providrs proverly configured to collect logs
Calculation	`M2 / M1`

CHAPTER

THIRTEEN

CIS CONTROL 9: EMAIL AND WEB BROWSER PROTECTIONS

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why is this CIS Control Critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email, or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons.

13.1 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

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

13.1.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

13.1.2 Inputs

1. `GV5`: Authorized software inventory
2. Authoritative source of information indicating supported/unsupported details by product.

13.1.3 Operations

1. Use `GV5` to identify and enumerate web browser and email client software (M1)
2. **Compare each software identified in Operation 1 to Input 2**
    1. Identify and enumerate software labeled as "supported" that is currently supported (M2)
    2. Identify and enumerate software labeled as "supported" that is currently unsupported (M3)
    3. Identify and enumerate software labeled as "unsupported" that is currently unsupported (M4)
    4. Identify and enumerate software labeled as "unsupported" that is currently supported (M5)

13.1.4 Measures

- M1 = Count of authorized web browser and email client software
- M2 = Count of software labeled as "supported" and currently supported
- M3 = Count of software labeled as "supported" and currently unsupported
- M4 = Count of software labeled as "unsupported" and currently unsupported
- M5 = Count of software labeled as "unsupported" and currently supported

13.1.5 Metrics

Percentage of Unsupported Web Browser/Email Client Software in Use

Metric	The percentage of unsupported web browser and email client software in use
Calculation	`(M3 + M4) / M1`

Rate of False Positives

Rate of False Negatives

13.2 9.2: Use DNS Filtering Services

Use DNS filtering services on all enterprise assets to block access to known malicious domains.

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

13.2.1 Dependencies

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

13.2.2 Inputs

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

13.2.3 Operations

1. Use `GV1` to identify and enumerate assets that support DNS filtering (M1)
2. Use `GV5` to identify and enumerate authorized DNS filtering services
3. **For each asset identified in Operation 1 check to see if it is configured properly `GV3` to support authorized DNS filtering services from Operation 2**
    1. Identify and enumerate assets properly configured (M2)
    2. Identify and enumerate assets not properly configured (M3)

13.2.4 Measures

- M1 = Count of enterprise assets capable of supporting DNS filtering
- M2 = Count of assets properly configured to support DNS filtering
- M3 = Count of assets not properly configured to support DNS filtering

13.2.5 Metrics

DNS Filtering Coverage

Metric	The percentage of assets configured to use authorized DNS filtering services
Calculation	`M2 / M1`

13.3 9.3: Maintain and Enforce Network-Based URL Filters

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

13.3.1 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 Processs

13.3.2 Inputs

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

13.3.3 Operations

1. Use `GV1` to identify and enumerate enterprise assets capable of supporting network-based URL filters (M1)
2. Use `GV5` to identify authorized web browsers/clients
3. **For each asset identified in Operation 1 check to see if it is configured properly `GV3` to support authorized web browsers/clients from Operation 2**
    1. Identify and enumerate assets properly configured (M2)
    2. Identify and enumerate assets not properly configured (M3)

13.3.4 Measures

- M1 = Count of enterprise assets capable of supporting network-based URL filters
- M2 = Count of assets properly configured to support network-based URL filters
- M3 = Count of assets not properly configured to support network-based URL filters

13.3.5 Metrics

Coverage

Metric	The percentage of assets configured to use authorized network-based URL filters
Calculation	`M2 / M1`

13.4 9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

13.4.1 Dependencies

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

13.4.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Aurhorized software inventory

13.4.3 Operations

1. Use `GV1` to identify and enumerate assets subject to browser/email plugin restrictions (M1)
2. Use `GV5` to identify authorized browser and email plugins
3. **For each asset listed in Operation 1, collect the list of installed browser plugins and compare to the output of Operation 2**
    1. Identify and enumerate assets with only authorized browser plugins installed or enabled (M2)
    2. Identify and enumerate assets with one or more unauthorized browser plugins installed or enabled (M3)
4. **For each asset listed in Operation 1, collect the list of installed email plugins and compare to the output of Operation 2**
    1. Identify and enumerate assets with only authorized email plugins installed or enabled (M4)
    2. Identify and enumerate assets with one or more unauthorized browser plugins installed or enabled (M5)

13.4.4 Measures

- M1 = Count of assets subject to browser/email plugin restrictions
- M2 = Count of assets with only authorized browser plugins installed or enabled
- M3 = Count of assets with unauthorized browser plugins installed or enabled
- M4 = Count of assets with only authorized email plugins installed or enabled
- M5 = Count of assets with unauthorized email plugins installed or enabled

13.4.5 Metrics

Browser Plugin Enforcement Quality

Metric	The percentage of assets compliant with authorized browser plugins.
Calculation	`M2 / M1`

Email Client Plugin Enforcement Quality

Metric	The percentage of assets compliant with authorized email plugins.
Calculation	`M4 / M1`

13.5 9.5: Implement DMARC

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

13.5.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

13.5.2 Inputs

1. DMARC Policy
2. TXT record published in DNS
3. The Mail Transfer Agent used by the enterprise
4. The Mail User Agent used by the enterprise

13.5.3 Assumptions

1. The DMARC configuration policy includes instructions to produce either Aggregate (rua) or Forensic (ruf) reports.
2. The enterprise has access to these reports either daily (for Aggregate) or in real-time (for Forensic).

13.5.4 Operations

1. **Check if enterprise has a DMARC policy**
    1. If the enterprise has a DMARC policy, M1 = 1
    2. If the enterprise does not have a DMARC policy, M1 = 0
2. **Examine Input 2 for a value indicative of the use of DMARC**
    1. If a value for DMARC is identified, M2 = 1
    2. If a value for DMARC is not identified, M2 = 0
3. **Examine Input 2 for a value indicative of the use of SPF**
    1. If a value for SPF is identified, M3 = 1
    2. If a value for SPF is not identified, M3 = 0
4. **Examine Input 2 for a value indicative of the use of DKIM**
    1. If a value for DKIM is identified, M4 = 1
    2. If a value for DKIM is not identified, M4 = 0
5. **Check if enterprise uses a Mail Transfer Agent**
    1. If the enterprise uses a Mail Transfer Agent, M5 = 1
    2. It the enterprise does not use a Mail Transfer Agent, M5 = 1
6. **Check if enterprise uses a Mail User Agent**
    1. If the enterprise uses a Mail User Agent, M6 = 1
    2. It the enterprise does not use a Mail User Agent, M6 = 1

13.5.5 Measures

- M1 = Output of Operation 1
- M2 = Output of Operation 2
- M3 = Output of Operation 3
- M4 = Output of Operation 4
- M5 = Output of Operation 5
- M6 = Output of Operation 6

13.5.6 Metrics

DMARC Usage

Metric	Usage and configuration of DMARC/SPF/DKIM
Calculation	`(M1 + M2 + M3 + M4 + M5 + M6) / 6`

13.6 9.6: Block Unnecessary File Types

Block unnecessary file types attempting to enter the enterprise?s email gateway.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

13.6.1 Dependencies

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

13.6.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

13.6.3 Operations

1. Use `GV1` to identify and enumerate assets configured as email gateways (M1)
2. **Using `GV3` check the attachment blocking configuration for every asset identified in Operation 1**
    1. Identify and enumerate email gateways properly configured to block unnecessary attachments (M2)
    2. Identify and enumerate email gateways not properly configured to block unnecessary attachments (M3)

13.6.4 Measures

- M1 = Count of email gateways
- M2 = Count of properly configured email gateways
- M3 = Count of improperly configured email gateways

13.6.5 Metrics

Coverage

Metric	The percentage of properly configured email gateways
Calculation	`M2 / M1`

13.7 9.7: Deploy and Maintain Email Server Anti-Malware Protections

Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

13.7.1 Dependencies

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

13.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standard

13.7.3 Operations

1. Use `GV1` to identify and enumerate all email servers within the enterprise (M1)
2. **For each email server identified in Operation 1, use `GV3` to check if native or external anti-malware protections are configured**
    1. Identify and enumerate email servers with configured anti-malware protection (M2)
    2. Identify and enumerate email servers without configured anti-malware protection (M3)

13.7.4 Measures

- M1 = Count of email servers
- M2 = Count of properly configured email servers
- M3 = Count of improperly configured email servers

13.7.5 Metrics

Coverage

Metric	The percentage of properly configured email servers
Calculation	`M2 / M1`

CHAPTER

FOURTEEN

CIS CONTROL 10: MALWARE DEFENSES

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is this CIS Control Critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Malware defenses must be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

14.1 10.1: Deploy and Maintain Anti-Malware Software

Deploy and maintain anti-malware software on all enterprise assets.

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

14.1.1 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

14.1.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized sofware inventory
3. `GV3`: Configuration standards

14.1.3 Operations

1. Use `GV1` to identify and enumerate assets capable of supporting anti-malware software: `GV30` (M1)
2. Use `GV5` to identify authorized anti-malware software: `GV31`
3. **For each asset identified in Operation 1, use the output of Operation 2**
    1. Identify and enumerate assets with at least one authorized anti-malware software intalled: `GV32` (M2)
    2. Identify and enumerate assets with only unauthorized anti-malware software installed (M3)
    3. Identify and enumerate assets without any anti-malware software installed (M4)
4. **For each asset wih a least one authorized anti-malware software installed from Operation 3.1, use `GV3` to check configurations**
    1. Identify and enumerate assets with properly configured anti-malware software (M5)
    2. Identify and enumerate assets with improperly configured anti-malware software (M6)

14.1.4 Measures

- M1 = Count of assets capable of supporting anti-malware software
- M2 = Count of assets with at least one authorized anti-malware software installed
- M3 = Count of assets with only unauthorized anti-malware software installed
- M4 = Count of assets without any anti-malware software installed
- M5 = Count of assets with properly configured authorized anti-malware software installed
- M6 = Count of assets with improperly configured authorized anti-malware software installed

14.1.5 Metrics

Coverage

14.2 10.2: Configure Automatic Anti-Malware Signature Updates

Configure automatic updates for anti-malware signature files on all enterprise assets.

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

14.2.1 Dependencies

- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

14.2.2 Inputs

1. `GV30`: Assets capable of supporting anti-malware software
2. `GV31`: Assets with at least one authorized anti-malware software intalled
3. `GV3`: Configuration standards

14.2.3 Operations

1. **For each asset in Input 2 `GV31`, check configuraions `GV3` to determine if anti-malware software is configured to autmatically update signature files**
    1. Identify and enumerate assets properly configured for automatic updates (M2)
    2. Identify and enumerate asets not properly configured for automatic updates (M3)

14.2.4 Measures

- M1 = Count of `GV30`
- M2 = Count of assets configured to automatically update signature files
- M3 = Count of assets not configured to automatically update signature files

14.2.5 Metrics

Coverage

14.3 10.3: Disable Autorun and Autoplay for Removable Media

Disable autorun and autoplay auto-execute functionality for removable media.

