Safeguard visualizations community project

"A visual guide" to The Center for Internet Security Critical Controls

Version 8

Developers

Pax8

Matt Lee

Senior Director of Security
and Compliance

Pax8

Veronika Dombayeva

Vendor Strategy Analyst

Collaboration from CIS

Center for Internet Security

Charity Otwell

Director, Critical Security Controls

Center for Internet Security

Joshua Franklin

Senior Cybersecurity Engineer

Special thanks to our Facilitators

Global Data Systems

Bob Miller

Blue Helm Technology

Stephen Kellogg

Contributors

Alex Dumas

Ember One

Andy Larin

allCare IT

Bob Miller

Global Data Systems

Brandon Martinez

ZenTop Consulting

Brendan Patterson

Watchguard

Chris Johnson

CompTIA

Dan Brinkmann

Summit Technology, LLC

Danny Banks

Watchguard

Dawn R. Sizer

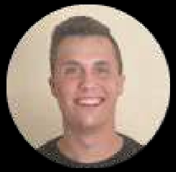
3rd Element Consulting

Eddie Phillips

Malwarebytes

Maria Scarmardo

Praxis Data Security


Evan Grace

Tenable

Heath Spencer

TraitWare

Henry Timm

Phantom Technology Solutions

Jack Skinner

Oversee My IT

Jordan Clark

CW IT Support

Joshua Franklin

Center For Internet Security

Karen Stanford

Archstone Security

Kenneth Brothers

Information Security Risk Management

Marc P. Menzies

Overview Technology Solutions

Tommy Takiari

CorCyber

Zach Kromowski

Senteon

Martin Perkins

Ki Security and Compliance Group

Heather Noggle

Codistac

Robert Ellis

Akana

Rui Lopes

Checkpoint

Stephen Kellogg

Blue Helm Technology

Teddy Guzek

Shield Cyber

Tim Golden

Compliance Scorecard

Tim Schnurr

Inquisitive IT

Todd Sieger

Pax8

Commendable Effort

(Over 25 hours of participation)

Bob Miller

Global Data Systems

Eddie Phillips

Malwarebytes

Heath Spencer

TraitWare

Heather Noggle

Codistac

Karen Stanford

Archstone Security

Maria Scarmardo

Praxis Data Security

Tim Golden

Compliance Scorecard

Zach Kromowski

Senteon

The objective of the following is to create a resourceful guide that assists security professionals in navigating through the alignment of their cybersecurity stack with the CIS Critical Controls™ and Safeguards. To do so this document presents visual representations of each safeguard's language broken down into specific taxonomical elements. Additional work has been done to help visualize the "interdependence" between the 153 safeguards that make up the CIS Critical Controls™.

Utilizing visual mappings of these elements, security teams have an effective way to evaluate their understanding of the breadth and depth of each safeguard, identify gaps, and plan for enhancements. While vendors may find this guide useful for aligning their products and service features with CIS Controls, the primary focus is supporting security teams in strengthening their preventative security measures.

These guides are born from an initiative utilizing these taxonomical elements to create a questionnaire that classifies vendors' products, and services, into the safeguards they aid. This involves a detailed evaluation criterion, including technical components and vendor attestation methods, to ensure comprehensive coverage capabilities for each respective safeguard. The resulting classifications and sorting of vendor tool products will additionally help reduce the curve of adoption of the CIS Critical Controls and will be available in many formats including in the Pax8 platform.

A note to the reader:

This publication is a result of a collaborative effort between Pax8, the Center of Internet Security (CIS), and a diverse group of industry leaders that span from practitioners to developers.

Nothing in this document should be taken to contradict or alter the existing CIS standards and/or guidelines. This guide is designed with the prerequisite understanding that the readers have a foundational knowledge of security principles. It is additionally helpful that the reader be aware of CIS Controls, CIS Implementation Groups, CIS Benchmarks, and the broader CIS body of work.

With a unified mission to level up cybersecurity best practices' businesses globally, this effort will continue to be a community collaboration of security professionals. We invite you to make the most of this freely available resource!

Thank you

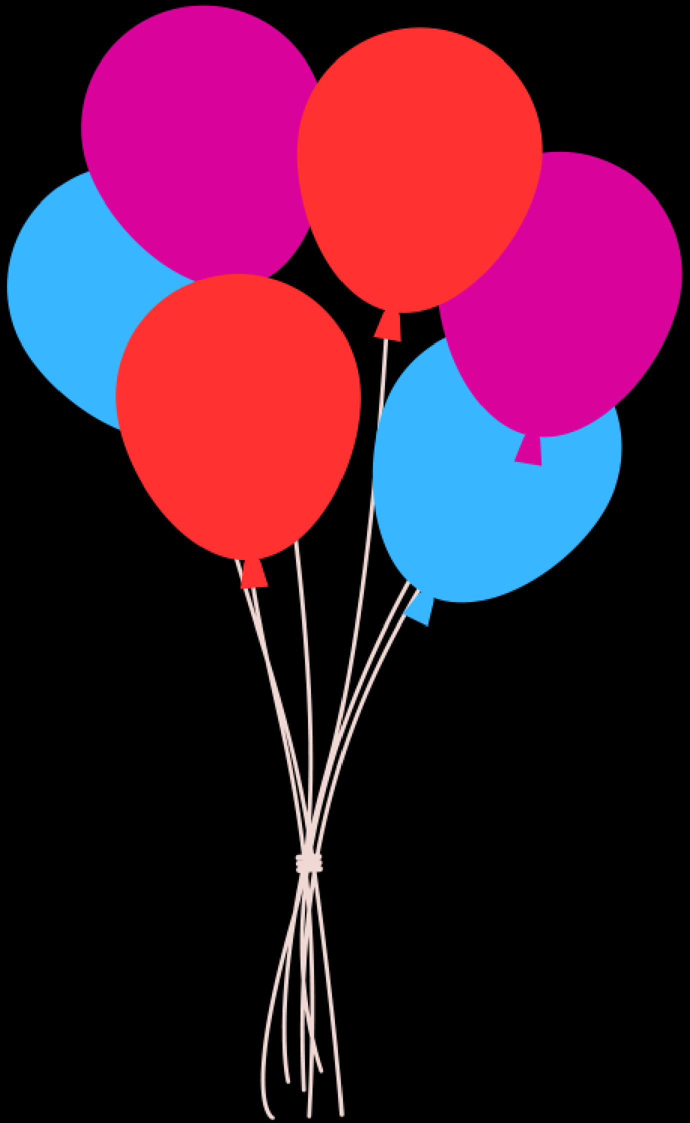
Finally, we would like to thank all who collaborated and invested many hours in the success of this project.

Understanding safeguard visualizations using balloons

A helpful precursor to the visualizations

Video Walkthrough

https://go.cybermattlee.com/balloonsafeguards



Green Rows, and Green Highlighted Numbering are NOT in the original "Cost of Cyber Defense" Document by CIS

Category	Tool	Safeguard
Asset Management	Enterprise Asset Management Policy / Process	1.1
	Enterprise and Software Asset Management Tool	1.1 1.2 2.1 2.2 2.3 2.4 9.1 12.1
	Software and Asset Discovery Tool	1.3 1.4 1.5 2.4
	Software Asset Management Policy / Process	2.1
	Application Control and Allowlisting Tool	2.5 2.6
	Script Control and Allowlisting Tool	2.7
	~~Service Provider Management Tool~~	~~15.1~~
Data Management	Data Management Policy/Process	3.1
	Data Management Tool	3.2
	Data Disposal Tool	3.5
	Data Classification Tool	3.7
	Data Flow Diagramming Tool	3.8
	Data Loss Prevention Tool	3.13
	Encryption Tool	3.6 3.9 3.10 3.11
Secure Configurations	Secure Configuration Policy / Process	4.1 4.2 3.12 8.4 8.6 8.7 8.8 8.12
	Configuration Management Tool	4.1 4.2 4.3 4.6 4.7 4.8 4.9 4.10 4.11 4.12 5.4 9.4 10.3 10.5
	Firewall	4.4 4.5 13.4 13.8
Account and Access Control Management	Account and Credential Management Policy / Process	6.1 6.2 6.6 6.7 6.8
	Identity and Access Management Tool	3.3 3.4 5.1 5.3 5.4 5.5 5.6 6.7 6.8 12.5
	Password Management Tool	5.2
	Multi-Factor Authentication Tool	6.3 6.4 6.5
Vulnerability Management	Vulnerability/Patch Management Policy / Process	7.1 7.7
	Vulnerability/Patch Management Tool	7.2 7.3 7.4
	Vulnerability Scanning Tool	7.5 7.6
Log Management	Log Management Policy / Process	3.14 8.1 8.5
	Log Analytics and Centralization Tool	8.9 8.10 8.11
	Log Management Tool	8.2 8.3 8.5 8.6 8.7 8.8 8.12
Malware Defense	Anti-Malware Software	10.1 10.2 10.4 10.6 10.7 13.2
	URL Filtering Tool	9.3
	DMARC Management Tool	9.5
	Anti-Malware Software Configuration Policy / Process	10.4 10.6 10.7
	Email Security Tool	9.6 9.7
	Security Alert Correlation Tool	13.1 13.6
	DNS Service/Server	9.2
Data Recovery	Data Recovery Policy / Process	11.1 11.5
	Data Backup and Recovery Tool	11.2 11.3 11.4 11.5
Network Security	Secure Network Management and Design Policy / Process	12.2 12.3 12.4 12.5 12.6 12.7 12.8
	Network Architecture Diagramming Tool	12.4
	VPN / Encryption Tool	12.7
Network Defense	Intrusion Detection System	13.3
	Intrusion Prevention Solution	13.7 13.8
	Device Posture Tool	13.5
	Network Flow Collection Tool	13.6
	Network Access Control Tool	13.9
	Firewall	13.4 13.8 13.10
	SOC Operations	13.11
Security Training	Security Training and Awareness Policy / Process	14.1
	Security Training and Awareness Tool(s)	14.2 14.3 14.4 14.5 14.6 14.7 14.8 14.9 16.9
Service Provider Management	Service Provider Management Policy	15.2 15.3 15.4 15.5 15.6 15.7
	Third-Party Risk Management (TPRM) Tool	15.1 15.5 15.6 15.7
	Contract Management	15.4
Secure Application Development	Secure Application Development Policy / Process	16.1 16.8 16.9 16.10 16.11 16.14
	Software Development Vulnerability Policy / Process	16.2 16.3 16.6
	Software Composition Tool	16.4 16.5
	Configuration Baseline Tool	16.7
	Code Analysis Tool	16.12
	Application Security Testing	16.13
Incident Response	Incident Response Planning	17.1 17.2 17.3 17.4 17.5 17.6 17.7 17.8 17.9
Penetration Testing	Penetration Testing Policy / Process	18.1 18.2 18.3 18.4 18.5

CONTROL 01

Inventory and Control of Enterprise Assets

SAFEGUARDS TOTAL	5	IG1	2/5	IG2	4/5	IG3	5/5

Overview

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.

Group Validated

1.1

Process Oriented Safeguard

IG1

Asset Management

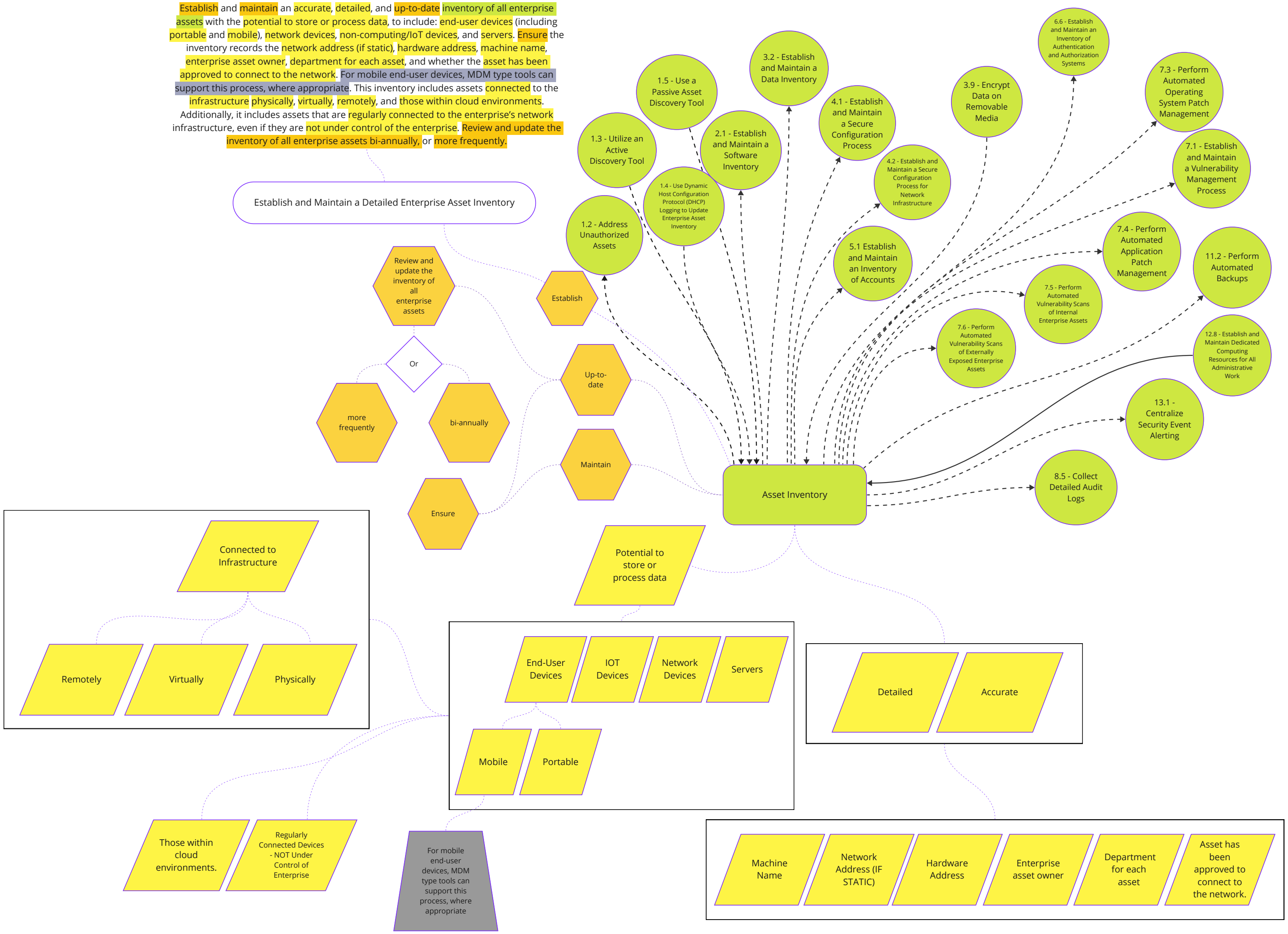
Identify

Enterprise Asset Management Policy / Process

Devices

Enterprise and Software Asset Management Tool

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, enterprise 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.