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

14.3.1 Dependencies

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

14.3.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

14.3.3 Operations

1. Use `GV1` to identify and enumerate enterprise assets capable of performing autorun, autoplay, and auto-execute functions (M1)
2. **Check the configurations `GV3` of each asset identified in Operation 1 to see if the autorun, autoplay, and auto-execute functions are disabled**
    1. Identify and enumerate properly configured assets (M2)
    2. Identify and enumerate improperly configured assets (M3)

14.3.4 Measures

- M1 = Count of assets capable of performing autorun, autoplay, and auto-excecute functions
- M2 = Count of assets properly configured to disable functions
- M3 = Count of assets not properly configured to disable functions

14.3.5 Metrics

Compliance

14.4 10.4: Configure Automatic Anti-Malware Scanning of Removable Media

Configure anti-malware software to automatically scan removable media.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

14.4.1 Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

14.4.2 Inputs

1. `GV30`: Assets capable of supporting anti-malware software
2. `GV32`: Assets with at least one authorized anti-malware software intalled
3. `GV3`: Configuration standards

14.4.3 Operations

1. **For each asset in Input 2 `GV32`, use configurations `GV3` to identify if software is configured to automatically scan removable media**
    1. Identify and enumerate assets with properly configured software (M2)
    2. Identify and enumerate assets with improperly configured software (M3)

14.4.4 Measures

- M1 = Count of `GV30`
- M2 = Count of assets with anti-malware properly configured to scan removable media
- M3 = Count of assets with anti-malware not properly configured to scan removable media

14.4.5 Metrics

Coverage

14.5 10.5: Enable Anti-Exploitation Features

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

14.5.1 Dependencies

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

14.5.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standards

14.5.3 Operations

1. **For each asset in `GV1`, use configuration standards `GV3` to determine if it is propely configured to enable anti-exploitation features**
    1. Identify and enumerate assets properly configured to enable anti-exploitation features (M2)
    2. Identify and enumerate assets not properly configured to enable anti-exploitation features (M3)

14.5.4 Measures

- M1 = Count of `GV1`
- M2 = Count of assets properly configured to enable anti-exploitation feautures
- M3 = Count of assets not properly configured to enable anti-exploitation features

14.5.5 Metrics

Coverage

14.6 10.6: Centrally Manage Anti-Malware Software

Centrally manage anti-malware software.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

14.6.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

14.6.2 Inputs

1. `GV30`: Assets capable of supporting anti-malware software
2. `GV31`: Authorized anti-malware software

14.6.3 Operations

1. **For each authorized anti-malware software `GV31`, check if it is centrally managed**
    1. Identify and enumerate anti-malware software that is centrally managed (M2)
    2. Identify and enumerate anti-malware software that is not centrally managed (M3)

14.6.4 Measures

- M1 = Count of `GV31`
- M2 = Count of authorized anti-malware software that is centrally managed
- M3 = Count of authorized anti-malware software that is not centrally managed

14.6.5 Metrics

Coverage

Metric	The percentage of anti-malware centrally managed
Calculation	`M2 / M1`

14.7 10.7: Use Behavior-Based Anti-Malware Software

Use behavior-based anti-malware software.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

14.7.1 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

14.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized sofware inventory
3. `GV3`: Configuration standards

14.7.3 Operations

1. Use `GV1` to identify and enumerate assets capable of supporting behavior-basaed anti-malware software (M1)
2. Use `GV5` to identify authorized behavior-basaed anti-malware software
3. **For each asset identified in Operation 1, use the output of Operation 2**
    1. Identify and enumerate assets with at least one authorized behavior-based anti-malware software intalled (M2)
    2. Identify and enumerate assets without any behavior-based anti-malware software installed (M3)
4. **For each asset wih a least one authorized behavior-based anti-malware software installed from Operation 3.1, use `GV3` to check configurations**
    1. Identify and enumerate assets with properly configured behavior-based anti-malware software (M4)
    2. Identify and enumerate assets with improperly configured behavor-based anti-malware software (M5)

14.7.4 Measures

- M1 = Count of assets capable of supporting behavor-based anti-malware software
- M2 = Count of assets with at least one authorized behavior-based anti-malware software installed
- M3 = Count of assets without any behavior-based anti-malware software installed
- M4 = Count of assets with properly configured authorized behavior-based anti-malware software installed
- M5 = Count of assets with improperly configured authorized behavior-based anti-malware software installed

14.7.5 Metrics

Coverage

CHAPTER

FIFTEEN

CIS CONTROL 11: DATA RECOVERY

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why is this CIS Control Critical?

In the cybersecurity triad – Confidentiality, Integrity, and Availability (CIA) – the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

15.1 11.1: Establish and Maintain a Data Recovery Process

Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

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

15.1.1 Dependencies

- None

15.1.2 Inputs

1. Data recovery process for the enterprise
2. Date of last update to the data recovery process

15.1.3 Operations

1. **Check if enterprise has a data recovery process Input 1**
    1. If so, M1 = 1
    2. If not, M1 = 0
2. **Examine the enterprise's data recovery process and determine if it addresses, at a minimum, the scope of data recovery activities, recovery prioritization, and the security of backup data**
    1. For each element included within the process, assing the element a value of 1. M2 = sum of all the values.
3. Compare the date of last update to the data recovery process to the curren date and capture timeframe in months (M3)

15.1.4 Measures

- M1 = Output of Operation 1
- M2 = Sum of elements included in the data recoery process
- M3 = Timeframe in months of last update to the data recovery process

15.1.5 Metrics

If M1 is 0, the safeguard receives a failing score. The other metrics don't apply. If M3 is greater than twelve, this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of elements included in the data recovery process
Calculation	`M2 / M3`

15.2 11.2: Perform Automated Backups

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

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

15.2.1 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

15.2.2 Inputs

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

15.2.3 Operations

1. For each asset in `GV1` identify and enumerate assets that are in-scope for automated backups: `GV33` (M1)
2. **Use `GV5` to identify authorized backup software and for each asset identified in Operation 1**
    1. Identify and enumerate assets covered by at least one authorized backup software: `GV34` (M2)
    2. Identify and enumerate assets not covered by at least one authorized backup software (M3)
3. **Use `GV3` to check if the software on assets identifed in Operation 2.1 is configured correctly**
    1. Identify and enumerate assets with properly configured backup software (M4)
    2. Identify and enumerate assets with improperly configured backup software (M5)
4. **For each asset with backup software identified in Operation 2.1, examine logs to determine the most recent successful backup date. Compare that date to current date and capture timeframe in days.**
    1. Identify and enumerate assets that have been backeup within seven days or less (M6)
    2. Identify and enumerate assets that have been backedup outside of a sevend day window (M7)

15.2.4 Measures

- M1 = Count of assets within scope for automated backups
- M2 = Count of in-scope assets with authorized backup software installed
- M3 = Count of in-scope assets without authorized backup software installed
- M4 = Count of in-scope assets with properly configured backup software
- M5 = Count of in-scope assets with improperly configured backup software
- M6 = Count of in-scope assets backed up within a week
- M7 = Count of in-scope assets not backed up within a week

15.2.5 Metrics

Coverage

Metric	The percentage of in-scoope assets with properly configured authorized backup software
Calculation	`M4 / M1`

Compliance

Metric	The percentage of in-scope assets backed up within a week timeframe
Calculation	`M6 / M1`

15.3 11.3: Protect Recovery Data

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

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

15.3.1 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

15.3.2 Inputs

1. `GV33`: Assets that are in-scope for automated backups
2. `GV34`: Assets with authorized backup software installed
3. `GV3`: Configuration Standard

15.3.3 Operations

1. **For each asset with backup software installed, use `GV3` to check if encryption is configured for backups**
    1. Identify and enumerate assets with software configured to encrypt backups (M2)
    2. Identify and enumerate assets with software not configured to encrypt backups (M3)

15.3.4 Measures

- M1 = Count of Input 1: `GV33`
- M2 = Count of software configured to encrypt backups
- M3 = Count of software not configured to encrypt backups

15.3.5 Metrics

Coverage

15.4 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

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

15.4.1 Dependencies

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

15.4.2 Inputs

1. `GV33`: Assets that are in-scope for automated backups
2. `GV34`: Assets with authorized backup software installed
3. `GV3`: Configuration standards

15.4.3 Assumptions

1. Configuration for backups will contain information about destination of backups

15.4.4 Operations

1. **For each asset in Input 2 `GV34`, use configuration standards in `GV3` to check destination of backups**
    1. Identify and enumerate assets properly configured to send backups to an isolated instance (M2)
    2. Identify and enumerate assets not properly configured to send backups to an isolated instance (M3)

15.4.5 Measures

- M1 = Count of Input 1 `GV33`
- M2 = Count of assets with backups sent to an isolated instance
- M3 = Count of assets with backups not sent to an isolated instance

15.4.6 Metrics

Coverage

Metric	The percentage of assets configured to send backups to an isolated instance
Calculation	`M2 / M1`

15.5 11.5: Test Data Recovery

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Asset Type	Security Function	Implementation Groups
Data	Recover	2, 3

15.5.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

15.5.2 Inputs

1. Current set of backups for the enterprise
2. Date of last backup recovery test

Assumption

1. Enterprise will know what a properly working restored backup looks like.

15.5.3 Operations

1. **Use Input 1 to restore a sampling of the backups to a temporary location**
    1. Enumerate the total numer of backups restored (M1)
    2. Identify and enumerate backups that are properly working after being restored (M2)
    3. Identify and enumerate backups that did not properly work after being restored (M3)
2. Compare Input 2 to current date and capture time frame in months (M4)

15.5.4 Measures

- M1 = Count of backups being tested
- M2 = Count of properly working backups after restoration
- M3 = Count of backups not properly working after restoration
- M4 = Timeframe between tests of backup recovery

15.5.5 Metrics

If M4 is greater than three months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Backup Integrity Quality

Metric	The percentage of restored backups sampling deemed to be properly working
Calculation	`M2 / M1`

CHAPTER

SIXTEEN

CIS CONTROL 12: NETWORK INFRASTRUCTURE MANAGEMENT

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why is this CIS Control Critical?

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches.

Default configurations for network devices are geared for ease-of-deployment and ease-of-use – not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed, but not removed when they are no longer applicable to the business's needs. In some cases, the security risk of an exception is neither properly analyzed nor measured against the associated business need and can change over time.

16.1 12.1: Ensure Network Infrastructure is Up-to-Date

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

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

16.1.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

16.1.2 Inputs

1. `GV1`: Enterprise asset inventory
2. Authoritative source of latest version information
3. Date of last review of network infrastructure

16.1.3 Operations

1. Use `GV1` to identify and enumerate assets that are part of the network infrastructure `GV35` (M1)
2. **Compare the network infrastructre asset version to the version in Input 2**
    1. Identify and enumerate assets that match the most recent version (M2)
    2. Identify and enumerate assets that don't match the most recent version (M3)
3. Compare Input 3 to current date and capture timeframe in days (M4)

16.1.4 Measures

- M1 = Count of network infrastructure assets
- M2 = Count of network infrastructure assets up to date
- M3 = Count of network infrastructure assets not up to date
- M4 = Timeframe since last review of network infrastrucute

16.1.5 Metrics

If M4 is greater than thirty days, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of network infrastructure assets that are up to date
Calculation	`M2 / M1`

16.2 12.2: Establish and Maintain a Secure Network Architecture

Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

16.2.1 Dependencies

- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)
- Safeguard 2.1: Establish and Maintain a Software Inventory

16.2.2 Inputs

1. `GV4`: Enterprise network architecture documentation
2. `GV5`: Authorized software inventory

16.2.3 Operations

1. Use the network architecture `GV4` to identify and enumerate the segments within the enterprise network `GV36` (M1)
2. **For each network segment identified in Operation 1, attempt to connect an unauthorized device**
    1. Identify and enumerate segments that allow you to connect unauthorized devices (M2)
    2. Identify and enumerate segments that do not allow you to connect unauthorized devices (M3)
3. Use `GV5` to identify authorized availability monitoring software
4. **For eah network segment identified in Operation 1, determine whether an authorized availability monitoring software from Operation 3 covers the segment**
    1. Identify and enumerate segments that are covered by availability monitoring software (M4)
    2. Identify and enumerate segments that are not covered by availability monitoring software (M5)

16.2.4 Measures

- M1 = Count of network segments within the enterprise
- M2 = Count of segments not compliant with least privilege
- M3 = Count of segments compliant with least privilege
- M4 = Count of segments monitored for availability
- M5 = Count of segments not monitored for availability

16.2.5 Metrics

Segmentation

Metric	If M1 is equal to 1, this metric is measured at a 0. Subsequent metrics can still be assessed.
Calculation	`If M1 <= 1, Fail or If M1 >= 1, Pass`

Least Privilege

Metric	The percentage of network segements implementing least privilege
Calculation	`M3 / M1`

Availability

Metric	The percentage of network segments monitored for network availability
Calculation	`M4 / M1`

16.3 12.3: Securely Manage Network Infrastructure

Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

16.3.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

16.3.2 Inputs

1. `GV36`: Segments within the enterprise network
2. `GV35`: Assets that are part of the network infrastructure
3. `GV37`: Network architectrure configuration standards

16.3.3 Operations

1. **For each asset in Input 2 `GV35`, use Input 3 `GV37` to check for the use of encrypted sessions**
    1. Identify and enumerate assets using encrypted sessions (M2)
    2. Identify and enumerate assets not using encrypted sessions (M3)
2. **For each network segment in Input 1 `GV36`, check for the use of infrastructure-as-code**
    1. Identify and enumerate network segments that use infrastructure-as-code for the whole segment or partial (M5)
    2. Identify and enumerate network segments that do not use infrastructure-as-code for any portion of the segment (M6)
3. **For each network segements identified in Operation 1, use Input 3 `GV37` to determine whether the infrastructure-as-code is managed using version control**
    1. Identify and enumerate network segments covered by version controlled infrastructure-as-code (M7)
    2. Identify and enumerate network segments covered by infrastructure-as-code not managed through version control (M8)

16.3.4 Measures

- M1 = Count of `GV35` assets that are part of the network infrastructure
- M2 = Count of network infrastructure assets using encrypted sessions
- M3 = Count of network infrastructure assets not using encrypted sessions
- M4 = Count of `GV36` segments within the enterprise network
- M5 = Count of network segments using infrastructure-as-code
- M6 = Count of network segements not using infrastructure-as-code
- M7 = Count of network segments covered by version controlled infrastructure-as-code
- M8 = Count of network sgements covered by unmanaged infrastructure-as-code

16.3.5 Metrics

Encrypted Session Coverage

Metric	The percentage of network infrastructure assets using encrypted sessions
Calculation	`M2 / M1`

Infrastructure-As-Code Coverage

16.4 12.4: Establish and Maintain Architecture Diagram(s)

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Network	Identify	2, 3

16.4.1 Dependencies

- None

16.4.2 Inputs

1. `GV4`: Enterprise network architecture documentation
2. Date of last review or update to documentation

16.4.3 Operations

1. **Determine if Input 1 `GV4` exists within the enterprise**
    1. If the network architecture documentation exists, M1 = 1
    2. If the network architecture documentation does not exist, M1 = 0
2. Compare Input 2 to the current date. Capture the timeframe in months.

16.4.4 Measures

- M1 = Output of Operation 1.
- M2 = Timeframe in months of last review or update to documentation

16.4.5 Metrics

If M1 is not provided or available, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply. If M2 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

16.5 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

Centralize network AAA.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

16.5.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

16.5.2 Inputs

1. `GV5`: Authorized Software Inventory
2. `GV35`: Assets that are part of the network infrastructure

16.5.3 Operations

1. Use Input 1 `GV5` to identify and enumerate all AAA services within the enterprise `GV38` (M1)
2. **For each centralized AAA point indentifed in Operation 1, determine whether it is necessary or can be consolidated**
    1. Identify and enumerate authentication points that are unnecesary or can be consolidated (M2)
    2. Identify and enumerate authentication points that are necesary and cannot be consolidated (M3)
3. **Use the output of Operation 1 to check if each asset in Input 2 `GV35` is covered by at least one AAA system**
    1. Identify and enumerate network infrastructure assets that are covered by at least one AAA system (M4)
    2. Identify and enumerate network infrastructure assets that are not covered by an AAA system (M5)

16.5.4 Measures

- M1 = Count of AAA services within the enterprise
- M2 = Count of unnecessary AAA services
- M3 = Count of necessary AAA services
- M4 = Count of network infrastructure covered by AAA services
- M5 = Count of network infrastructure not covered by AAA services
- M6 = Count of `GV35`

16.5.5 Metrics

Centralized AAA

Metric	Percentage of properly centralized AAA services
Calculation	`M3 / M1`

Network Coverage

Metric	Percentage of network infrastructure assets managed through AAA
Calculation	`M4 / M6`

16.6 12.6: Use of Secure Network Management and Communication Protocols

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

16.6.1 Dependencies

- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.2: Establish and Maintain a Secure Network Architecture

16.6.2 Inputs

1. `GV36`: Segments within the enterprise network
2. `GV37`: Network infrastructure configuration standards
3. Authorized list of secure network management and communication protocols

16.6.3 Operations

1. **For each network segment in Input 1 `GV36`, use Input 3 to identify communication protocols**
    1. Identify and enumerate segments using only communication protocols on the authorized list (M2)
    2. Identify and enumerate segments using communication protocols not on the authorized list (M3)
2. **For each communication protocol identified in Operation 1.1, check configuration standards `GV37`**
    1. Identify and enumerate segments using properly configured communication protocols (M4)
    2. Identify and enumerate segments using improperly configured communication protocols (M5)
3. **For each network segment in Input 1 `GV36`, use Input 3 to identify network management protocols**
    1. Identify and enumerate segments using only network management protocols on the authorized list (M6)
    2. Identify and enumerate segments using network management protocols not on the authorized list (M7)
4. **For each communication protocol identified in Operation 1.1, check configuration standards `GV37`**
    1. Identify and enumerate segments using properly configured network management protocols (M8)
    2. Identify and enumerate segments using improperly configured network management protocols (M9)

16.6.4 Measures

- M1 = Count of `GV36`
- M2 = Count of segments using authorized communication protocols
- M3 = Count of segments using unauthorized communication protocols
- M4 = Count of segments using properly configured authorized communication protocols
- M5 = Count of segments using improperly configured authorized communication protocols
- M6 = Count of segments using unauthorized network management protocols
- M7 = Count of segments using unauthorized network management protocols
- M8 = Count of segments using properly configured authorized network management protocols
- M9 = Count of segments using improperly configured authorized network management protocols

16.6.5 Metrics

Communication Protocol Coverage

Network Managememt Protocol Coverage

16.7 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

16.7.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

16.7.2 Inputs

1. `GV1`: Enterprise Asset Inventory
2. `GV5`: Authorized Software Inventory
3. `GV38`: AAA services within the enterprise
4. `GV37`: Network infrastructure configuration standards

16.7.3 Operations

1. Use Input 1 `GV1` to identify and enumerate remote enterprise assets `GV39` (M1)
2. Use Input 1 `GV1` and Input 2 `GV5` to identify and enumerate all VPN devices and software (M2)
3. **Use the output of Operation 2 and Input 4 :code:`GV37`to check configuration of VPN**
    1. Identify and enumerate VPN devices and software properly configured to require authentication prior to granting access (M3)
    2. Identify and enumerate VPN devices and software not properly configured to require authentication prior to granting access (M4)
4. **For each asset identified in Operation 1, check if is covered by a VPN device or software identified in Operation 3.1**
    1. Identify and enumerate assets that are covered by a VPN (M5)
    2. Identify and enumerate assets that are not covered by a VPN (M6)
5. **Use Input 3 `GV38` and Input 4 `GV37` to check configuration of AAA services**

1. Identify and enumerate AAA services properly configured to require authentication prior to granting access (M7)
2. Identify and enumerate AAA services not properly configured to require authentication prior to granting access (M8)

6. **For each asset indentified in Operation 1, check if it is covered an AAA service identified in Operation 5.1**
    1. Identify and enumerate assets that are covered by an AAA service (M9)
    2. Identify and enumerate assets that are not covered by an AAA service (M10)
7. **Compare the output of Operation 4.1 and 6.1**
    1. Identify and enumerate assets covered by both VPN and AAA (M1)

16.7.4 Measures

- M1 = Count of remote enterprise assets
- M2 = Count of VPN devices and software
- M3 = Count of properly configured VPN devices and sofware
- M4 = Count of improperly configured VPN devices and software
- M5 = Count of remote assets covered by a properly configured VPN
- M6 = Count of remote assets not covered by a properly configured VPN
- M7 = Count of properly configured AAA services
- M8 = Count of improperly configured AAA services
- M9 = Count of remote assets covered by a properly configured AAA service
- M10 = Count of remote assets not covered by a properly configured AAA service
- M11 = Count of remote assets covered by both VPN and AAA
- M12 = Count of AAA services within the enterprise

16.7.5 Metrics

VPN Compliance

Metric	The percentage of properly configured VPN devices and software
Calculation	`M3 / M2`

AAA Compliance

Metric	The percentage of properly configured AAA services
Calculation	`M7 / M12`

Coverage

Metric	The percentage of remote assets using VPN and AAA
Calculation	`M11 / M1`

16.8 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

16.8.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

16.8.2 Inputs

1. `GV1`: Enterprise Asset Inventory
2. `GV37`: Network infrastructure configuration standards

16.8.3 Operations

1. Use Input 1 `GV1` to identify and enumerate assets used for administrative purposes (M1)
2. **For each asset identified in Operation 1, use Input 2 `GV37` to check configurations**
    1. Identify and enumerate assets that do not have internet access (M2)
    2. Identify and enumerate assets that have internet access (M3)
    3. Identify and enumerate assets that are physically or logically seperated from the primary network (M4)

4. Identify and enumerate assets that are not physically or logically seperated from the primary network (M5)

3. **Compare the ouput of Operation 2.1 and 2.3**

    1. Identify and enumerate assets that do not have internet access and are physically or logically seperated (M6)

16.8.4 Measures

- M1 = Count of assets used for administrative purposes
- M2 = Count of assets configured to not allow internet access
- M3 = Count of assets configured to allow internet access
- M4 = Count of assets physically or logically seperated from the primary network
- M5 = Count of assets not physically or logically seperated from the primary network
- M6 = Count of assets configured to not allow internet acces and are physically or logically seperated

16.8.5 Metrics

Compliance

Metric	The percentage of properlu configured administrative assets
Calculation	`M6 / M1`

CHAPTER

SEVENTEEN

CIS CONTROL 13: NETWORK MONITORING AND DEFENSE

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Why is this CIS Control Critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies, and support regulatory compliance for many enterprises.