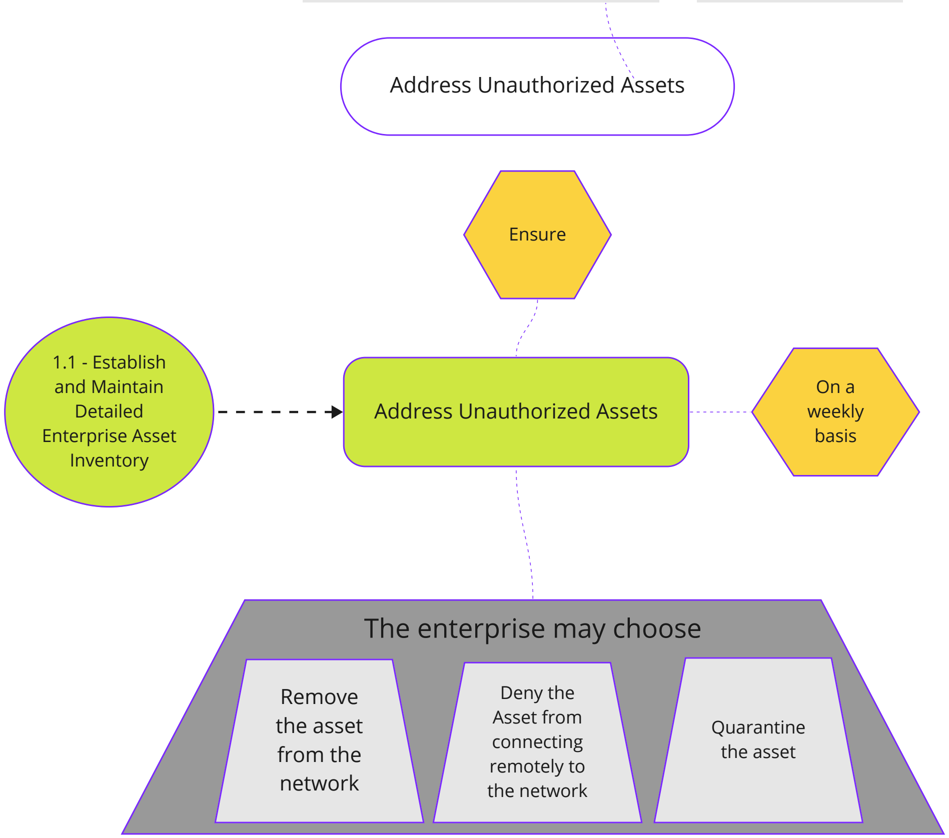


Establish and Maintain a Detailed Enterprise Asset Inventory
Review and update the inventory of all enterprise assets
Or
more frequently
bi-annually
Establish
Up-to-date
Maintain
Ensure
1.5 - Use a Passive Asset Discovery Tool
3.2 - Establish and Maintain a Data Inventory
1.3 - Utilize an Active Discovery Tool
2.1 - Establish and Maintain a Software Inventory
4.1 - Establish and Maintain a Secure Configuration Process
3.9 - Encrypt Data on Removable Media
6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems
7.3 - Perform Automated Operating System Patch Management
1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure
7.1 - Establish and Maintain a Vulnerability Management Process
1.2 - Address Unauthorized Assets
5.1 Establish and Maintain an Inventory of Accounts
7.4 - Perform Automated Application Patch Management
11.2 - Perform Automated Backups
7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets
7.6 - Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets
12.8 - Establish and Maintain Dedicated Computing Resources for All Administrative Work
13.1 - Centralize Security Event Alerting
Asset Inventory
8.5 - Collect Detailed Audit Logs
Connected to Infrastructure
Remotely
Virtually
Physically
Potential to store or process data
End-User Devices
IOT Devices
Network Devices
Servers
Mobile
Portable
Detailed
Accurate
Those within cloud environments.
Regularly Connected Devices - NOT Under Control of Enterprise
For mobile end-user devices, MDM type tools can support this process, where appropriate
Machine Name
Network Address (IF STATIC)
Hardware Address
Enterprise asset owner
Department for each asset
Asset has been approved to connect to the network.

Group Validated

1.2

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.



Address Unauthorized Assets

Ensure

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

Address Unauthorized Assets

On a weekly basis

The enterprise may choose

Remove the asset from the network

Deny the Asset from connecting remotely to the network

Quarantine the asset

IG1

Asset management

Respond

Enterprise and Software Asset Management Tool

Devices

Group Validated

1.3

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.

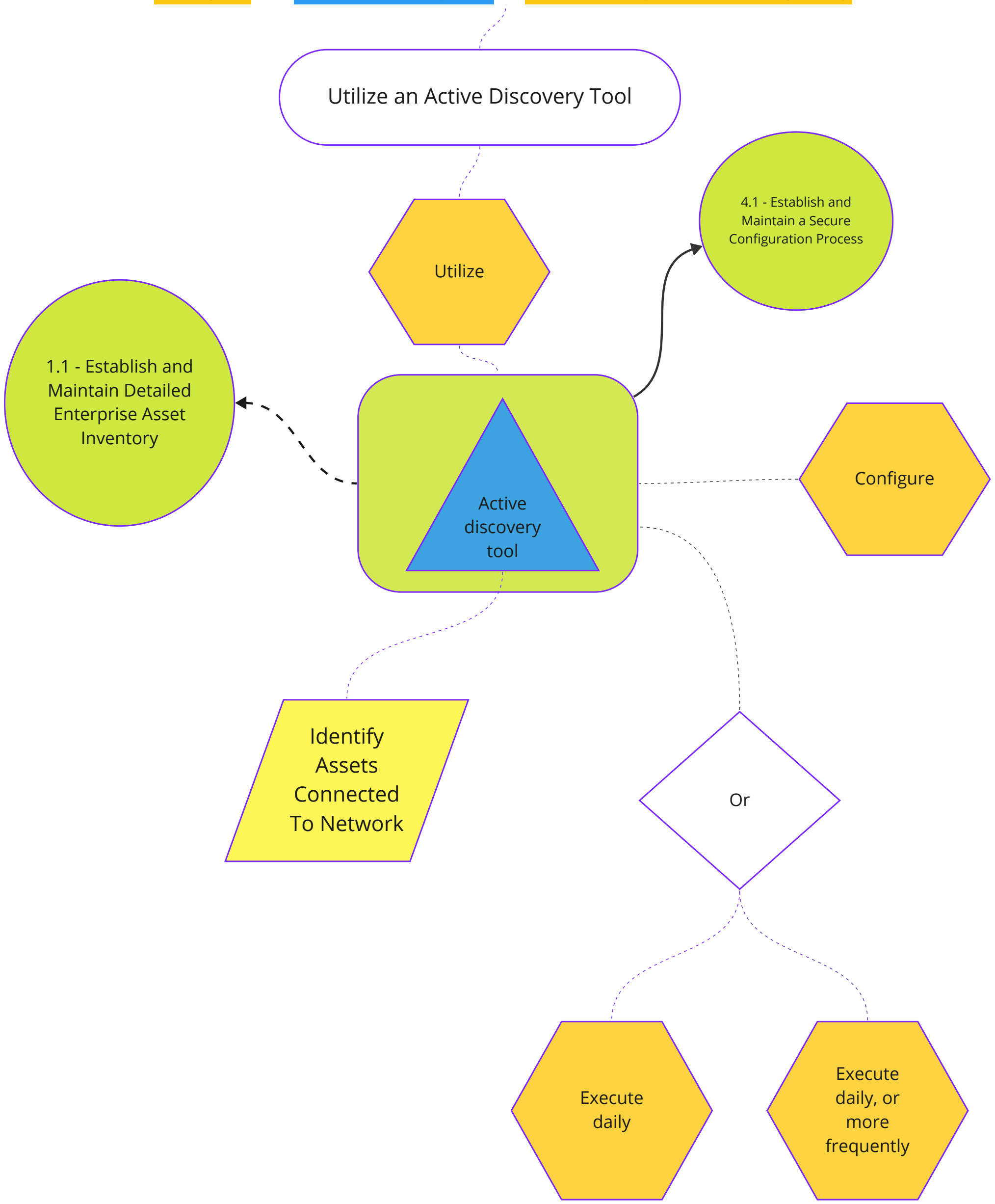
IG2

Asset Management

Detect

Devices

Software and Asset Discovery Tool



Utilize an Active Discovery Tool

Utilize

4.1 - Establish and Maintain a Secure Configuration Process

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

Active discovery tool

Configure

Identify Assets Connected To Network

Or

Execute daily

Execute daily, or more frequently

Group Validated

1.4

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.

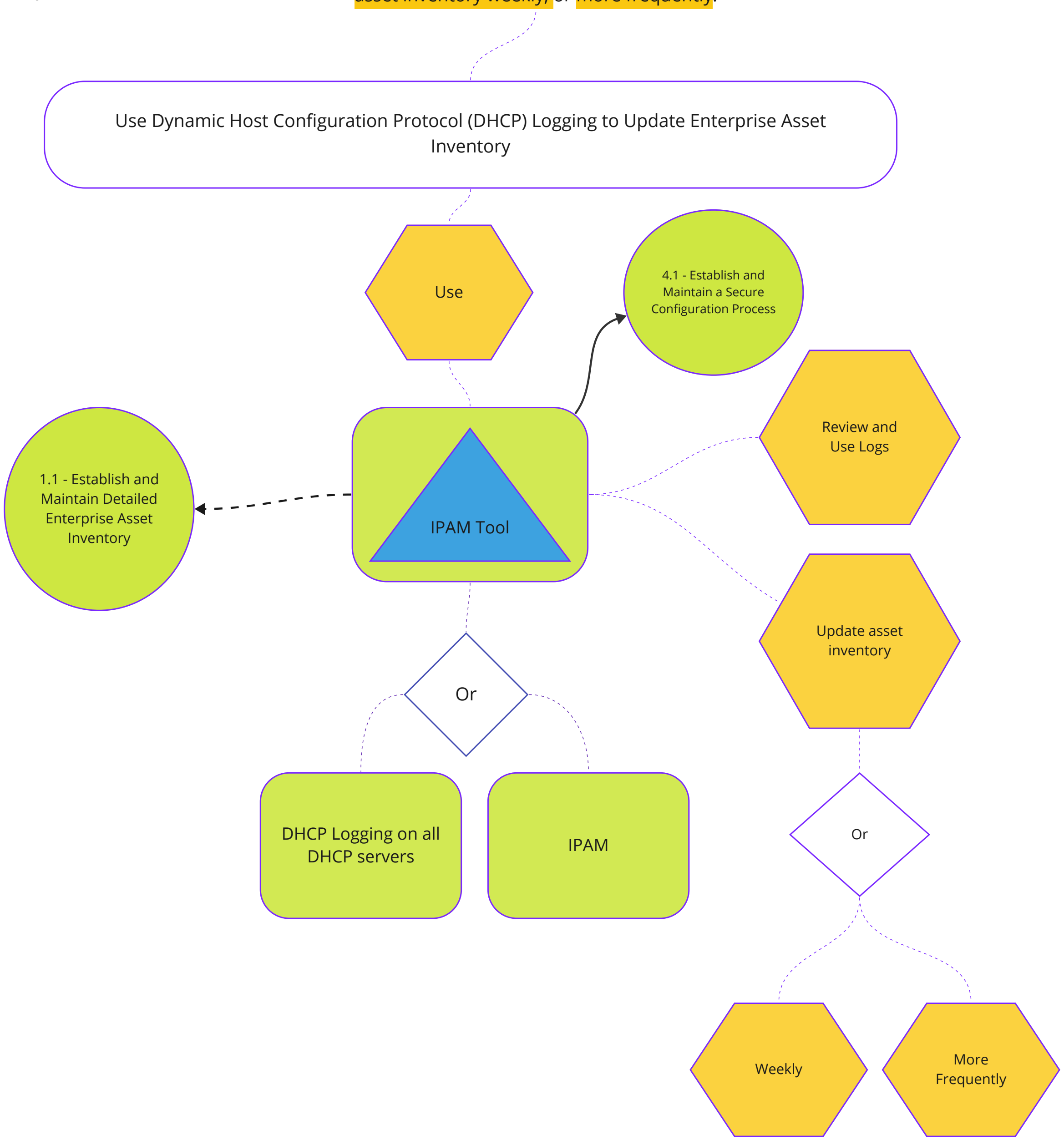
IG2

Identify

Devices

Asset Management

Software and Asset Discovery Tool



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

Use

4.1 - Establish and Maintain a Secure Configuration Process

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

IPAM Tool

Review and Use Logs

Update asset inventory

Or

DHCP Logging on all DHCP servers

IPAM

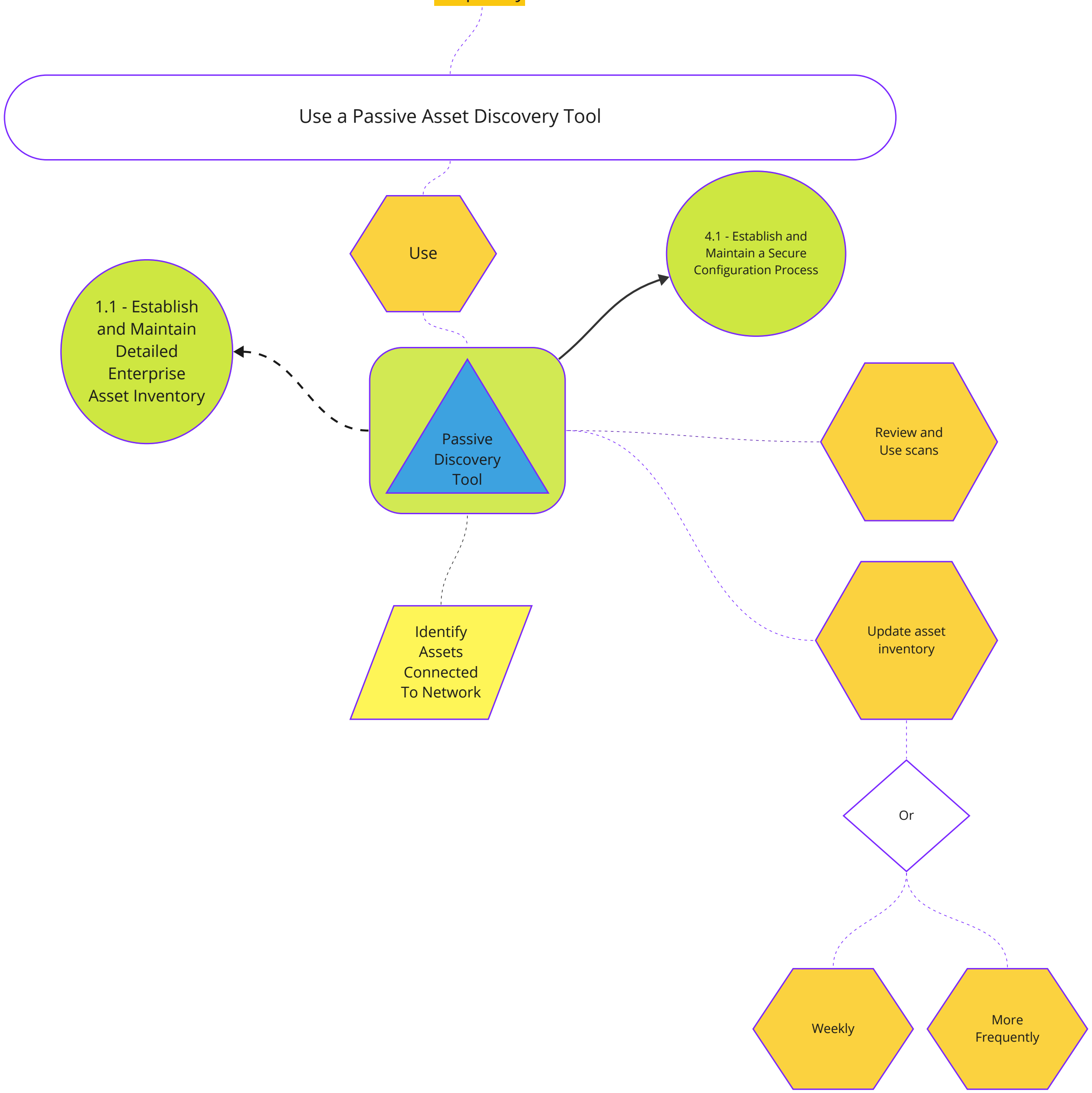
Or

Weekly

More Frequently

Group Validated

1.5 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.



Use a Passive Asset Discovery Tool

Use

4.1 - Establish and Maintain a Secure Configuration Process

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

Passive Discovery Tool

Review and Use scans

Update asset inventory

Identify Assets Connected To Network

Or

Weekly

More Frequently

IG3

Detect

Devices

Asset Management

Software and Asset Discovery Tool

CONTROL 02

Inventory and Control of Software Assets

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	3/7	6/7	7/7

Overview

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.

Group Validated

2.1

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.

Process Oriented Safeguard

IG1

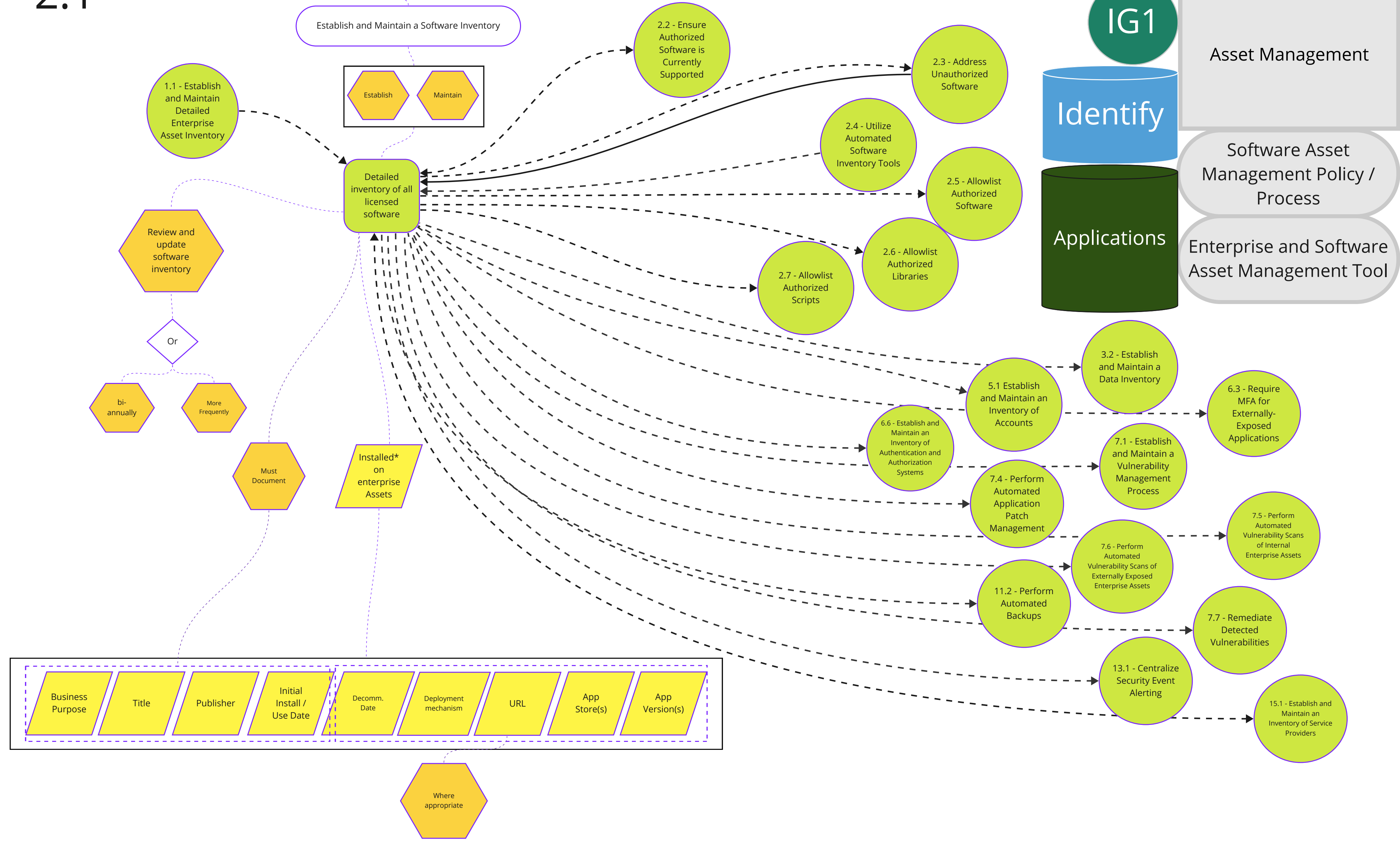
Asset Management

Identify

Applications

Software Asset Management Policy / Process

Enterprise and Software Asset Management Tool



Establish and Maintain a Software Inventory

Establish

Maintain

Detailed inventory of all licensed software

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

Review and update software inventory

Or

bi-annually

More Frequently

Must Document

Installed* on enterprise Assets

Business Purpose

Title

Publisher

Initial Install / Use Date

Decomm. Date

Deployment mechanism

URL

App Store(s)

App Version(s)

Where appropriate

2.2 - Ensure Authorized Software is Currently Supported

2.3 - Address Unauthorized Software

2.4 - Utilize Automated Software Inventory Tools

2.5 - Allowlist Authorized Software

2.6 - Allowlist Authorized Libraries

2.7 - Allowlist Authorized Scripts

3.2 - Establish and Maintain a Data Inventory

5.1 Establish and Maintain an Inventory of Accounts

6.3 - Require MFA for Externally-Exposed Applications

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

7.1 - Establish and Maintain a Vulnerability Management Process

7.4 - Perform Automated Application Patch Management

7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets

7.6 - Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets

11.2 - Perform Automated Backups

7.7 - Remediate Detected Vulnerabilities

13.1 - Centralize Security Event Alerting

15.1 - Establish and Maintain an Inventory of Service Providers

Group Validated

2.2

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.