As we have seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. This is critical to respond quickly when malware is discovered, credentials are stolen, or when sensitive data is compromised to reduce impact to the enterprise.

Through good situational awareness (i.e., security operations), enterprises will identify and catalog Tactics, Techniques, and Procedures (TTPs) of attackers, including their IOCs that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

17.1 13.1: Centralize Security Event Alerting

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

17.1.1 Dependencies

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

17.1.2 Inputs

1. Location of `GV42`: log correlation or log analytic tool
2. `GV1`: Enterprise asset inventory

17.1.3 Operations

1. **Check if Input 1 exists within the enterprise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. Use `GV1` to identify and enumerate enterprise assets that produce security event logs (M2)
3. **For every asset identified in Operation 2, check if logs are centralized at the location of the log correlation or log analytic tool Input 1**
    1. Identify and enumerate assets whose logs are centralized (M3)
    2. Identify and enumerate assets whose logs are not centralized (M4)

17.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of assets that produce security event logs
- M3 = Count of assets with security event logs being centralized
- M4 = Count of assets with security event logs not being centralized

17.1.5 Metrics

If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of asses whose security even logs are centralized
Calculation	`M3 / M2`

17.2 13.2: Deploy a Host-Based Intrusion Detection Solution

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

17.2.1 Dependencies

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

17.2.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

17.2.3 Operations

1. Use `GV1` to identify and enumerate assets capable of supporting host based intrusion detection systems (M1)
2. Use: code:*GV5* to identify authorized host based intrusion detection software
3. **For each asset identified in Operation 1 check if it is covered by at least one authorized host based intrusion detection software**
    1. Identify and enumerate assets with host based intrusion detection software installed (M2)
    2. Identify and enumerate assets without host based intrusion detection software installed (M3)

17.2.4 Measures

- M1 = Count of enterprise assets capable of supporting host based intrusion detection systems
- M2 = Count of assets with host based intrusion detection systems
- M3 = Count of assets without host based intrusion detection systems

17.2.5 Metrics

Coverage

17.3 13.3: Deploy a Network Intrusion Detection Solution

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

17.3.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

17.3.2 Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV4`: Enterprise Network Architecture Documentation

17.3.3 Operations

1. Use Input 1 `GV35` to identify the network intrusion detection solutions for the enterprise
2. Use Input 2 `GV4` to identify and enumerate network boundaries (M1)
3. **For each network boundary identified in Operation 2, determine whether it is covered by at least one network intrusion detection solution**
    1. Identify and enumerate boundaries covered by at least one network intrusion detection solution (M2)
    2. Identify and enumerate boundaries not covered by at least one network intrusion detection solution (M3)

17.3.4 Measures

- M1 = Count of network boundaries
- M2 = Count of network boundaries covered by a network intrusion detection solution
- M3 = Count of network boundaries not covered by a network intrusion detection solution

17.3.5 Metrics

Coverage

17.4 13.4: Perform Traffic Filtering Between Network Segments

Perform traffic filtering between network segments, where appropriate.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

17.4.1 Dependencies

- None

17.4.2 Inputs

1. `GV36`: Segments within the enterprise network
2. `GV35`: Assets that are part of the network infrastructure
3. `GV37`: Network infrastructure configuration standards

17.4.3 Operations

1. Use Input 1 `GV36` to identify and enumerate network segments that require communication with other network segments (M1)
2. For each network segment identified in Operation 1, use Input 2 `GV35` to identify network infrastructure assets responsible for traffic filtering
3. **For each network infrastructure asset identified in Operation 1, check configurations using Input 3 `GV37` to determine whether each semgment is properly configured to filter traffic**
    1. Identify and enumerate network segments with properly configured filtering assets (M2)
    2. Identify and enumerate network segments with improperly configured filtering assets (M3)

17.4.4 Measures

- M1 = Count of network segments that communicate with other network segments
- M2 = Count of network segments with properly configured filtering assets
- M3 = Count of network segments wih improperly configured filtering assets

17.4.5 Metrics

Coverage

Metric	The percentage of network segments properly configured to filter traffic between segments
Calculation	`M2 / M1`

17.5 13.5: Manage Access Control for Remote Assets

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

17.5.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

17.5.2 Inputs

1. `GV23`: Authentication and Authorization System Inventory
2. `GV3`: Configuration Standard
3. `GV39`: Remote enterprise assets

17.5.3 Operations

1. Use Input 1 `GV23` to identify and enumerate authorization systems that allow remote logins (M1)
2. **For each authorization system identified in Operation 1, use Input 2 :code`GV3` to check if configuration for each type of policy**
    1. Identify and enumerate authorization systems properly configured for all the policies (M2)
    2. Identify and enumerate authorization systems for which at least one configuration does not comply with the policies (M3)
3. **For each remote enterprise asset from Input 3 `GV39`, compare to the output of Operation 2.1**
    1. Identify and enumerate assets that are covered by at least one compliant authorization system (M4)
    2. Identify and enumerate assets that are not covered by a compliant authorization system (M5)

17.5.4 Measures

- M1 = Count of authorization systems that allow remote logins
- M2 = Count of authorization systems properly configured to comply with policies
- M3 = Count of authorization systems not properly configured to comply with policies
- M4 = Count of remote enterprise assets covered by a compliant authorization system
- M5 = Count of remote enterprise assets not covered by a compliant authorization system
- M6 = Count of remote enterprise assets `GV39`

17.5.5 Metrics

Authorization System Compliance

Metric	The percentage of properly configured authorizations systems that allow remote login
Calculation	`M2 / M1`

Coverage

17.6 13.6: Collect Network Traffic Flow Logs

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Asset Type	Security Function	Implementation Groups
Network	Detect	2, 3

17.6.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

17.6.2 Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV37`: Network infrastructure configuration standards

17.6.3 Operations

1. Use Input 1 `GV35` to identify and enumerate network boundary assets (M1)
2. **For each network boundary asset identified in Operation 1, check configurations `GV37` to determine if network traffic or network traffic flow loggins is enabled**
    1. Identify and enumerate assets with either network traffic flow or network traffic logging enabled (M2)
    2. Identify and enumerate assets that have neither network traffic flow or network traffic logging enabled (M3)

17.6.4 Measures

- M1 = Count of network boundary assets
- M2 = Count of properly configured network boundary assets
- M3 = Count of improperly configured network boundary assets

17.6.5 Metrics

Coverage

Metric	The percentage of network boundary assets properly configured to log network traffic flow or network traffic
Calculation	`M2 / M1`

17.7 13.7: Deploy a Host-Based Intrusion Prevention Solution

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

17.7.1 Dependencies

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

17.7.2 Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory

17.7.3 Operations

1. Use `GV1` to identify and enumerate assets capable of supporting host based intrusion prevention systems (M1)
2. Use: code:*GV5* to identify authorized host based intrusion prevention software
3. **For each asset identified in Operation 1 check if it is covered by at least one authorized host based intrusion prevention software**
    1. Identify and enumerate assets with host based intrusion prevention software installed (M2)
    2. Identify and enumerate assets without host based intrusion prevention software installed (M3)

17.7.4 Measures

- M1 = Count of enterprise assets capable of supporting host based intrusion prevention systems
- M2 = Count of assets with host based intrusion prevention systems
- M3 = Count of assets without host based intrusion prevention systems

17.7.5 Metrics

Coverage

17.8 13.8: Deploy a Network Intrusion Prevention Solutions

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

17.8.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

17.8.2 Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV40`: Network Boundaries

17.8.3 Operations

1. Use Input 1 `GV35` to identify the network intrusion prevention solutions for the enterprise
2. **For each network boundary identified in Input 2, determine whether it is covered by at least one network intrusion prevention solution**
    1. Identify and enumerate boundaries covered by at least one network intrusion prevention solution (M2)
    2. Identify and enumerate boundaries not covered by at least one network intrusion prevention solution (M3)

17.8.4 Measures

- M1 = Count of network boundaries `GV40`
- M2 = Count of network boundaries covered by a network intrusion prevention solution
- M3 = Count of network boundaries not covered by a network intrusion prevention solution

17.8.5 Metrics

Coverage

17.9 13.9: Deploy Port-Level Access Control

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Asset Type	Security Function	Implementation Groups
Devices	Protect	3

17.9.1 Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

17.9.2 Inputs

1. `GV5`: Authorized Software Inventory
2. `GV38`: AAA services within the enterprise
3. `GV41`: List of CMDB servers
4. `GV35`: Assets that are part of the network infrastructure
5. `GV37`: Network infrastructure configuration standards

17.9.3 Operations

If the enterprise uses an 802.1x network design to control network access:

1. Use Input 1 GV5 to identify and enumerate 802.1x authenticators (M1)
2. **For each authenticator identified in Operation 1, use Input 5 :code:`GV37`to check configurations**
    1. Identify and enumerate properly configured authenticators (M2)
    2. Identify and enumerate improperly configured authenticators (M3)
3. Use Input 2 GV38 to identify 802.1x authentication servers (M4)
4. **For each authentication server identified in Operation 3, use Input 5 GV37`to check configurations to ensure a connection to at least one CMDB server from Input 3 :code:`GV41**
    1. Identify and enumerate properly configured authentication servers (M5)
    2. Identify and enumerate improperly configured authentication servers (M6)

If the enterprise does not use 802.1x network design to control network access:

1. **For each asset in Input 4 GV35, use Inp;ut 5 GV37 to check client authentication certificate configuration**
    1. Identify and enumerate properly configured assets (M8)
    2. Identify and enumerate improperly configured assets (M9)

17.9.4 Measures

- M1 = Count of 802.1x authenticators
- M2 = Count of 802.1x properly configured authenticators
- M3 = Count of 802.1x improperly configured authenticators
- M4 = Count of 802.1x authentication servers
- M5 = Count of 802.1x properly configured authentication servers
- M6 = Count of 802.1x improperly configured authentication servers
- M7 = Count of Input 4 GV35
- M8 = Count of assets properly configured for client authentication certificates
- M9 = Count of assets improperly configured for client authentication certificates

17.9.5 Metrics

If the enterprise uses an 802.1x network design to control network access:

Authenticator Coverage

Metric	The percentage of properly configured authenticator
Calculation	`M2 / M1`

Authentication Server Coverage

Metric	The percentage of properly configured authentication servers
Calculation	`M5 / M4`

If the enterprise does not use 802.1x network design to control network access:

Client Authentication Certificate Coverage

17.10 13.10: Perform Application Layer Filtering

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

17.10.1 Dependencies

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

17.10.2 Inputs

1. `GV35`: Assets that are part of the network infrastructure
2. `GV5`: Authorized Software Inventory

17.10.3 Operations

1. Use Input 2 `GV5` to identify software used for application layer filtering
2. **For each asset in Input 1 :code:`GV35, determine whether it is covered by at least one sofware identified in Operation 1**
    1. Identify and enumerate assets covered by application layer filtering software (M2)
    2. Identify and enumerate assets not covered by application layer filtering software (M3)

17.10.4 Measures

- M1 = Count of network infrastructure assets
- M2 = Count of network infrastructure assets covered by application layer filtering software
- M3 = Count of network infrastructure assets not covered by application layer filtering software

17.10.5 Metrics

Coverage

Metric	The percentage of network infrastructure assets covered by application layering software
Calculation	`M2 / M1`

17.11 13.11: Tune Security Event Alerting Thresholds

Tune security event alerting thresholds monthly, or more frequently.