Process Oriented Safeguard

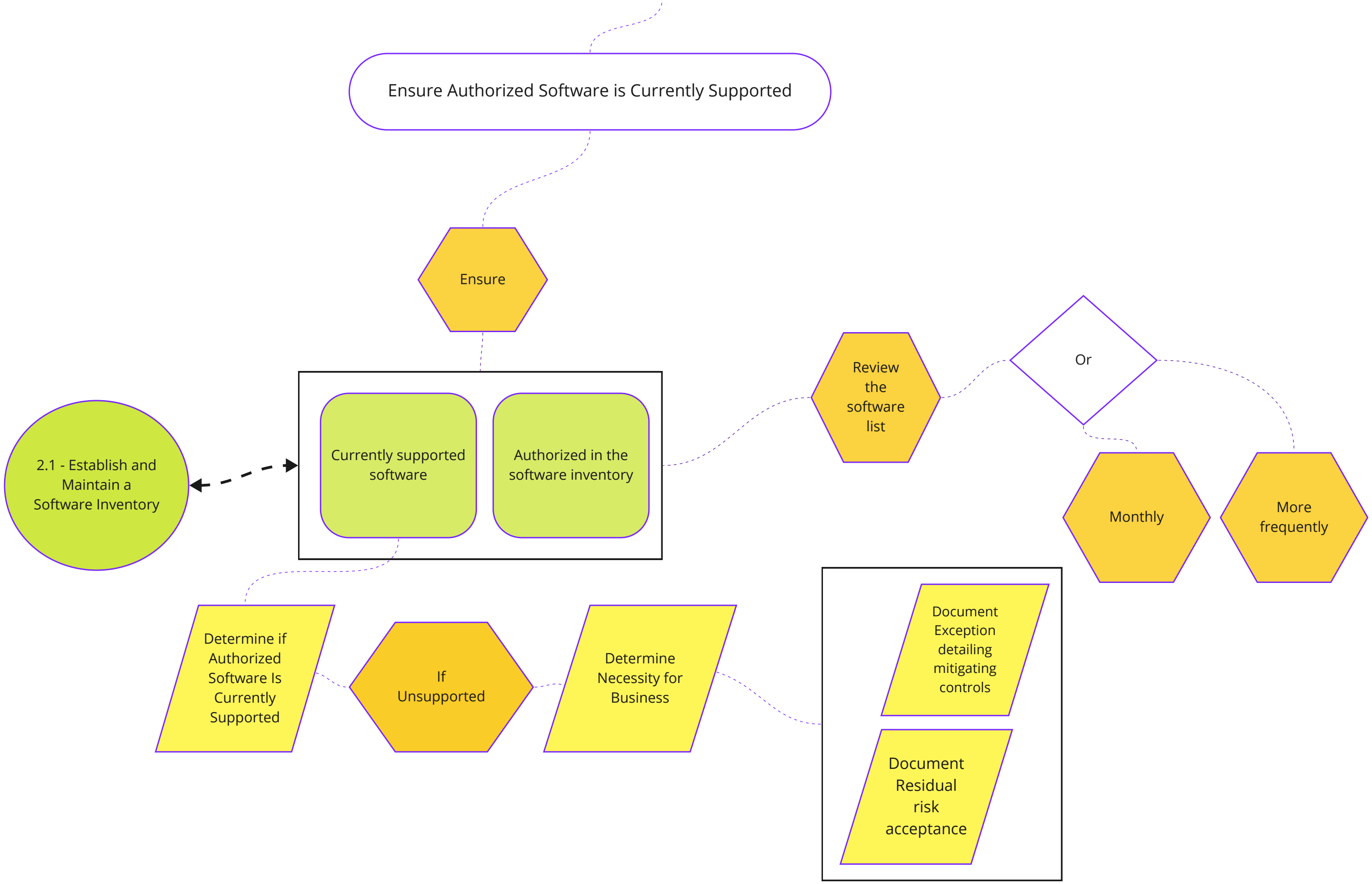
IG1

Asset Management

Identify

Enterprise and Software Asset Management Tool

Applications



Ensure Authorized Software is Currently Supported

Ensure

Currently supported software

Authorized in the software inventory

2.1 - Establish and Maintain a Software Inventory

Review the software list

Or

Monthly

More frequently

Determine if Authorized Software Is Currently Supported

If Unsupported

Determine Necessity for Business

Document Exception detailing mitigating controls

Document Residual risk acceptance

Group Validated

2.3

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

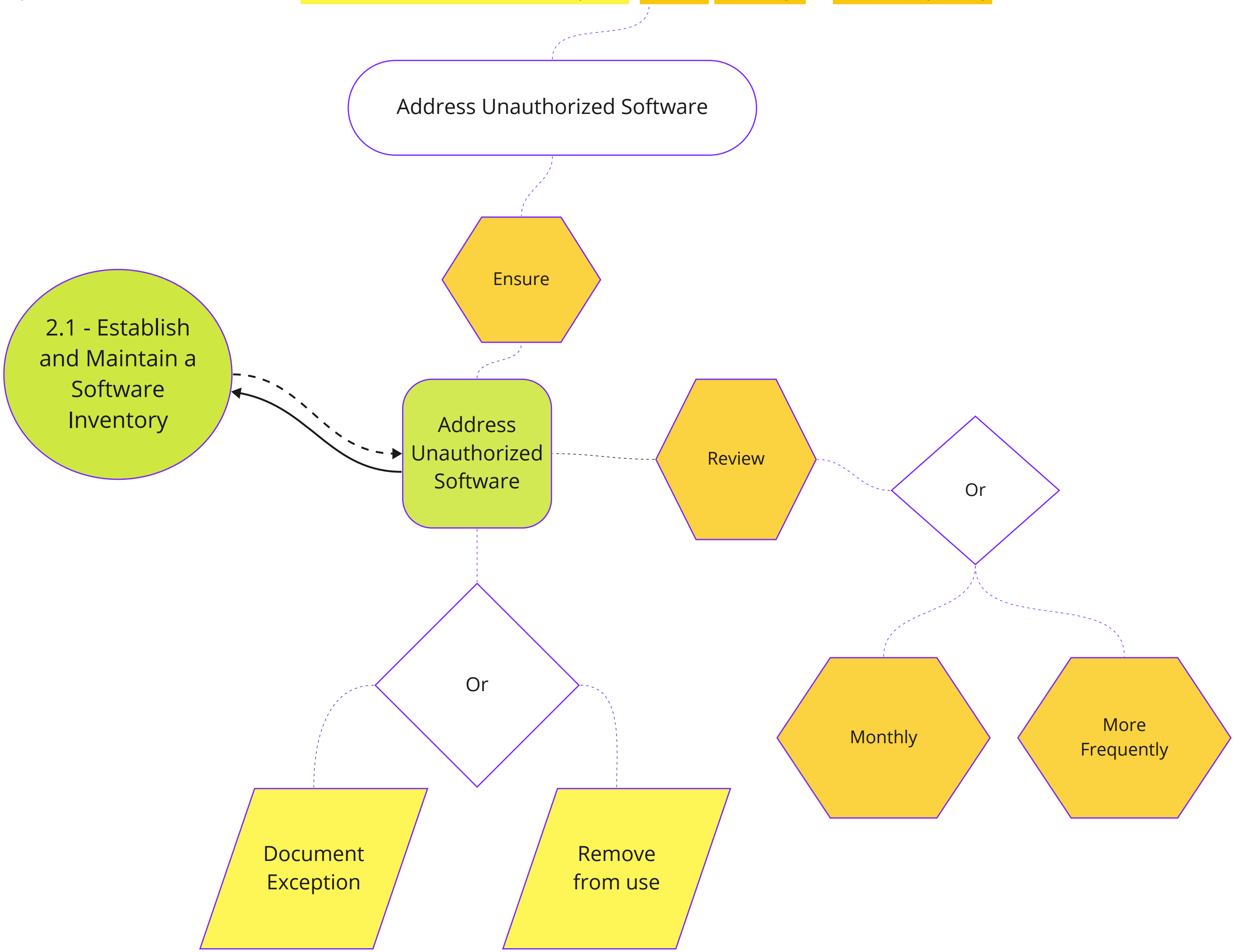
IG1

Asset Management

Respond

Applications

Enterprise and Software Asset Management Tool

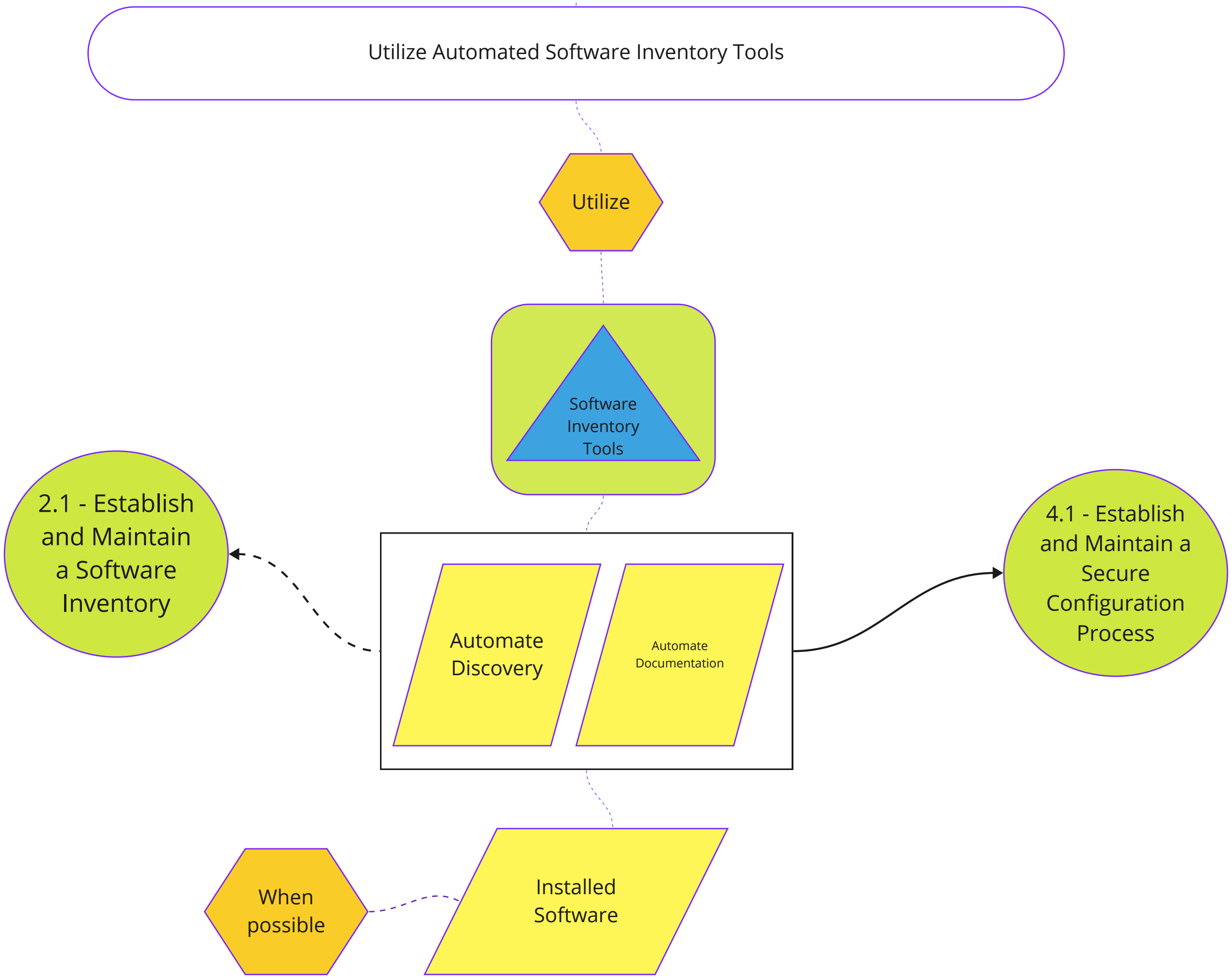


Address Unauthorized Software
Ensure
2.1 - Establish and Maintain a Software Inventory
Address Unauthorized Software
Review
Or
Or
Monthly
More Frequently
Document Exception
Remove from use

Group Validated

2.4

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



Utilize Automated Software Inventory Tools

Utilize

Software Inventory Tools

Automate Discovery

Automate Documentation

Installed Software

When possible

2.1 - Establish and Maintain a Software Inventory

4.1 - Establish and Maintain a Secure Configuration Process

IG2

Asset Management

Detect

Applications

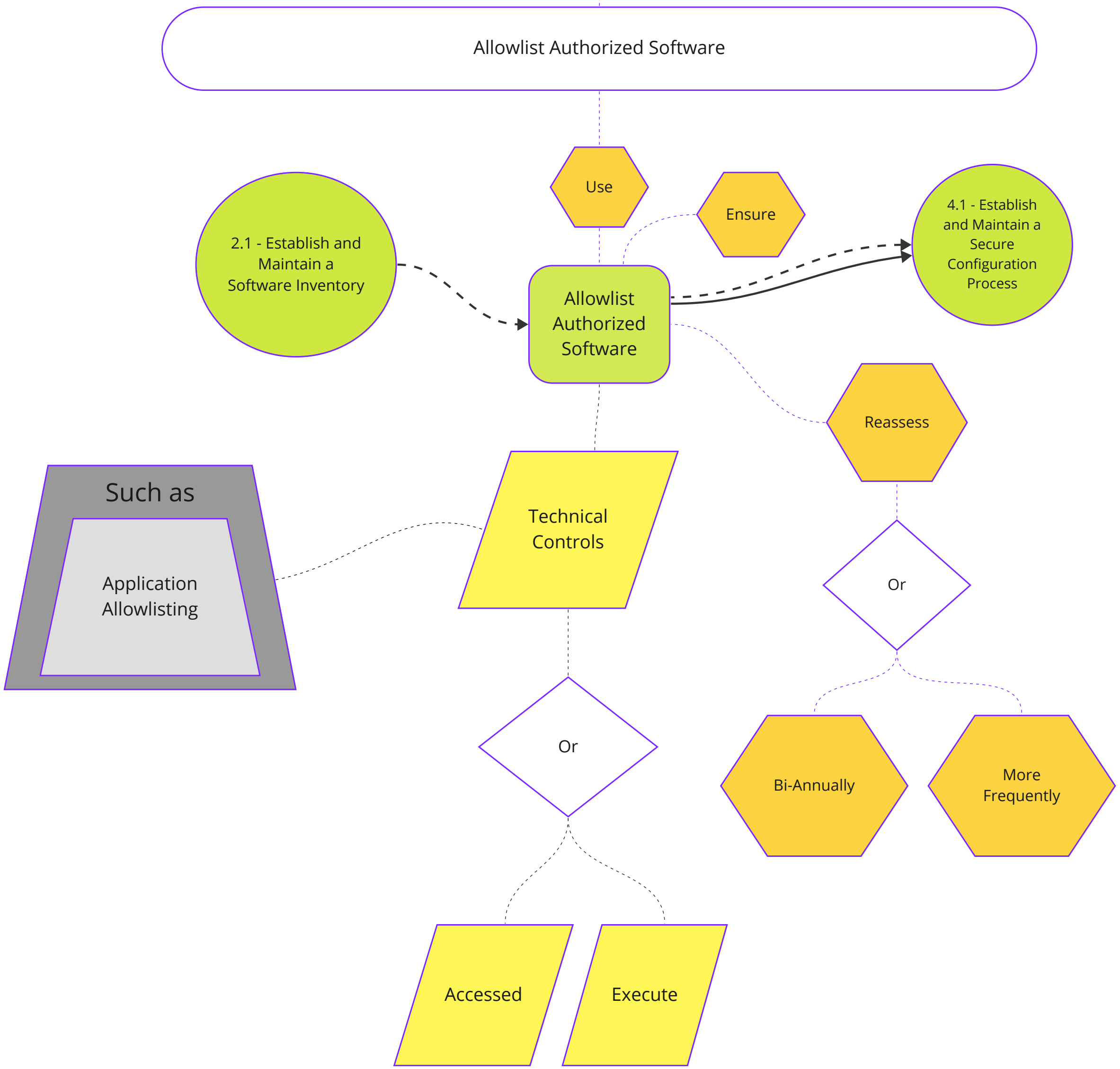
Enterprise and Software Asset Management Tool

Software and Asset Discovery Tool

Group Validated

2.5

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



Allowlist Authorized Software

Use

Ensure

2.1 - Establish and Maintain a Software Inventory

Allowlist Authorized Software

4.1 - Establish and Maintain a Secure Configuration Process

Reassess

Such as

Application Allowlisting

Technical Controls

Or

Bi-Annually

More Frequently

Or

Accessed

Execute

IG2

Asset Management

Protect

Application Control and Allowlisting Tool

Applications

OS Dependent

Group Validated

2.6

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.

IG2

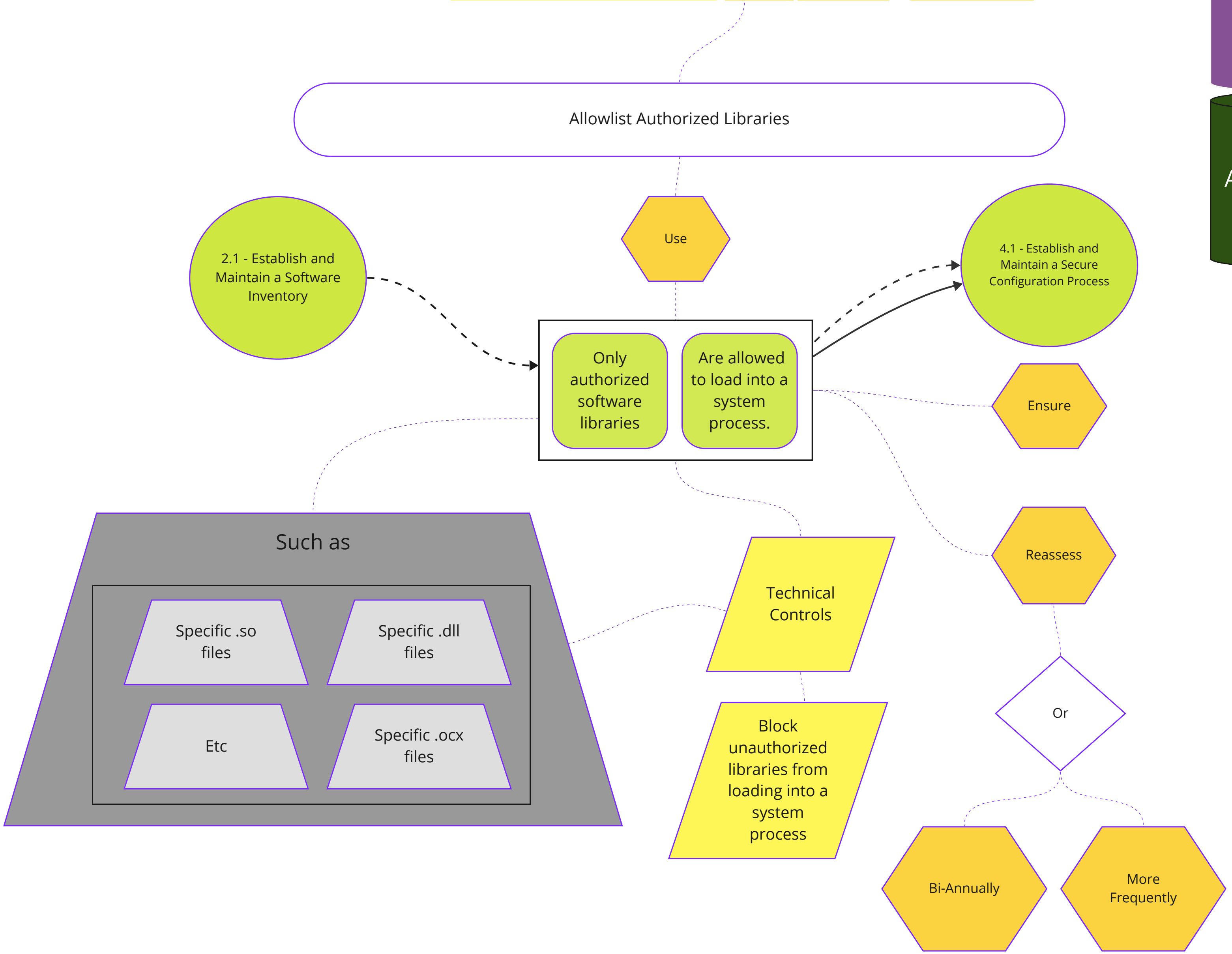
Asset management

Protect

Application Control and Allowlisting Tool

Applications

OS Dependent



Allowlist Authorized Libraries

Use

2.1 - Establish and Maintain a Software Inventory

4.1 - Establish and Maintain a Secure Configuration Process

Only authorized software libraries

Are allowed to load into a system process.

Ensure

Such as

Specific .so files

Specific .dll files

Etc

Specific .ocx files

Technical Controls

Block unauthorized libraries from loading into a system process

Reassess

Or

Bi-Annually

More Frequently

Group Validated

2.7

IG3

Asset management

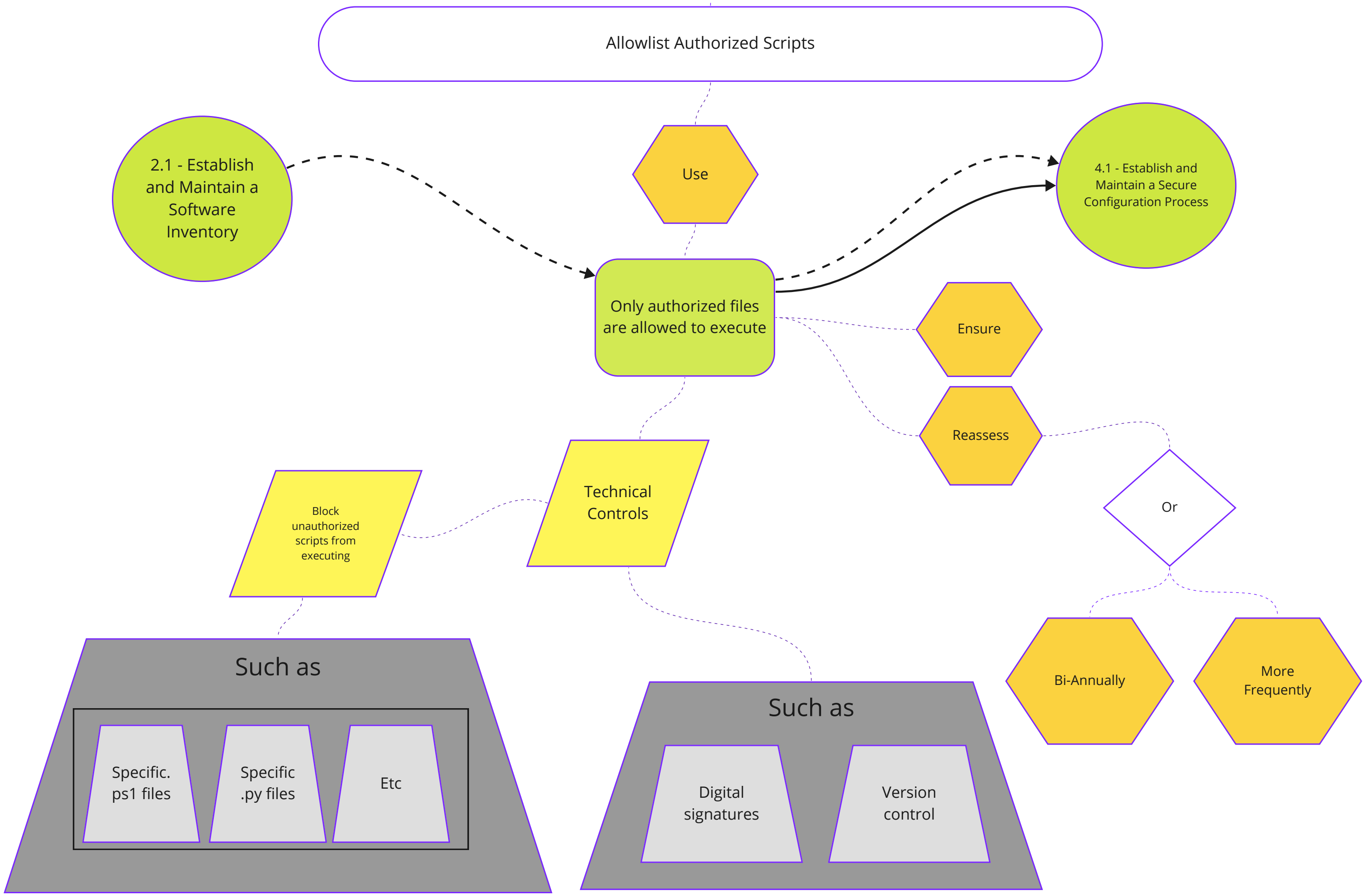
Protect

Script Control and Allowlisting Tool

Applications

OS Dependent

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.