Asset Type	Security Function	Implementation Groups
Network	Detect	3

17.11.1 Dependencies

- Safeguard 13.1: Centralize Security Event Alerting

17.11.2 Inputs

1. Date of last tuning of security event alert thresholds of `GV42` Log correlation or log analytic tool

17.11.3 Operations

1. Compare Input 1 to current date and capture timeframe in days

17.11.4 Measures

- M1 = Timeframe in days since last tuning of security event alert thresholds for log correlation or log analytic tool

17.11.5 Metrics

If M1 is greater than thirty days, then this safeguard is measured at a 0 and receives a failing score.

CHAPTER

EIGHTEEN

CIS CONTROL 14: SECURITY AWARENESS AND SKILLS TRAINING

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why is this CIS Control Critical?

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly.

Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites.

No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. Users at every level of the enterprise have different risks. For example: executives manage more sensitive data; system administrators have the ability to control access to systems and applications; and users in finance, human resources, and contracts all have access to different types of sensitive data that can make them targets.

The training should be updated regularly. This will increase the culture of security and discourage risky workarounds.

18.1 14.1: Establish and Maintain a Security Awareness Program

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.1.1 Dependencies

- None

18.1.2 Inputs

1. Security awareness program
2. `GV43`: List of workforce members
3. List of most recent security awareness training completion dates for each workforce member
4. Date of last review or update to security awareness program content

18.1.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. Compare the date in Input 4 to the current date and capture timeframe in months (M2)
3. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M4)
    2. Identify and enumerate members who have not completed any training (M5)
4. For every member of the workforce identified in Operation 3.1, identify the date of most recently completed security awareness training
5. **For every member of the workforce identified in Operation 3.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M6)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M7)

18.1.4 Measures

- M1 = Output of Operation 1
- M2 = Output of Operation 2
- M3 = Count of Input 2 `GV43`
- M4 = Count of workforce members that have completed training
- M5 = Count of workforce members that have not completed training
- M6 = Count of workforce members whose training is up to date
- M7 = Count of workforce members whose training is not up to date

18.1.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M4 / M3`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M6 / M3`

18.2 14.2: Train Workforce Members to Recognize Social Engineering Attacks

Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.2.1 Dependencies

- None

18.2.2 Inputs

1. Recognizing Social Engineering Attacks training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.2.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.2.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.2.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.3 14.3: Train Workforce Members on Authentication Best Practices

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.3.1 Dependencies

- None

18.3.2 Inputs

1. Authentication Best Practices training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.3.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)

2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.3.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.3.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.4 14.4: Train Workforce on Data Handling Best Practices

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.4.1 Dependencies

- None

18.4.2 Inputs

1. Data Handling Best Practices training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.4.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.4.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.4.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.5 14.5: Train Workforce Members on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.5.1 Dependencies

- None

18.5.2 Inputs

1. Causes of Unintentional Data Exposure training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.5.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.5.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.5.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.6 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

Train workforce members to be able to recognize a potential incident and be able to report such an incident.

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

18.6.1 Dependencies

- None

18.6.2 Inputs

1. Recognizing and Reporting Security Incidents training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.6.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.6.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.6.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.7 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.7.1 Dependencies

- None

18.7.2 Inputs

1. How to Identify and Report if Their Enterprise Assets are Missing Security Updates training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.7.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.7.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.7.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.8 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.8.1 Dependencies

- None

18.8.2 Inputs

1. Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.8.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.8.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.8.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

18.9 14.9: Conduct Role-Specific Security Awareness and Skills Training

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

Asset Type	Security Function	Implementation Groups
N/A	Protect	1, 2, 3

18.9.1 Dependencies

- None

18.9.2 Inputs

1. Role-Specific Security Awareness and Skills Training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

18.9.3 Operations

1. **Check enterprise to determine if Input 1 exists**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training**
    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)
3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training
4. **For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to current date. Capture timeframe in months.**
    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from current date (M5)

2. Identify and enumerate members whose most recent training date is greater than twelve months from current date (M6)

18.9.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1 `GV43`
- M3 = Count of workforce members that have completed training
- M4 = Count of workforce members that have not completed training
- M5 = Count of workforce members whose training is up to date
- M6 = Count of workforce members whose training is not up to date

18.9.5 Metrics

- If M1 is measured at a 0, this safeguard receives a failing score. The other metrics don't apply.

Initial Training Compliance

Metric	The percentage of workforce members that have received initial training
Calculation	`M2 / M1`

Up to Date Training

Metric	The percentage of compliant workforce members
Calculation	`M4 / M1`

CHAPTER

NINETEEN

CIS CONTROL 15: SERVICE PROVIDER MANAGEMENT

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why is this CIS Control Critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions.

There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Most data security and privacy regulations require their protection extend to third-party service providers, such as with Health Insurance Portability and Accountability Act (HIPAA) Business Associate agreements in healthcare, Federal Financial Institutions Examination Council (FFIEC) requirements for the financial industry, and the United Kingdom (U.K.) Cyber Essentials. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise.

While reviewing the security of third-parties has been a task performed for decades, there is not a universal standard for assessing security; and, many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. This is because every enterprise has a different "checklist" or set of standards to grade the service provider. There are only a few industry standards, such as in finance, with the Shared Assessments program, or in higher education, with their Higher Education Community Vendor Assessment Toolkit (HECVAT). Insurance companies selling cybersecurity policies also have their own measurements.

While an enterprise might put a lot of scrutiny into large cloud or application hosting companies because they are hosting their email or critical business applications, smaller firms are often a greater risk. Often times, a third-party service provider contracts with additional parties to provide other plugins or services, such as when a third-party uses a fourth-party platform or product to support the main enterprise.

19.1 15.1: Establish and Maintain an Inventory of Service Providers

Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Identify	1, 2, 3

19.1.1 Dependencies

- None

19.1.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV46`: Date of last review or update of the service provider inventory

19.1.3 Operations

1. **Determine whether the enterprise maintains a service provider inventory list by checking for Input 1,**
    1. If Input 1 exists, M1 = 1
    2. If Input 2 does not exist, M1 = 0
2. **Review Input 1 and determine if it includes, at a minimum, the following components: service provider, classification of provider, and an enterprise contact for the provider**
    1. For each component included, assign a value of 1. Sum all values. (M2)
3. **For each service provider indentied in Input 1 `GV45`, determine whether they are accurately listed**
    1. Identify and enumerate providers that are accurately listed (M4)
    2. Identify and enumerate providers that are erroneously listed (M5)
    3. Identify and enumerate providers that should be listed but are missing (M6)
4. Compare the date from Input 2 with the current date and capture the time frame in months (M7)

19.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the inventory
- M3 = Count of service providers in the inventory
- M4 = Count of accurately listed providers
- M5 = Count of erroneously listed providers
- M6 = Count of missing providers from list
- M7 = Timeframe since last update or review of the inventory

19.1.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.
- If M7 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

Metric	The percentage of components included in the inventory
Calculation	`M2 / 3`

Accuracy of Inventory

Metric	The perecentage of accurately listed service providers in the inventory
Calculation	`M4 / (M3 - M5 + M6)`

19.2 15.2: Establish and Maintain a Service Provider Management Policy

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Identify	2, 3

19.2.1 Dependencies

- None

19.2.2 Inputs

1. `GV45`: Service Provider Management Policy
2. Date of last review or update of the policy

19.2.3 Operations

1. **Determine whether the enterprise maintains a service provider management policy by checking for Input 1,**
    1. If Input 1 exists, M1 = 1
    2. If Input 2 does not exist, M1 = 0
2. **Review Input 1 and determine if it includes, at a minimum, the following components: service provider inventory, classification, assessment, monitoring, and decommissioning of service providers**
    1. For each component included, assign a value of 1. Sum all values. (M2)
3. Compare the date from Input 2 with the current date and capture the time frame in months (M3)

19.2.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the policy
- M3 = Timeframe since last update or review of the policy

19.2.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Policy

Metric	The percentage of components included in the policy
Calculation	`M2 / 5`

19.3 15.3: Classify Service Providers

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Identify	2, 3

19.3.1 Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

19.3.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy
3. `GV46`: Date of last review or update to service provider inventory

19.3.3 Operations

1. **Use Input 2 `GV45` to determine if the enterprise policy includes classification process of service providers by one or more characteristics**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Compare date of Input 3 `GV46` to current date and capture timeframe in months (M2)
3. **Review Input 1 `GV45` and determine whether service providers are classified using one or more characteristic per the enterprise's policy**
    1. Identify and enumerate service providers with an assigned classification (M4)
    2. Identify and enumerate service providers without a classification (M5)

19.3.4 Measures

- M1 = Output of Operation 1
- M2 = Timeframe since last update or review of service provider inventory
- M3 = Count of service providers in inventory
- M4 = Count of service providers with classification
- M5 = Count of service providers without classification

19.3.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Coverage

Metric	The percentage of service providers with a classification
Calculation	`M4 / M3`

19.4 15.4: Ensure Service Provider Contracts Include Security Requirements

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Asset Type	Security Function	Implementation Groups
N/A	Protect	2, 3

19.4.1 Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

19.4.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy
3. Date of last update or review of contracts

19.4.3 Operations

1. **Use Input 2 `GV45` to determine if the enterprise policy includes security program requirements for service providers**
    1. If the security requirements exist, M1 = 1
    2. If the security requirements do not exist, M1 = 0
2. **Use Input 1 `GV44` to determine if each listed service provider has a contract**
    1. Identify and enumerate service providers with contracts (M3)
    2. Identify and enumerate service providers without contracts (M4)
3. **For each service provider with a contract identified in Operation 2.1, compare the date from input 3 to current date and capture timeframe in months**
    1. Identify and enumerate service providers whose contract has been reviewed within twelve months or less (M5)
    2. Identify and enumerate service providers whose contract has been reviewed outside the twelve month window (M6)

19.4.4 Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with contracts
- M4 = Count of service providers without contracts
- M5 = Count of service providers with up to date contracts
- M6 = Count of service providers without out dated contracts

19.4.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of service providers with up to date contract
Calculation	`M5 / M2`

19.5 15.5: Assess Service Providers

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Asset Type	Security Function	Implementation Groups
N/A	Identify	3

19.5.1 Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

19.5.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy

19.5.3 Operations

1. **Use Input 2 `GV45` to determine if the enterprise policy includes monitoring guidance for service providers**
    1. If the assessment scope exist, M1 = 1
    2. If the assessment scope does not exist, M1 = 0
2. **Use Input 1 `GV44` to determine if each listed service provider has monitoring guidance included in the policy**
    1. Identify and enumerate service providers with monitoring guidance (M3)
    2. Identify and enumerate service providers without monitoring guidance (M4)

19.5.4 Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with monitoring guidance
- M4 = Count of service providers without monitoring guidance

19.5.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

19.6 15.6: Monitor Service Providers

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Asset Type	Security Function	Implementation Groups
Data	Detect	3

19.6.1 Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

19.6.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy

19.6.3 Operations

1. **Use Input 2 `GV45` to determine if the enterprise policy includes monitoring guidance for service providers**
    1. If the monitoring guidance exist, M1 = 1
    2. If the monitoring guidance does not exist, M1 = 0
2. **Use Input 1 `GV44` to determine if each listed service provider has monitoring guidance provided in the policy**
    1. Identify and enumerate service providers with monitoring guidance provided (M3)
    2. Identify and enumerate service providers without monitoring guidance provided (M4)

19.6.4 Measures

- M1 = Output of Operation 1
- M2 = Count of service providers in inventory
- M3 = Count of service providers with monitoring guidance provided
- M4 = Count of service providers without monitoring guidance provided

19.6.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of service providers with up to date assessments
Calculation	`M3 / M2`

19.7 15.7: Securely Decommission Service Providers

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems

Asset Type	Security Function	Implementation Groups
Data	Protect	3

19.7.1 Dependencies

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
- Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

19.7.2 Inputs

1. `GV44`: Service Provider Inventory List
2. `GV45`: Service Provider Management Policy

19.7.3 Operations

1. **Use Input 2 `GV45` to determine if the enterprise policy includes guidance for securely decommissioning service providers**
    1. If the monitoring guidance exist, M1 = 1
    2. If the monitoring guidance does not exist, M1 = 0
2. Use Input 1 `GV44` to identify and enumerate any service providers terminated over the last twelve months (M2)
3. **For each service provider identified in Operation 2, determine if the provider was decommissioned per the policy**
    1. Identify and enumerate service providers properly terminated (M3)
    2. Identify and enumerate service providers improperly terminated (M4)

19.7.4 Measures

- M1 = Output of Operation 1
- M2 = Count of service providers terminated over the last twelve months
- M3 = Count of service providers properly terminated
- M4 = Count of service providers improperly terminated

19.7.5 Metrics

- If M1 is a 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of service providers properly terminated
Calculation	`M3 / M2`

CHAPTER

TWENTY

CIS CONTROL 16: APPLICATION SOFTWARE SECURITY

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why is this CIS Control Critical?

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimize the need for users to deal directly with complex (and potentially error-prone) system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors. This is why protecting user credentials (specifically application credentials) defined in CIS Control 6 is so important. Lacking credentials, application flaws are the attack vector of choice. However, today's applications are developed, operated, and maintained in a highly complex, diverse, and dynamic environment. Applications run on multiple platforms: web, mobile, cloud, etc., with application architectures that are more complex than legacy client-server or database-web server structures. Development life cycles have become shorter, transitioning from months or years in long waterfall methodologies, to DevOps cycles with frequent code updates. Also, applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, existing code, and new code. There are also modern and evolving data protection regulations dealing with user privacy. These may require compliance to regional or sector-specific data protection requirements. These factors make traditional approaches to security, like control (of processes, code sources, run-time environment, etc.), inspection, and testing, much more challenging. Also, the risk that an application vulnerability introduces might not be understood, except in a specific operational setting or context. Application vulnerabilities can be present for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Attackers can exploit specific vulnerabilities, including buffer overflows, exposure to Structured Query Language (SQL) injection, cross-site scripting, cross-site request forgery, and click-jacking of code to gain access to sensitive data, or take control over vulnerable assets within the infrastructure as a launching point for further attacks. Applications and websites can also be used to harvest credentials, data, or attempt to install malware onto the users who access them. Finally, it is now more common to acquire Software as a Service (SaaS) platforms, where software is developed and managed entirely through a third-party. These might be hosted anywhere in the world. This brings challenges to enterprises that need to know what risks they are accepting with using these platforms; and, they often do not have visibility into the development and application security practices of these platforms. Some of these SaaS platforms allow for customizing of their interfaces and databases. Enterprises that extend these applications should follow this CIS Control, similar to if they were doing ground-up customer development.

20.1 16.1: Establish and Maintain a Secure Application Development Process

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.1.1 Dependencies

- None

20.1.2 Inputs

1. `GV49`: Secure Application Development Process
2. Date of last update or review of the secure application development process

20.1.3 Operations

1. **Determine whether Input 1 exists within the enterprise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 1
2. **Review Input 1 and dermine whether it includes, at a minimum, the following components: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures**
    1. For each component included in the process, assign a value of 1. Sum all values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

20.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the process
- M3 = Timeframe in months since last review or update

20.1.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

20.2 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.2.1 Dependencies

- None

20.2.2 Inputs

1. `GV48`: Process to Accept and Address Software Vulnerabilities
2. Date of last update or review of process

20.2.3 Operations

1. **Determine whether Input 1 exists within the enterprise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 1
2. **Review Input 1 `GV48` and dermine whether it includes, at a minimum, the following components: reporting process, responsible party for handling vulnerability reports, a process for intake, assignment, remediation, remediation testing, and a vulnerability tracking system**
    1. For each component included in the process, assign a value of 1. Sum all values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

20.2.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the process
- M3 = Timeframe in months since last review or update

20.2.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

20.3 16.3: Perform Root Cause Analysis on Security Vulnerabilities

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.3.1 Dependencies

- Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

20.3.2 Inputs

1. Root Cause Analysis Process
2. Vulnerabilities addressed over the last twelve months

20.3.3 Operations

1. **Determine whether Input 1 exists within the enterprise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 1
2. **Review Input 1 and dermine whether it includes, at a minimum, the following components: categorization of vulnerabilities, guidance for how lessons learned are incorporated into the development process**
    1. For each component included in the process, assign a value of 1. Sum all values. (M2)
3. **For each vulnerability addressed over the last twelve months, assess whether the root cause analysis process was followed**

1. Identify and enumerate vulnerabilities for which the process was followed (M4)
2. Identify and enumerate vulnerabilities for which the process was not followed (M5)

20.3.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the process
- M3 = Count of Input 2
- M4 = Count of vulnerabilities for which root cause analysis was conducted
- M5 = Count of vulnerabilities for which root cause analysis was not conducted

20.3.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Completeness of Process

Compliance

20.4 16.4: Establish and Manage an Inventory of Third-Party Software Components

Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.4.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

20.4.2 Inputs

1. `GV47`: Inventory of Third-Party Software Components
2. Date of last review or update of the inventory

20.4.3 Operations

1. **Determine whether Input 1 exists within the enterprise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 1
2. **Use Input 1 and dermine whether each software component listed includes, at a minimum, the following information: risk associated with components, whether component is supported**
    1. Identify and enumerate software components with complete information (M3)
    2. Identify and enumerate software components with missing information (M4)
3. Compare date of Input 2 to current date and capture timeframe in days (M5)

20.4.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 1
- M3 = Count of software components with complete information
- M4 = Count of software components with missing information
- M5 = Timeframe since last review or update of the inventory

20.4.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M5 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness of Inventory

20.5 16.5: Use Up-to-Date and Trusted Third-Party Software Components

Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.5.1 Dependencies

- Safeguard 16.4: Establish and Manage an Inventory of Third-Party Software Components

20.5.2 Inputs

1. `GV47`: Inventory of Third-Party Software Components

20.5.3 Operations

1. **For each software component in Input 1 `GV47`, determine whether the latest component is being used**
    1. Identify and enumerate software components that are up-to-date (M2)
    2. Identify and enumerate software components that are not up-to-date (M3)
2. **For each software component identified in Operaion 1.1, determine whether they are explicitly trusted by the enterprise**
    1. Identify and enumerate software components that are trusted by the enterprise (M4)

20.5.4 Measures

- M1 = Count of Input 1
- M2 = Count of software components that are up-to-date
- M3 = Count of software components that are not up-to-date
- M4 = Count of software components that are up to date and trusted

20.5.5 Metrics

Compliance

Metric	The percentage of up-to-date and trusted software components
Calculation	`M4 / M1`

20.6 16.6: Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.6.1 Dependencies

- Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

20.6.2 Inputs

1. `GV48`: Process to Accept and Address Software Vulnerabilities
2. Date of last update or review of the severity rating system and process

20.6.3 Operations

1. **Using Input 1 `GV48` determine whether the enterprise has a severity rating system and process for application vulnerabilities**
    1. If the system and process exist, M1 = 1
    2. If the system and process do not exist, M1 = 0
2. **Review Input 1 `GV48` and dermine whether it includes, at a minimum, the following components: guidance for prioritizing the order vulnerabilities are fixed, level of security acceptability for releasing code or applications**
    1. For each component included in the process, assign a value of 1. Sum all values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

20.6.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the process
- M3 = Timeframe in months since last review or update

20.6.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

20.7 16.7: Use Standard Hardening Configuration Templates for Application Infrastructure

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.7.1 Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

20.7.2 Inputs

1. `GV1`: Enterprise Asset Inventory
2. `GV37`: Network infrastructure configuration standards

20.7.3 Operations

1. Use Input 1 `GV1` to identify and enumerate application infrastructure components `GV50` (M1)
2. **For each infastructure component identified in Operation 1, check configurations using Input 2 `GV37` and determine if they meet industry recommended hardening configuraion standards**
    1. Identify and enumerate infrastructure components that meet industry standards (M2)
    2. Identify and enumerate infrastructure components that do not meet industry standards (M3)

20.7.4 Measures

- M1 = Count of application infrastructure components
- M2 = Count of components that meet industry standards
- M3 = Count of components that do not meet industry standards

20.7.5 Metrics

Compliance

Metric	The percentage of application infrastructure components that meet industry configuration standards
Calculation	`M2 / M1`