Allowlist Authorized Scripts

2.1 - Establish and Maintain a Software Inventory

Use

4.1 - Establish and Maintain a Secure Configuration Process

Only authorized files are allowed to execute

Ensure

Reassess

Or

Technical Controls

Block unauthorized scripts from executing

Bi-Annually

More Frequently

Such as

Specific. ps1 files

Specific .py files

Etc

Such as

Digital signatures

Version control

CONTROL 03

Data Protection

SAFEGUARDS TOTAL	IG1	IG2	IG3
14	6/14	12/14	14/14

Overview

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

Group Validated

3.1

Process Oriented Safeguard

IG1

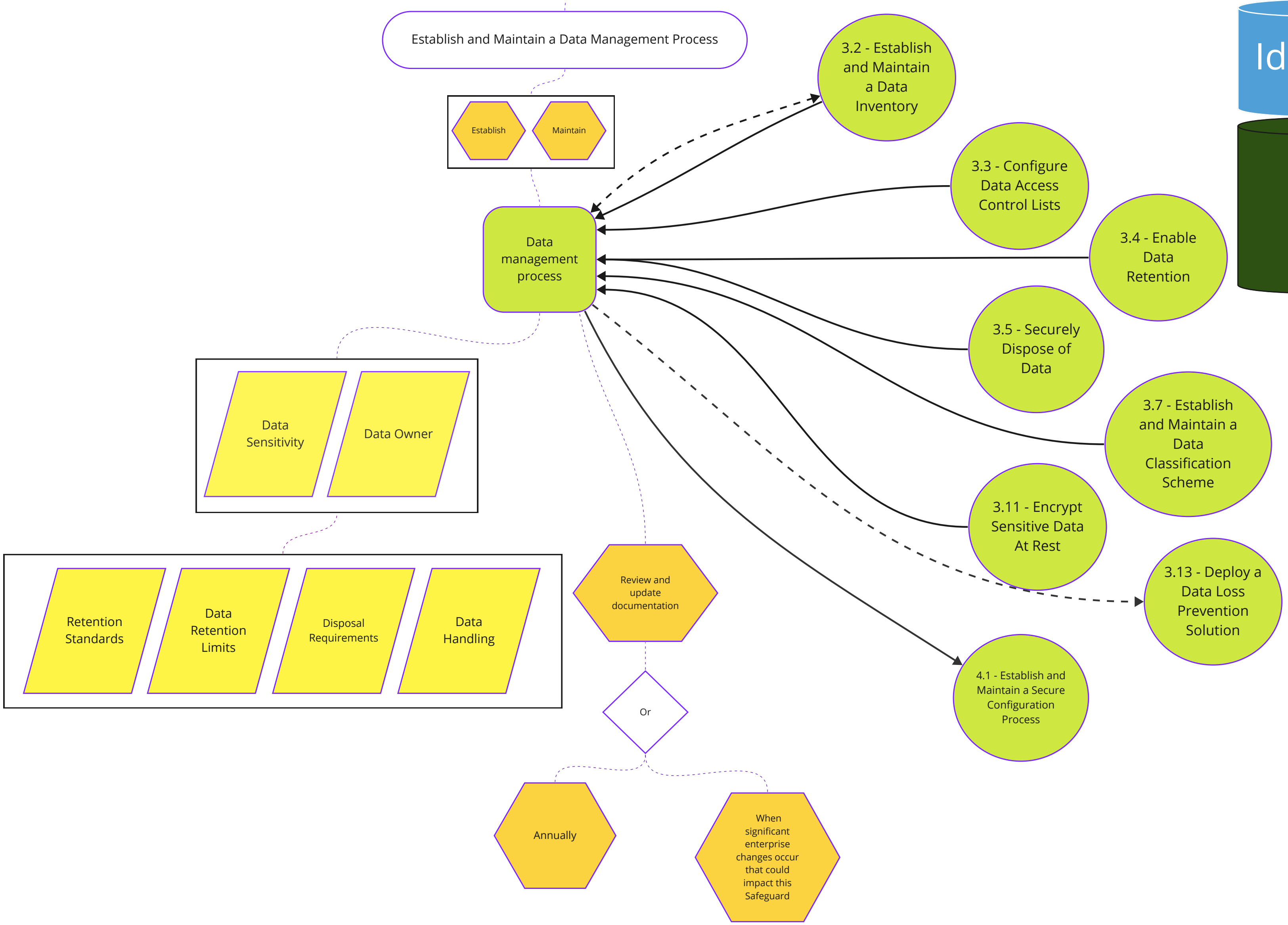
Identify

Data

Data Management

Data Management Policy / 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.



Establish and Maintain a Data Management Process

Establish

Maintain

Data management process

Data Sensitivity

Data Owner

Retention Standards

Data Retention Limits

Disposal Requirements

Data Handling

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

3.2 - Establish and Maintain a Data Inventory

3.3 - Configure Data Access Control Lists

3.4 - Enable Data Retention

3.5 - Securely Dispose of Data

3.7 - Establish and Maintain a Data Classification Scheme

3.11 - Encrypt Sensitive Data At Rest

3.13 - Deploy a Data Loss Prevention Solution

4.1 - Establish and Maintain a Secure Configuration Process

Group Validated

3.2

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.

Process Oriented Safeguard

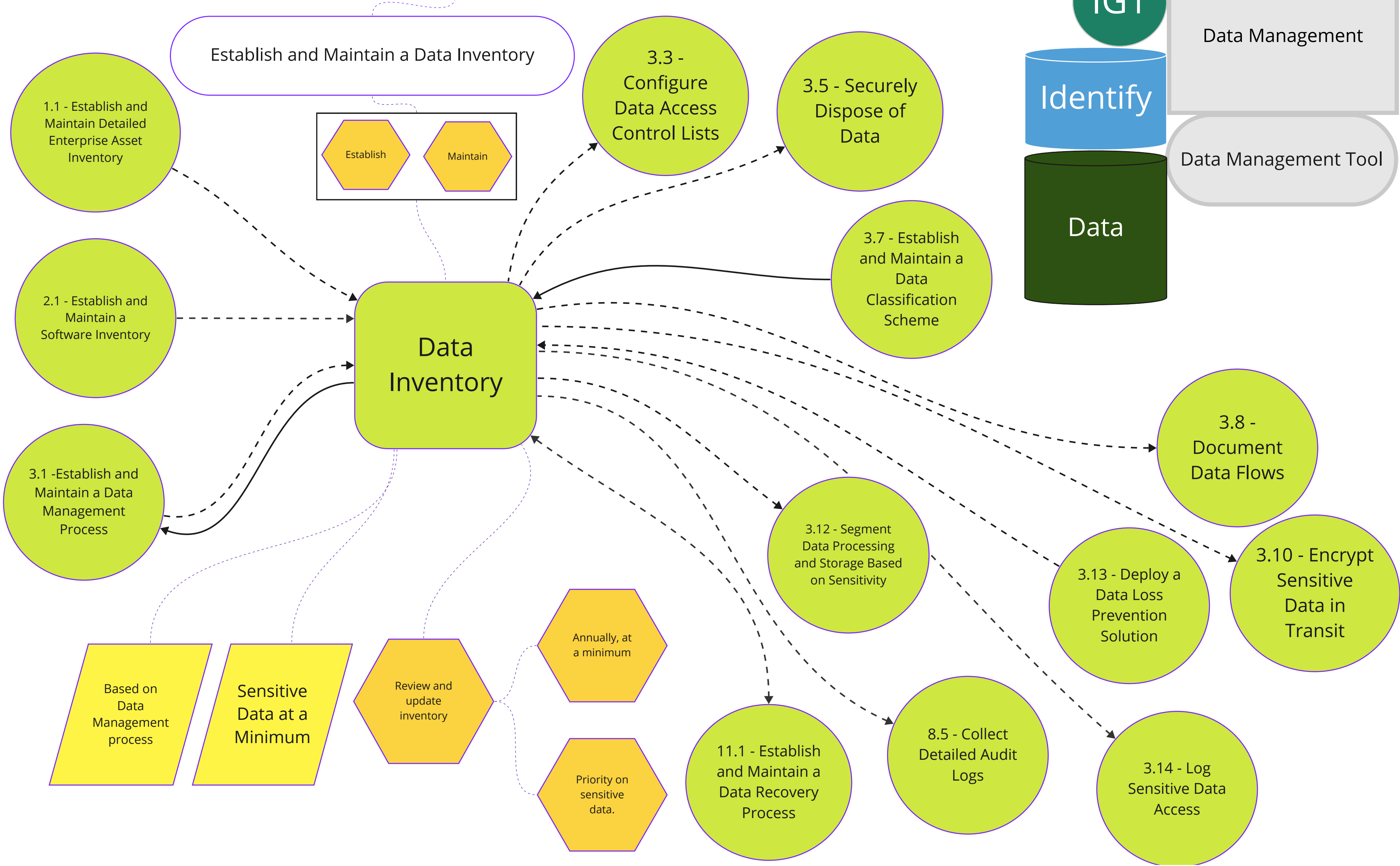
IG1

Identify

Data

Data Management

Data Management Tool



Establish and Maintain a Data Inventory

Establish

Maintain

Data Inventory

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

3.1 -Establish and Maintain a Data Management Process

3.3 - Configure Data Access Control Lists

3.5 - Securely Dispose of Data

3.7 - Establish and Maintain a Data Classification Scheme

3.8 - Document Data Flows

3.10 - Encrypt Sensitive Data in Transit

3.12 - Segment Data Processing and Storage Based on Sensitivity

3.13 - Deploy a Data Loss Prevention Solution

3.14 - Log Sensitive Data Access

8.5 - Collect Detailed Audit Logs

11.1 - Establish and Maintain a Data Recovery Process

Based on Data Management process

Sensitive Data at a Minimum

Review and update inventory

Annually, at a minimum

Priority on sensitive data.

Group Validated

3.3

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.

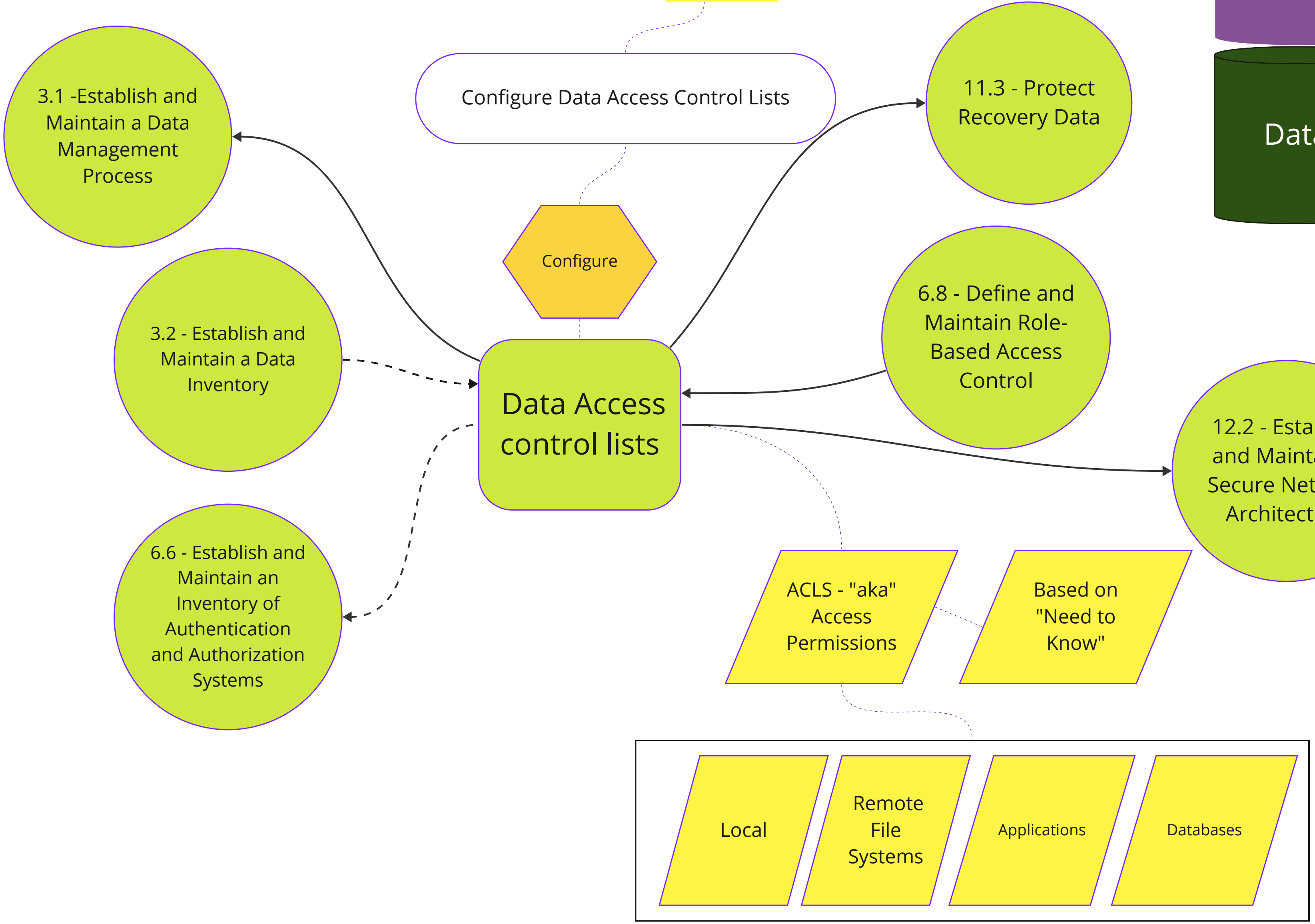
IG1

Protect

Data

Account and Access Control Management

Identity and Access Management Tool


Configure Data Access Control Lists
Configure
Data Access control lists
3.1 -Establish and Maintain a Data Management Process
3.2 - Establish and Maintain a Data Inventory
6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems
11.3 - Protect Recovery Data
6.8 - Define and Maintain Role-Based Access Control
12.2 - Establish and Maintain a Secure Network Architecture
ACLS - "aka" Access Permissions
Based on "Need to Know"
Local
Remote File Systems
Applications
Databases