20.8 16.8: Separate Production and Non-Production Systems

Maintain separate environments for production and non-production systems.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.8.1 Dependencies

- None

20.8.2 Inputs

1. `GV1`: Enterprise Asset Inventory

20.8.3 Operations

1. Use Input 1 `GV1` to identify and enumerate productions systems (M1)
2. **For each production system identified in Operation 1, use Input 1 `GV1` to identify if at least one non-production system exists for the system**
    1. Identify and enumerate productions systems with at least one non-production system (M2)
    2. Identify and enumerate productions systems without a non-production system (M3)

20.8.4 Measures

- M1 = Count of production systems
- M2 = Count of production systems with a non-production system to complement
- M3 = Count of productions systems without a non-production system to complement

20.8.5 Metrics

Coverage

20.9 16.9: Train Developers in Application Security Concepts and Secure Coding

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.9.1 Dependencies

- None

20.9.2 Inputs

1. List of software developing personnel with assigned roles and development environments
2. List of required courses for each role and development environment
3. Date of last training course

20.9.3 Operations

1. **For each individual in Input 1, determine whether they have taken the applicable courses per role and environment**
    1. Identify and enumerate personnel that have completed the appropriate courses (M2)
    2. Identify and enumerate personnel that have not completed the appropriate courses (M3)
2. **For each individual who has completed the appropriate courses, compare the date of last training from Input 3 to current date and capture timeframe in months**
    1. Identify and enumerate personnel that have completed all appropriate training within twelve months or less (M4)
    2. Identify and enumerate personnel that have not completed all appropriate training within twelve months or less (M5)

20.9.4 Measures

- M1 = Count of software developing personnel
- M2 = Count of software developing personnel with completed courses
- M3 = Count of software developing personnel without completed courses
- M4 = Count of software developing personnel with training in scope
- M5 = Count of software developing personnel with training out of scope

20.9.5 Metrics

Compliance

20.10 16.10: Apply Secure Design Principles in Application Architectures

Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.10.1 Dependencies

- Safeguard 16.1: Establish and Maintain a Secure Application Development Process

20.10.2 Inputs

1. `GV49`: Secure Application Development Process
2. `GV50`: Application Infrastructure Components

20.10.3 Operations

1. **Use Input 1 `GV49` to determine whether the process outlines a secure software framework that includes secure design principles**
    1. If the framework exists, M1 = 1
    2. If the framework does not exist, M1 = 0
2. **For each application infrastructure component in Input 2 `GV50`, determine whether the secure design principles were applied per the framework**
    1. Identify and enumerate application infrastructure components where design principles are applied (M3)

2. Identify and enumerate application infrastructure components where design principles are not applied (M4)

20.10.4 Measures

- M1 = Output of Operation 1
- M2 = Count of Input 2 `GV50`
- M3 = Count of applications infrastructure components with design principles applied
- M4 = Count of applications infrastructure components without design principles applied

20.10.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

20.11 16.11: Leverage Vetted Modules or Services for Application Security Components

Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Asset Type	Security Function	Implementation Groups
Applications	Protect	2, 3

20.11.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

20.11.2 Inputs

1. `GV5`: Authorized Software Inventory

20.11.3 Operations

1. Use Input 1 `GV5` to identify and enumerate application security components (M1)
2. **For each application security component identifed in Operation 1, determine whether custom code exists**
    1. Identify and enumerate components that contain custom code (M2)
    2. Identify and enumerate components that do not contain custom code (M3)
3. **For each application security component identifed in Operation 2.1, determine whether vetted modules or services exist**
    1. Identify and enumerate components for which vetted modules or services exist (M4)
    2. Identify and enumerate components for which vetted modules or services do not exist (M5)

20.11.4 Measures

- M1 = Count of application security components
- M2 = Count of application security components containing custom code
- M3 = Count of application security components not containing custom code
- M4 = Count of application security components containing custom code and vetted modules or services do exist
- M5 = Count of application security components containing custom code and vetted modules or services do not exist

20.11.5 Metrics

Compliance

Metric	The percentage of application security components using vetted modules or services when available
Calculation	`(M3 + M5) / M1`

20.12 16.12: Implement Code-Level Security Checks

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

20.12.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

20.12.2 Inputs

1. `GV5`: Authorized Software Inventory

20.12.3 Operations

1. Use Input 1 `GV5` to identify and enumerate in-house developed software (M1)
2. Use Input 1 `GV5` to identify static analysis tools
3. **For each software identified in Operation 1, determine if it is verified by a static tool identified in Operation 2**
    1. Identify and enumerate software verified by a static tool (M2)
    2. Identify and enumerate software not verified by a static tool (M3)
4. Use Input 1 `GV5` to identify dynamic analysis tools
5. **For each software identified in Operation 1, determine if it is verified by a dynaic tool identified in Operation 4**
    1. Identify and enumerate software verified by a dynamic tool (M4)
    2. Identify and enumerate software not verified by a dynamic tool (M5)

20.12.4 Measures

- M1 = Count of in-house developed software
- M2 = Count of in-house developed software verified by a static analysis tool
- M3 = Count of in-house developed software not verified by a static analysis tool
- M4 = Count of in-house developed software verified by a dynamic analysis tool
- M5 = Count of in-house developed software not verified by a dynamic analysis tool

20.12.5 Metrics

Static Analysis Tool Coverage

Metric	The percentage of in-house developed software verified by a static analysis tool
Calculation	`M2 / M1`

Dynamic Analysis Tool Coverage

Metric	The percentage of in-house developed software verified by a dynamic analysis tool
Calculation	`M4 / M1`

20.13 16.13: Conduct Application Penetration Testing

Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

20.13.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

20.13.2 Inputs

1. `GV5`: Authorized Software Inventory
2. Application Penetration Process for enterprise

20.13.3 Operations

1. **Determine whether Input 2 exists for the enterprise**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Use Input 1 `GV5` to identify and enumerate all applications within the enterprise (M2)
3. **For each application identified in Operation 2, determine whether an unauthenticated penentration test has been conducted per the process outlined in Input 2**
    1. Identify and enumerate applications that have been tested (M3)
    2. Identify and enumerate applications that have not been tested (M4)
4. Use the output of Operation 2, identify and enumerate critical applications within the list of applications (M5)
5. **For each application identified in Operation 4, determine whether an authenticated penentration test has been conducted per the process outlined in Input 2**
    1. Identify and enumerate applications that have been tested (M6)
    2. Identify and enumerate applications that have not been tested (M7)

20.13.4 Measures

- M1 = Output of Operation 1
- M2 = Count of applications within the enterprise
- M3 = Count of applications that have undergone unauthenticated penetration testing per enterprise's process
- M4 = Count of applications that have not undergone unauthenticated penetration testing per enterprise's process
- M5 = Count of critical applications
- M6 = Count of critical applications that have undergone authenticated penetration testing per enterprise's process
- M7 = Count of critical applications that have not undergone authenticated penetration testing per enterprise's process

20.13.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Unauthenticated Penetration Testing Coverage

Metric	The percentage of applications that underwent unauthenticated penetration testing per enterprise's process
Calculation	`M3 / M2`

Authenticated Penetration Testing Coverage

Metric	The percentage of critical applications that underwent authenticated penetration testing per enterprise's process
Calculation	`M6 / M5`

20.14 16.14: Conduct Threat Modeling

Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

Asset Type	Security Function	Implementation Groups
Applications	Protect	3

20.14.1 Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

20.14.2 Inputs

1. `GV5`: Authorized Software Inventory
2. Threat Modeling Process for the enterprise

20.14.3 Operations

1. **Determine whether Input 2 exists for the enterprise**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Use Input 1 `GV5` to identify and enumerate all in-house developed applications (M2)
3. **For each application identified in Operation 2, determine whether the threat modeling process was followed**
    1. Identify and enumerate applications for which threat modeling was conducted (M3)
    2. Identify and enumerate applications for which threat modeling was not conducted (M4)

20.14.4 Measures

- M1 = Output of Operation 1
- M2 = Count of in-house developed applications
- M3 = Count of in-house developed applications that underwent threat modeling
- M4 = Count of in-house developed applications that did not undergo threat modeling

20.14.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of in-house developed applications that underwent threat modeling
Calculation	`M3 / M2`

CHAPTER

TWENTYONE

CIS CONTROL 17: INCIDENT RESPONSE MANAGEMENT

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why is this CIS Control Critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan – even with good people – it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

21.1 17.1: Designate Personnel to Manage Incident Handling

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Respond	1, 2, 3

21.1.1 Dependencies

- None

21.1.2 Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

21.1.3 Operations

1. **Determine whether the enterprise documents designated personnel to manage incident handling by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.**
    1. If documentation designating personnel exists, M1 = 1
    2. If documentation designating personnel does not exist, M1 = 0
2. **Determine whether the documentation, at a minimum, outlines the following components: primary personnel, backup personnel, roles and responsibilities of each**
    1. For each component included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

21.1.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included for designated personnel documentation
- M3 = Timeframe since last update or review of documentation in months

21.1.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in documentation for designated incident handling personnel
Calculation	`M2 / 3`

21.2 17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

Asset Type	Security Function	Implementation Groups
N/A	Respond	1, 2, 3

21.2.1 Dependencies

- None

21.2.2 Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

21.2.3 Operations

1. **Determine whether the enterprise documents establish and maintain contact information for reporting security incidents by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.**
    1. If documentation outlining contact information exists, M1 = 1
    2. If documentation outlining contact information does not exist, M1 = 0
2. Compare Input 2 to current date and capture timeframe in months (M2)

21.2.4 Measures

- M1 = Output of Operation 1
- M2 = Timeframe since last update or review of documentation in months

21.2.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

21.3 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Respond	1, 2, 3

21.3.1 Dependencies

- None

21.3.2 Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

21.3.3 Operations

1. **Determine whether the enterprise documents process for reporting incidents by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.**
    1. If documentation for reporting incidents exists, M1 = 1
    2. If documentation for reporting incidents does not exist, M1 = 0
2. **Determine whether the documentation, at a minimum, outlines the following components: reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported**
    1. For each component included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)
4. **Determine whether the process documentation is available to the whole workforce**
    1. If it is available to all, M4 = 1
    2. If it is not available to all, M4 = 0

21.3.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included for reporting incidents process documentation
- M3 = Timeframe since last update or review of documentation in months
- M4 = Output of Operation 4

21.3.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M4 is 0, this safeguard receives a failing score for this metric. Other metrics still apply.

Completeness

Metric	The percentage of components included in documentation for designated incident handling personnel
Calculation	`M2 / 4`

21.4 17.4: Establish and Maintain an Incident Response Process

Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Respond	2, 3

21.4.1 Dependencies

- None

21.4.2 Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

21.4.3 Operations

1. **Determine whether the enterprise documents an incident response process: `GV52` by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.**
    1. If documentation for an incident response process exists, M1 = 1
    2. If documentation for an incident response process does not exist, M1 = 0
2. **Determine whether the documentation, at a minimum, outlines the following components: roles and responsibilities, compliance requirements, and a communication plan**
    1. For each component included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

21.4.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included for incident response process documentation
- M3 = Timeframe since last update or review of documentation in months

21.4.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in documentation for designated incident handling personnel
Calculation	`M2 / 3`

21.5 17.5: Assign Key Roles and Responsibilities

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Respond	2, 3

21.5.1 Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

21.5.2 Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

21.5.3 Operations

1. **Determine whether the enterprise documents key roles and responsibilities by reviewing Input 1 `GV52`**
    1. If documentation exists, M1 = 1
    2. If documentation does not exist, M1 = 0
2. Using the documentation in Input 1 `GV52`, identify and enumerate the roles and responsibilities (M2)
3. **For each role and responsibility identified in Operation 2, determine whether an individual is mapped to that role and responsibility**
    1. Identify and enumerate those that are mapped (M3)
    2. Identify and enumerate those that are not mapped (M4)
4. Compare Input 2 to current date and capture timeframe in months (M5)

21.5.4 Measures

- M1 = Output of Operation 1
- M2 = Count of roles and responsibilities outlined in process
- M3 = Count of roles and responsibilities that are mapped to an individual
- M4 = Count of roles and responsibilities that are not mapped to an individual
- M5 = Timeframe since last update or review of documentation in months

21.5.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M5 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of roles and responsibilities that are mapped to an individual
Calculation	`M3 / M2`

21.6 17.6: Define Mechanisms for Communicating During Incident Response

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	Respond	2, 3

21.6.1 Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

21.6.2 Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

21.6.3 Operations

1. **Determine whether the enterprise document mechanisms for communication by reviewing Input 1 `GV52`**
    1. If documentation for an incident response process exists, M1 = 1
    2. If documentation for an incident response process does not exist, M1 = 0
2. **Determine whether the documentation, at a minimum, outlines primary and secondary mechanisms for communication**
    1. For each mechanism included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

21.6.4 Measures

- M1 = Output of Operation 1
- M2 = Count of mechanisms for communication included in documentation
- M3 = Timeframe since last update or review of documentation in months

21.6.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in documentation for designated incident handling personnel
Calculation	`M2 / 2`

21.7 17.7: Conduct Routine Incident Response Exercises

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

Asset Type	Security Function	Implementation Groups
N/A	Recover	2, 3

21.7.1 Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

21.7.2 Inputs

1. `GV52`: Incident response process
2. Date of last exercise or test

21.7.3 Operations

1. **Determine whether the enterprise's incident response process includes routine incident response exercises by reviewing Input 1 `GV52`**
    1. If the documentation includes exercises, M1 = 1
    2. If the documentation does not include exercises, M1 = 0
2. **Determine whether the documentation for exercises, at a minimum, outlines test communication channels, decision making, and workflows**
    1. For each mechanism included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

21.7.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in documentation
- M3 = Timeframe since last exercise or test in months

21.7.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in documentation for incident response exercises
Calculation	`M2 / 3`

21.8 17.8: Conduct Post-Incident Reviews

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Asset Type	Security Function	Implementation Groups
N/A	Recover	2, 3

21.8.1 Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

21.8.2 Inputs

1. `GV52`: Incident response process
2. Last post-incident review

21.8.3 Operations

1. **Determine whether the enterprise's incident response process includes post-incident reviews by reviewing Input 1 `GV52`**
    1. If the documentation includes post-indicent reviews, M1 = 1
    2. If the documentation does not include post-incident reviews, M1 = 0
2. **Use Input 2 to determine if post-incident reviews include, at a minimum, the following components: lessons learned and follow-up actions**
    1. For each component included, assign a value of 1. Sum the values. (M2)

21.8.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in documentation

21.8.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in post-incident reviews incident response exercises
Calculation	`M2 / 2`

21.9 17.9: Establish and Maintain Security Incident Thresholds

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
N/A	N/A	1, 2, 3

21.9.1 Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

21.9.2 Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

21.9.3 Operations

1. **Determine whether the enterprise documents security incident threshold by reviewing Input 1 `GV52`**
    1. If documentation for a security incident threshold exists, M1 = 1
    2. If documentation for a security incident threshold does not exist, M1 = 0
2. **Determine whether the documentation, at a minimum, outlines the following components: differentiates between incident and event, prioritization schema based on known or potential impact, procedure relying on this schema is used to determine status update frequency during incident handling, and procedure relying on this schema is used to determine escalation paths during incident handling**
    1. For each mechanism included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date and capture timeframe in months (M3)

21.9.4 Measures

- M1 = Output of Operation 1
- M2 = Count of components included in documentation
- M3 = Timeframe since last update or review of documentation in months

21.9.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of components included in documentation for security incident thresholds
Calculation	`M2 / 4`

CHAPTER

TWENTYTWO

CIS CONTROL 18: PENETRATION TESTING

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why is this CIS Control Critical?

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses.

Often, penetration tests are performed for specific purposes: • As a "dramatic" demonstration of an attack, usually to convince decision-makers of their enterprise's weaknesses • As a means to test the correct operation of enterprise defenses ("verification") • To test that the enterprise has built the right defenses in the first place ("validation")

Independent penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration testing differs from vulnerability testing, described in CIS Control 7. Vulnerability testing just checks for presence of known, insecure enterprise assets, and stops there. Penetration testing goes further to exploit those weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability. This is an important detail, and often penetration testing and vulnerability testing are incorrectly used interchangeably. Vulnerability testing is exclusively automated scanning with sometimes manual validation of false positives, whereas penetration testing requires more human involvement and analysis, sometimes supported through the use of custom tools or scripts. However, vulnerability testing is often a starting point for a penetration test.

Another common term is "Red Team" exercises. These are similar to penetration tests in that vulnerabilities are exploited; however, the difference is the focus. Red Teams simulate specific attacker TTPs to evaluate how an enterprise's environment would withstand an attack from a specific adversary, or category of adversaries.

22.1 18.1: Establish and Maintain a Penetration Testing Program

Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Asset Type	Security Function	Implementation Groups
N/A	Identify	2, 3

22.1.1 Dependencies

- None

22.1.2 Inputs

1. :code:`GV53`Penetration Testing Program Documentation
2. Date of last update to the penetration testing program documentation

22.1.3 Operations

1. **Determine if Input 1 `GV53` exists within the enterpise**
    1. If Input 1 exists, M1 = 1
    2. If Input 1 does not exist, M1 = 0
2. **Check Input 1 for completeness. At a minimum, it should include scope of the program, frequency, point of contact information, remediation, and retrospective requirements.**
    1. For each component included in the documentation, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to current date. Capture timeframe in months (M3)

22.1.4 Measures

- M1 = Output of Operation 1
- M2 = Sum of components included in documenation
- M3 = Timeframe in months since last update to documentation

22.1.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	The percentage of minimum components included in the program documentaion
Calculation	`M2 / 5`

22.2 18.2: Perform Periodic External Penetration Tests

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

Asset Type	Security Function	Implementation Groups
Network	Identify	2, 3

22.2.1 Dependencies

- Safeguard 18.1: Establish and Maintain a Penetration Testing Program

22.2.2 Inputs

1. `GV54`: Most Recent External Penetration Report

22.2.3 Operations

1. Check Input 1 `GV54` for date of most recent external penetration test. Compare date to current date and capture timeframe in months (M1)

22.2.4 Measures

- M1 = Timeframe since last external penetration test

22.2.5 Metrics

- If M1 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

22.3 18.3: Remediate Penetration Test Findings

Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

Asset Type	Security Function	Implementation Groups
Network	Protect	2, 3

22.3.1 Dependencies

- Safeguard 18.2: Perform Periodic External Penetration Tests

22.3.2 Inputs

1. :code:`GV53: Penetration Testing Program Documentation
2. `GV54`: Most Recent External Penetration Report
3. External penetration report prior to most recent report

22.3.3 Operations

1. Use the findings in Input 3 to identify and enumerate the vulnerabilities outlined (M1)
2. Use the findings in Input 2 `GV54` to identify the vulnerabilites outlined
3. **Compare the output of Operation 1 and Operation 1**
    1. Identify and enumerate vulnerabilities found in Input 3 that continue to be in Input 2 (M2)
    2. Identify and enumerate vulnerabilities found in Input 3 that no longer appear in Input 2 (M3)
4. **Using the program documentation from Input 1 `GV53` determine whether the ouput of Operation 3.2 is still within scope based on enterprise's policy**
    1. Identify and enumerate vulnerabilities within scope (M4)
    2. Identify and enumerate vulnerabilities out of scope (M5)

22.3.4 Measures

- M1 = Count of initial vulnerabilities identified by penetration test
- M2 = Count of successfully remediated vulnerabilities
- M3 = Count of vulnerabilities that have not been remediated
- M4 = Count of unremediated vulnerabilities still in scope
- M5 = Count of unremediated vulnerabilities out of scope

22.3.5 Metrics

Compliance

Metric	The percent of successfully remediated or still within scope vulnerabilities identified in the intial penetration test findings
Calculation	`(M3 + M4) / M1`

22.4 18.4: Validate Security Measures

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

Asset Type	Security Function	Implementation Groups
Network	Protect	3

22.4.1 Dependencies

- Safeguard 18.1: Establish and Maintain a Penetration Testing Program

22.4.2 Inputs

1. `GV53`: Penetration Testing Program Documentation
2. `GV54`: Most Recent External Penetration Report
3. `GV55`: Most Recent Internal Penetration Report

22.4.3 Operations

1. **Check Input 1 `GV53` to determine if it incluces an enterprise process for validating security measures after a penetration test**
    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0
2. Using the findings from both Input 2 `GV54` an Input 3 `GV55`, as applicable, identify and enumerate security measures that required modification (M2)
3. **For each security measure identified in Operation 2, check if modifications have been made**
    1. Identify and enumerate security measures that have been modified per the enterprise's defined process (M3)
    2. Identify and enumerate security measures not yet modified per the enterprise's defined process (M4)

22.4.4 Measures

- M1 = Output of Operation 1
- M2 = Count of security measures requiring modification
- M3 = Count of security measures requiring modification that are properly addressed
- M4 = Count of security measures requiring modification that are not yet addressed

22.4.5 Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Compliance

Metric	The percentage of security measures requiring modification that have been properly addressed
Calculation	`M3 / M2`

22.5 18.5: Perform Periodic Internal Penetration Tests

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

Asset Type	Security Function	Implementation Groups
N/A	Identify	3

22.5.1 Dependencies

- Safeguard 18.1: Establish and Maintain a Penetration Testing Program

22.5.2 Inputs

1. `GV55`: Most Recent Internal Penetration Report

22.5.3 Operations

1. Check Input 1 `GV55` for date of most recent internal penetration test. Compare date to current date and capture timeframe in months (M1)

22.5.4 Measures

- M1 = Timeframe since last internal penetration test

22.5.5 Metrics

- If M1 is greater than twelve months, then this safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.