Group Validated

3.4

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

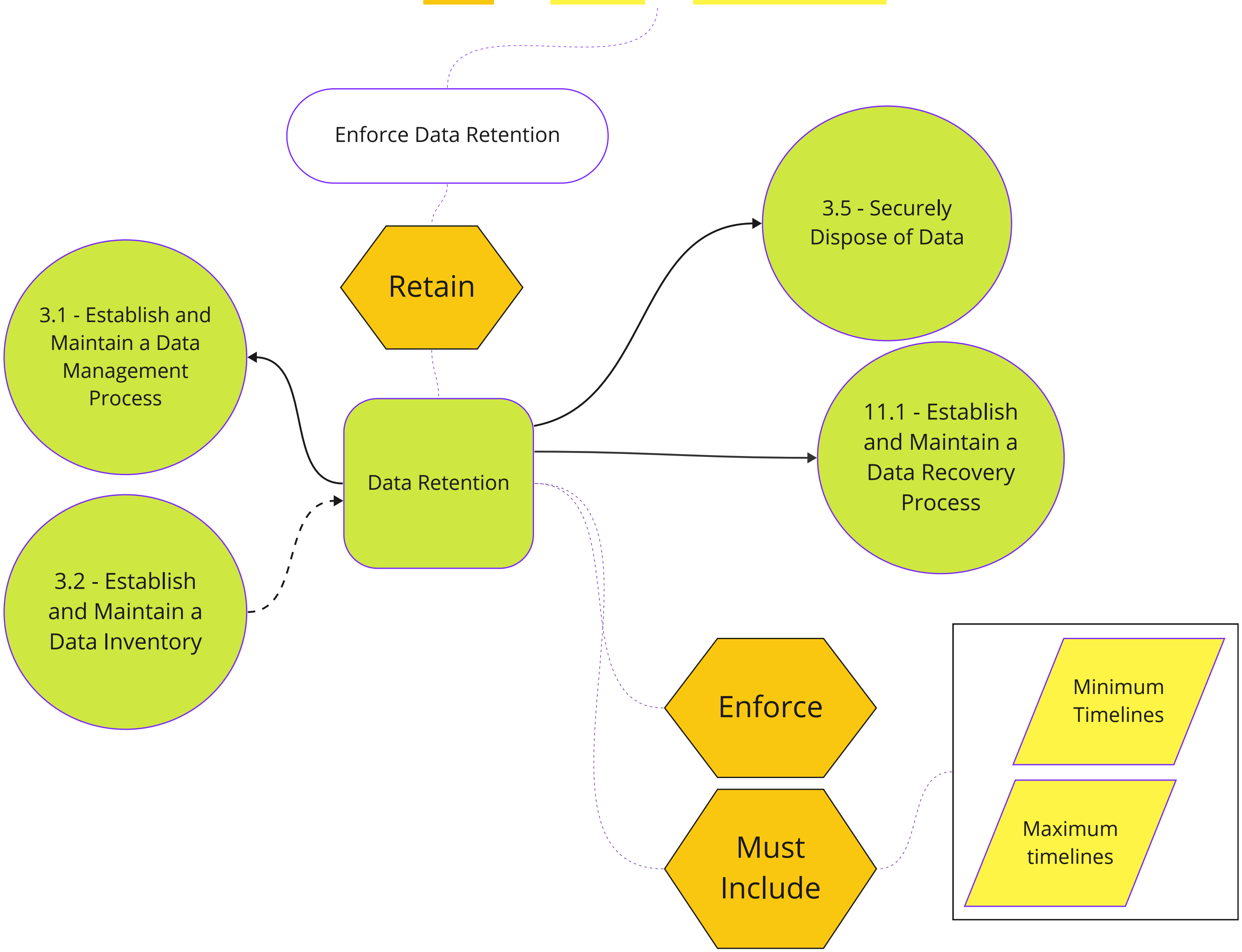
IG1

Protect

Data

Account and Access Control Management

Identity and Access Management Tool



Enforce Data Retention

Retain

Data Retention

3.1 - Establish and Maintain a Data Management Process

3.2 - Establish and Maintain a Data Inventory

3.5 - Securely Dispose of Data

11.1 - Establish and Maintain a Data Recovery Process

Enforce

Must Include

Minimum Timelines

Maximum timelines

Group Validated

3.5

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.

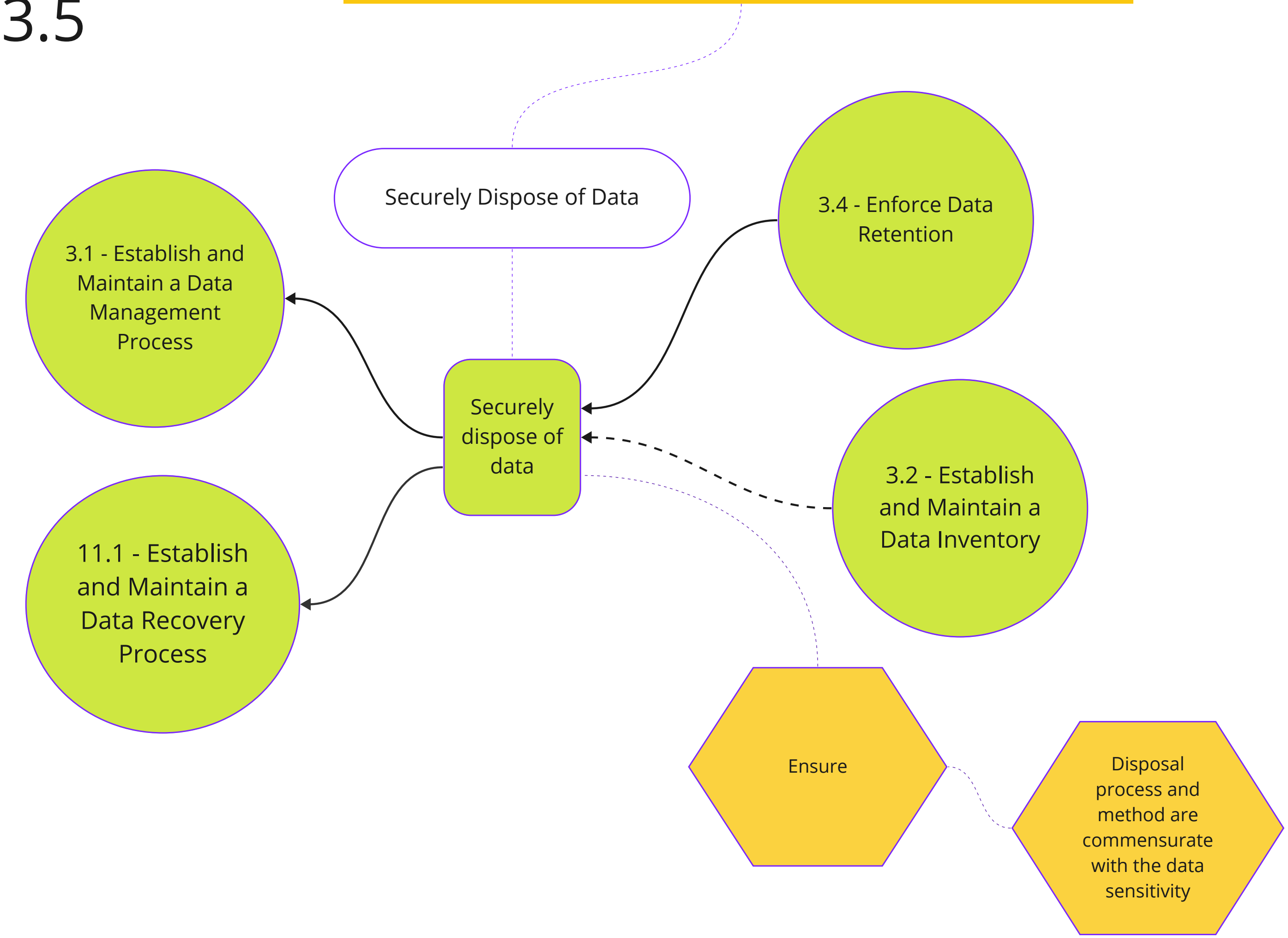
IG1

Data Management

Protect

Data

Data Disposal Tool



Securely Dispose of Data

Securely dispose of data

3.1 - Establish and Maintain a Data Management Process

11.1 - Establish and Maintain a Data Recovery Process

3.4 - Enforce Data Retention

3.2 - Establish and Maintain a Data Inventory

Ensure

Disposal process and method are commensurate with the data sensitivity

Group Validated

3.6

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

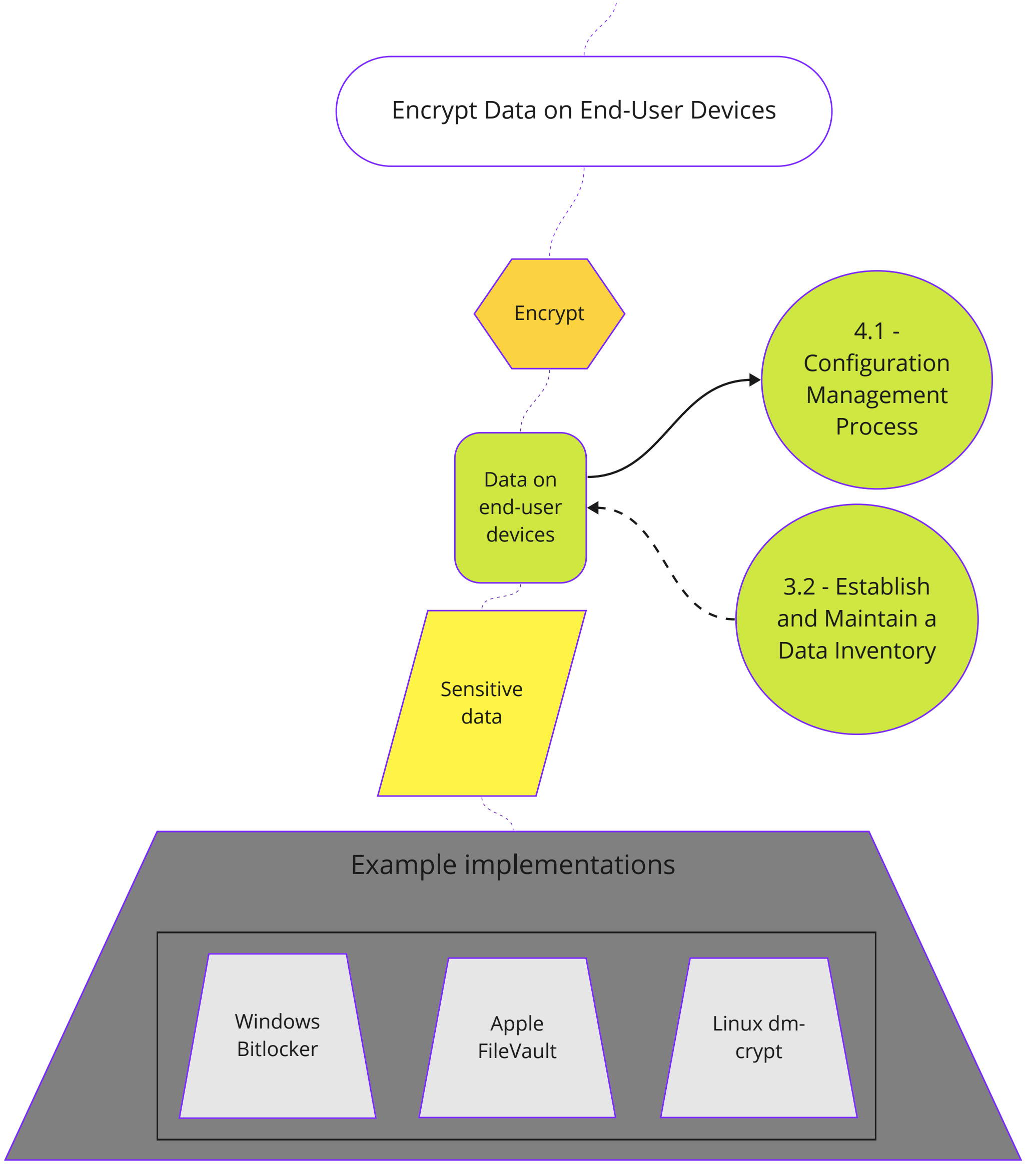
IG1

Data Management

Protect

Encryption Tool

Data



Encrypt Data on End-User Devices

Encrypt

Data on end-user devices

4.1 - Configuration Management Process

3.2 - Establish and Maintain a Data Inventory

Sensitive data

Example implementations

Windows Bitlocker

Apple FileVault

Linux dm-crypt

Group Validated

3.7

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.

Process Oriented Safeguard

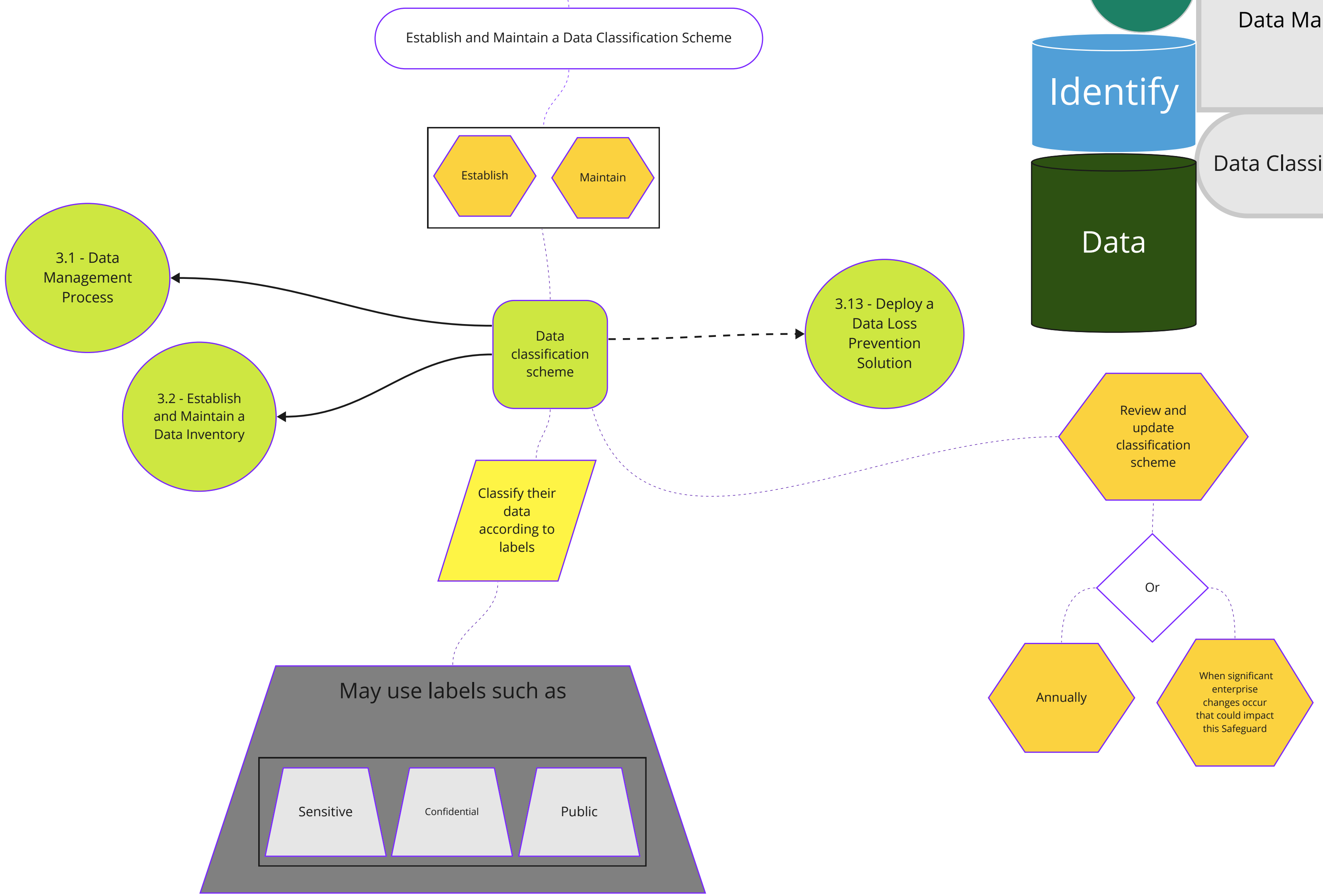
IG2

Data Management

Identify

Data Classification Tool

Data



Establish and Maintain a Data Classification Scheme

Establish

Maintain

Data classification scheme

3.1 - Data Management Process

3.2 - Establish and Maintain a Data Inventory

3.13 - Deploy a Data Loss Prevention Solution

Classify their data according to labels

May use labels such as

Sensitive

Confidential

Public

Review and update classification scheme

Or

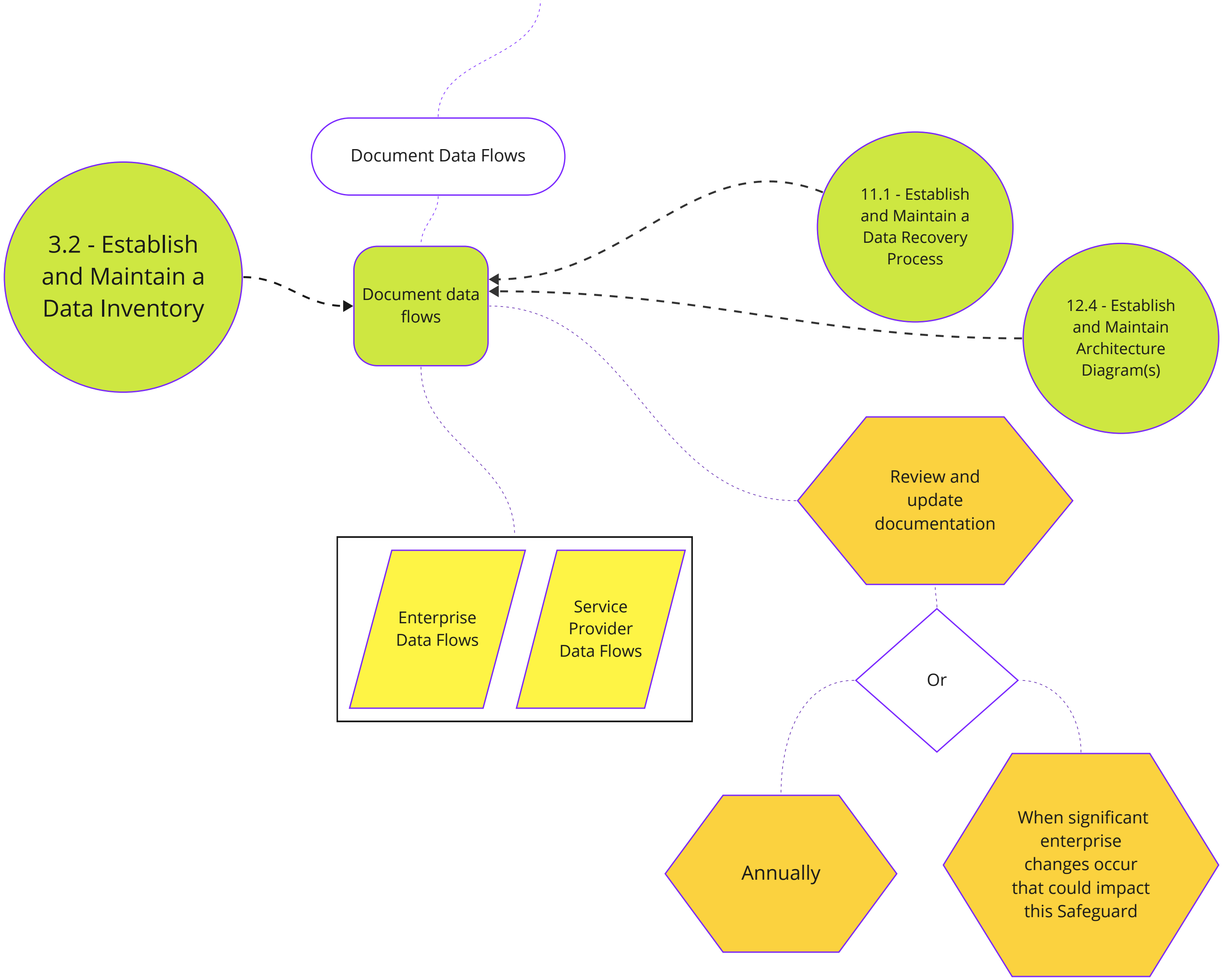
Annually

When significant enterprise changes occur that could impact this Safeguard

Group Validated

3.8

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.



Document Data Flows

3.2 - Establish and Maintain a Data Inventory

Document data flows

11.1 - Establish and Maintain a Data Recovery Process

12.4 - Establish and Maintain Architecture Diagram(s)

Review and update documentation

Enterprise Data Flows

Service Provider Data Flows

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Process Oriented Safeguard

IG2

Data Management

Identify

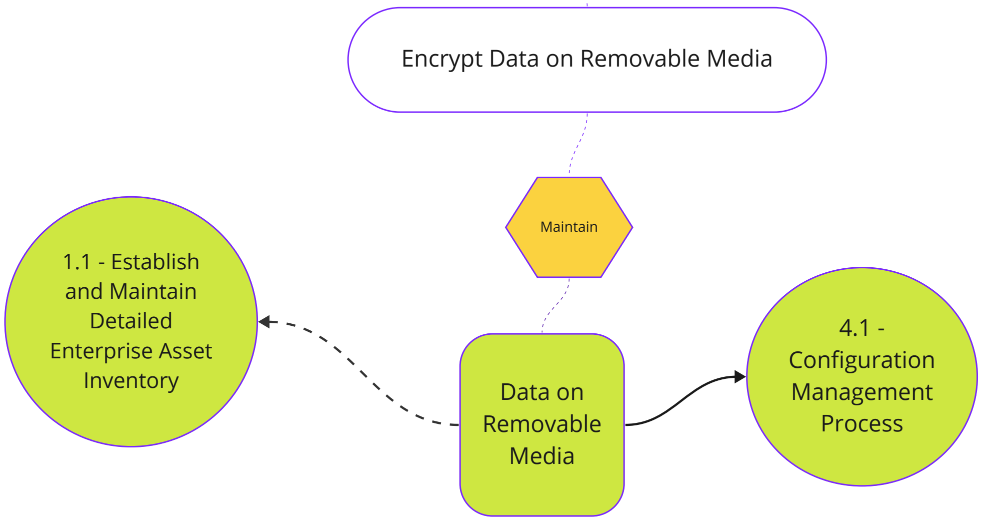
Data

Data Flow Diagramming Tool

Group Validated

3.9

Encrypt Data on Removable Media



Encrypt Data on Removable Media

Maintain

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

Data on Removable Media

4.1 - Configuration Management Process

IG2

Data Management

Protect

Encryption Tool

Data

Group Validated

3.10

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

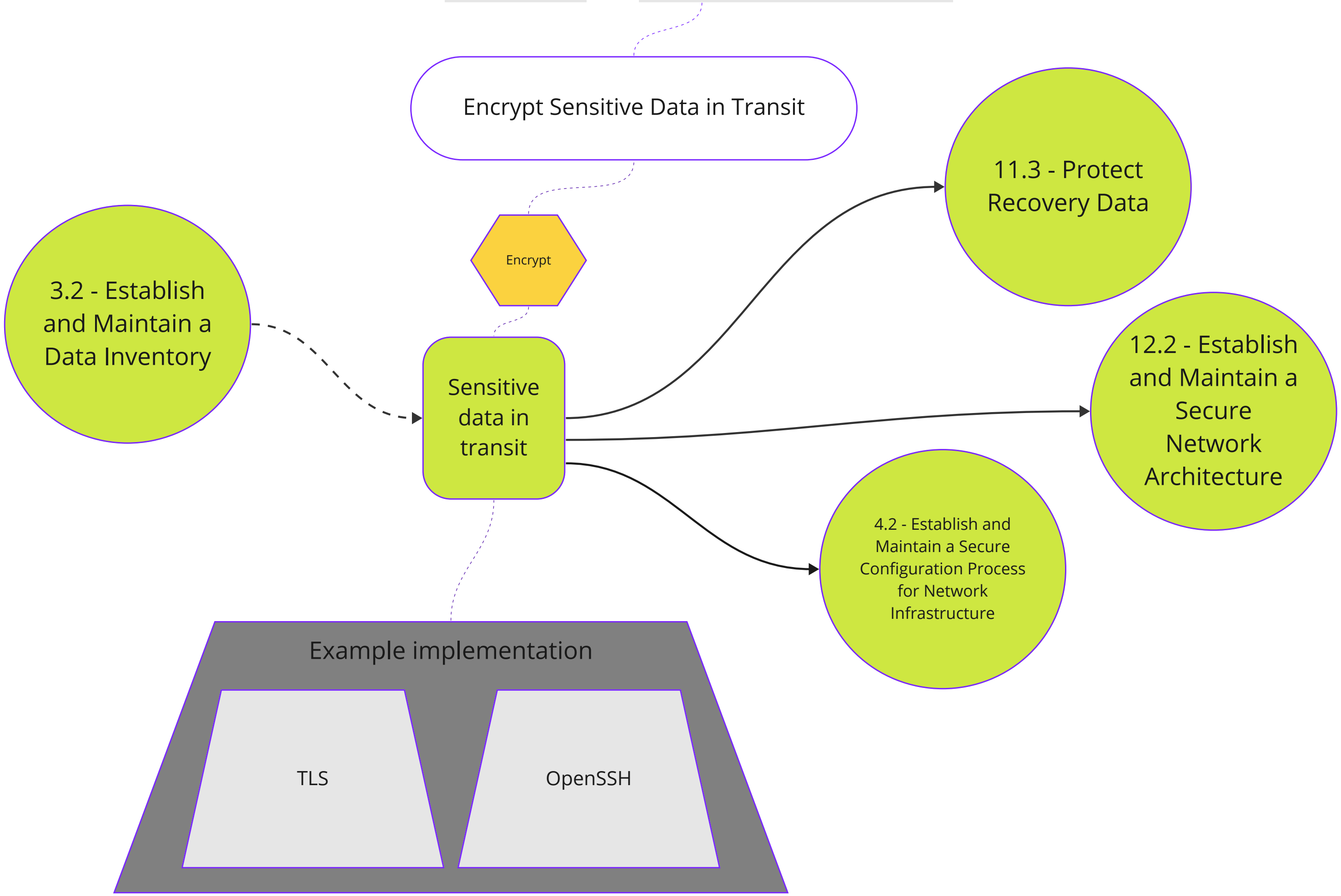
IG2

Data Management

Protect

Data

Encryption Tool



Encrypt Sensitive Data in Transit

Encrypt

3.2 - Establish and Maintain a Data Inventory

Sensitive data in transit

11.3 - Protect Recovery Data

12.2 - Establish and Maintain a Secure Network Architecture

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

Example implementation

TLS

OpenSSH

Group Validated

3.11

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.

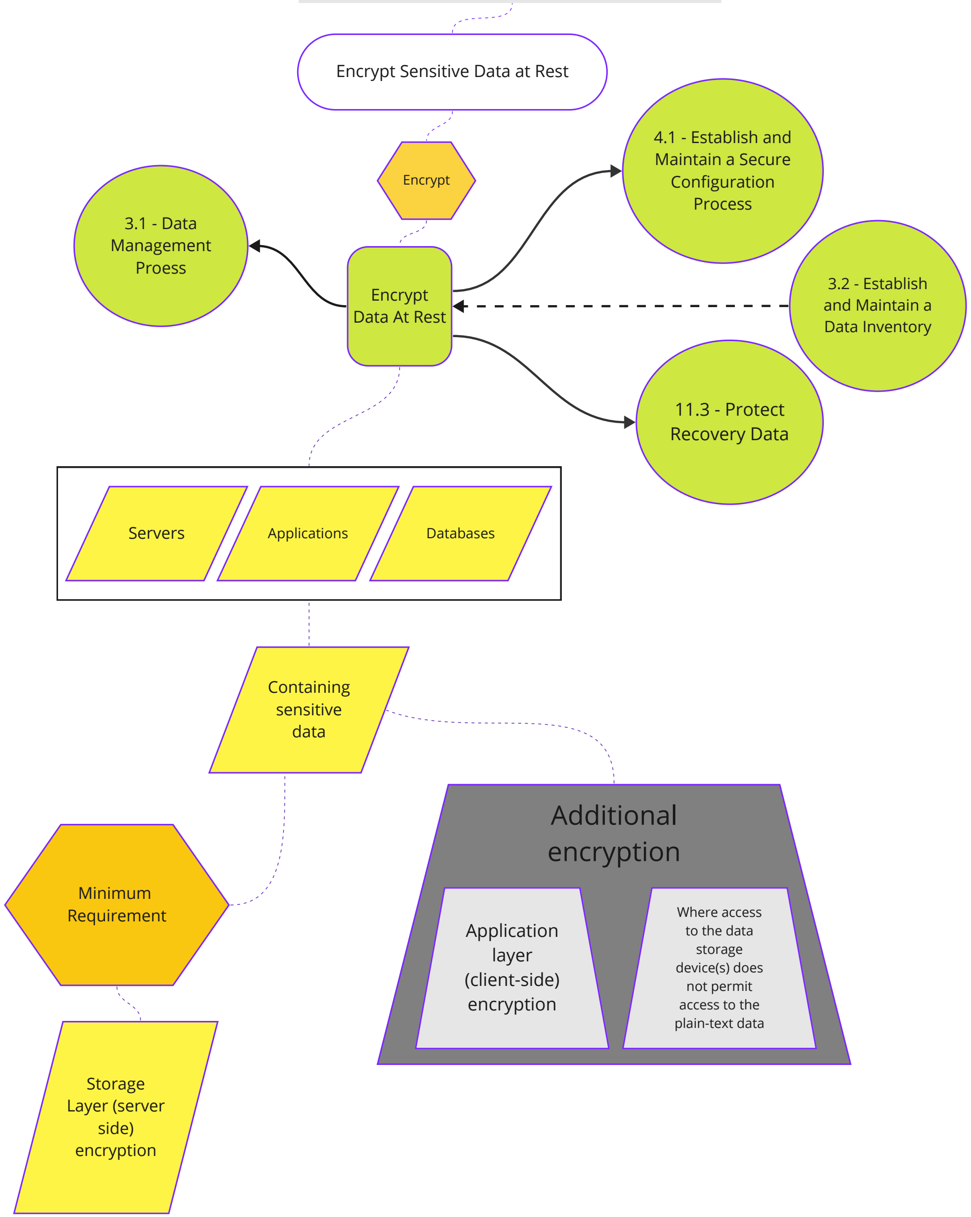
IG2

Data Management

Protect

Encryption Tool

Data



Encrypt Sensitive Data at Rest

Encrypt

3.1 - Data Management Proess

Encrypt Data At Rest

4.1 - Establish and Maintain a Secure Configuration Process

3.2 - Establish and Maintain a Data Inventory

11.3 - Protect Recovery Data

Servers

Applications

Databases

Containing sensitive data

Minimum Requirement

Storage Layer (server side) encryption

Additional encryption

Application layer (client-side) encryption

Where access to the data storage device(s) does not permit access to the plain-text data

Group Validated

3.12

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.

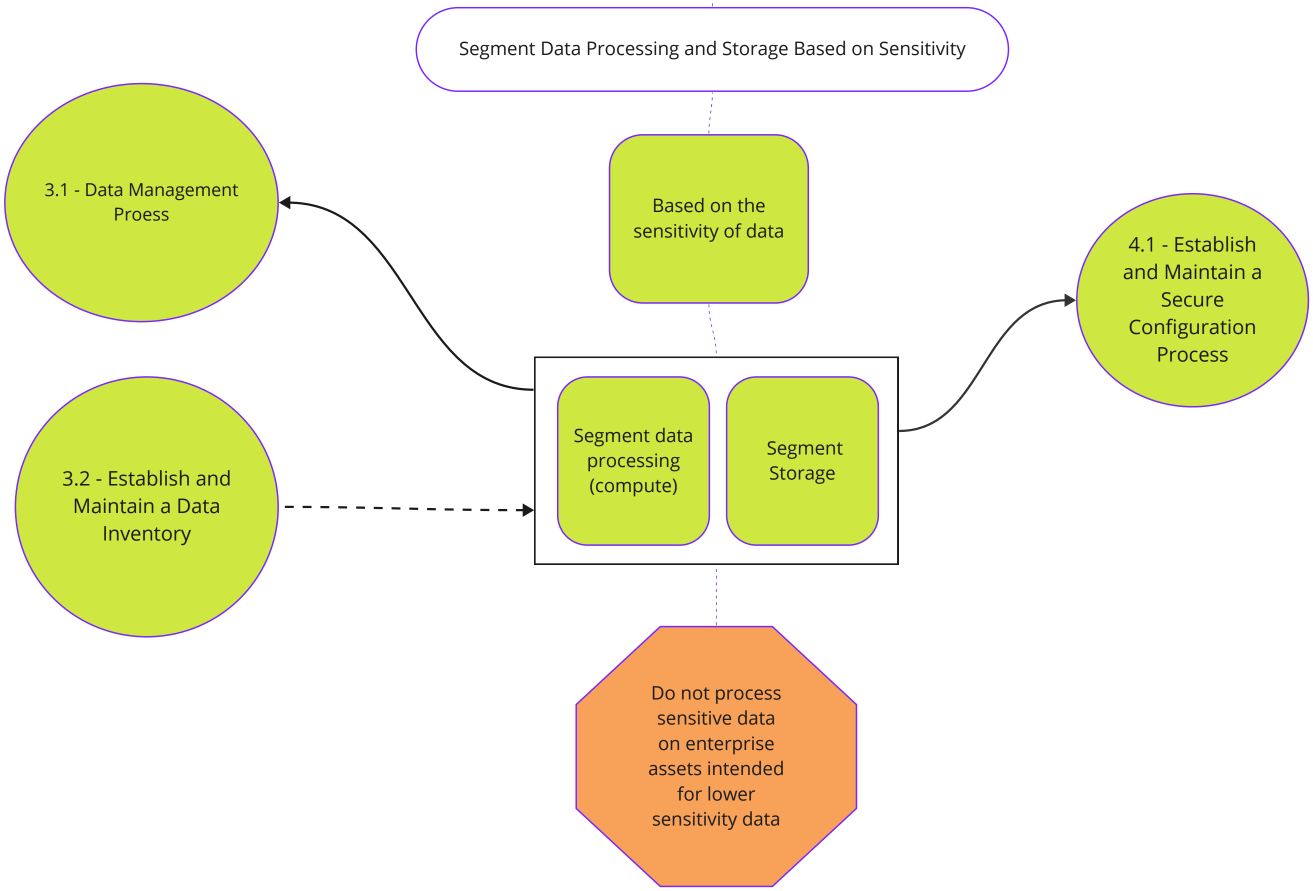
IG2

Secure Configurations

Protect

Secure Configuration Policy/Process

Network



Segment Data Processing and Storage Based on Sensitivity

Based on the sensitivity of data

Segment data processing (compute)

Segment Storage

Do not process sensitive data on enterprise assets intended for lower sensitivity data

3.1 - Data Management Proess

3.2 - Establish and Maintain a Data Inventory

4.1 - Establish and Maintain a Secure Configuration Process

Group Validated

3.13

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.

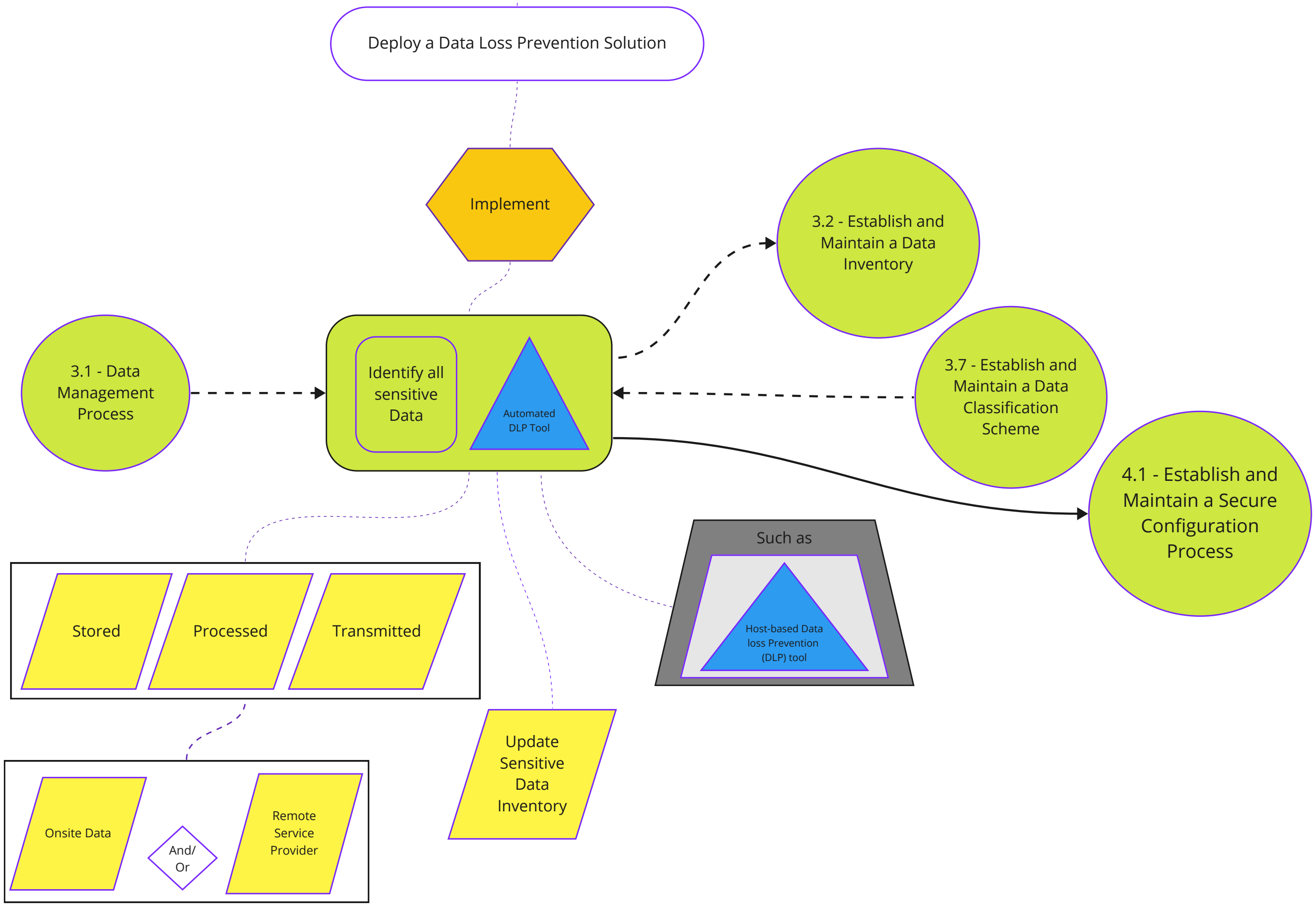
IG3

Protect

Data

Data Management

Data Loss Prevention Tool



Deploy a Data Loss Prevention Solution
Implement
3.1 - Data Management Process
Identify all sensitive Data
Automated DLP Tool
3.2 - Establish and Maintain a Data Inventory
3.7 - Establish and Maintain a Data Classification Scheme
4.1 - Establish and Maintain a Secure Configuration Process
Such as
Host-based Data loss Prevention (DLP) tool
Stored
Processed
Transmitted
Onsite Data
And/ Or
Remote Service Provider
Update Sensitive Data Inventory

Group Validated

3.14

Log sensitive data access, including modification and disposal.

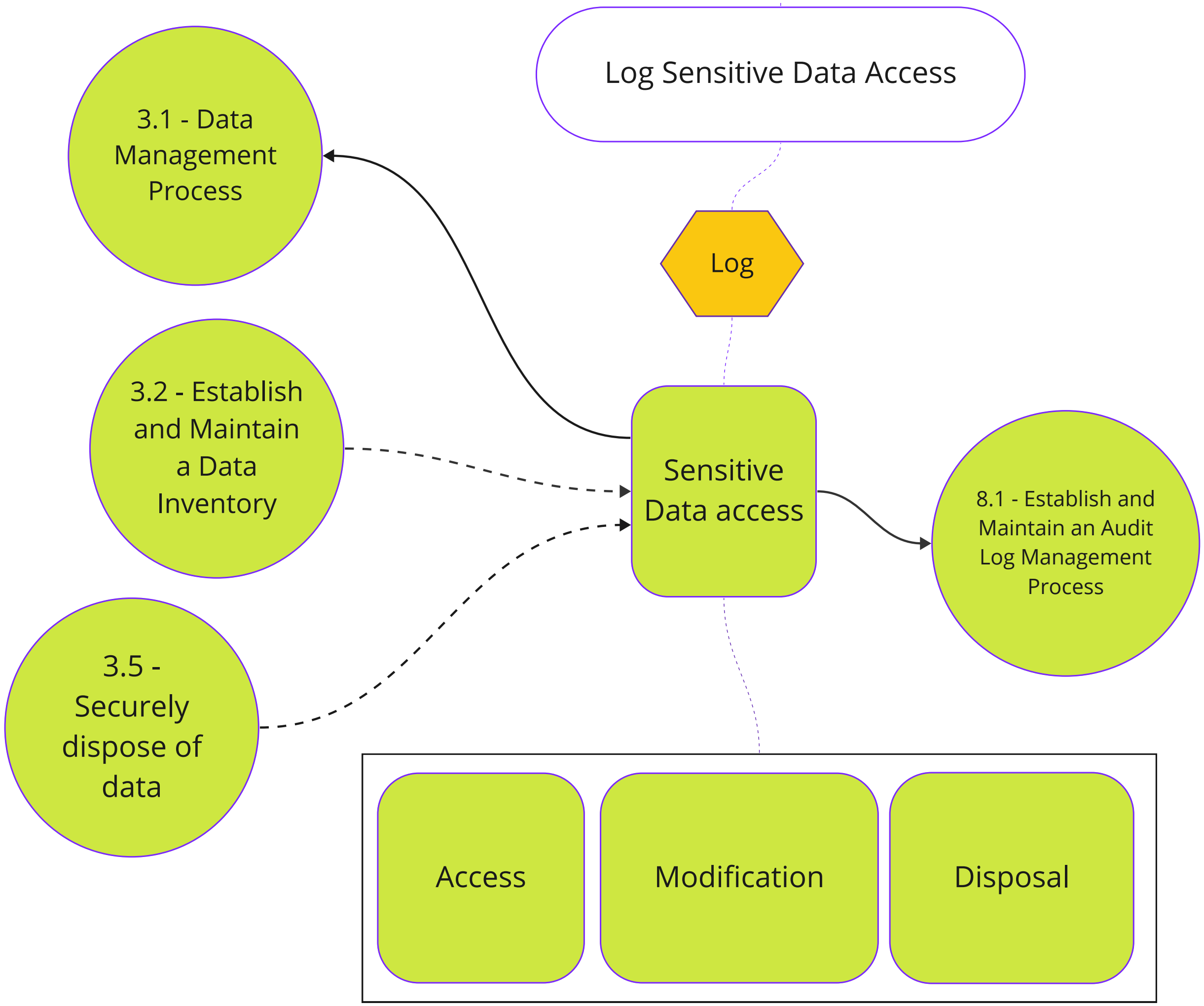
IG3

Protect

Data

Log Management

Log Management Policy/Process



Log Sensitive Data Access

Log

Sensitive Data access

3.1 - Data Management Process

3.2 - Establish and Maintain a Data Inventory

3.5 - Securely dispose of data

8.1 - Establish and Maintain an Audit Log Management Process

Access

Modification

Disposal

CONTROL 04

Secure Configuration of Enterprise Assets and Software

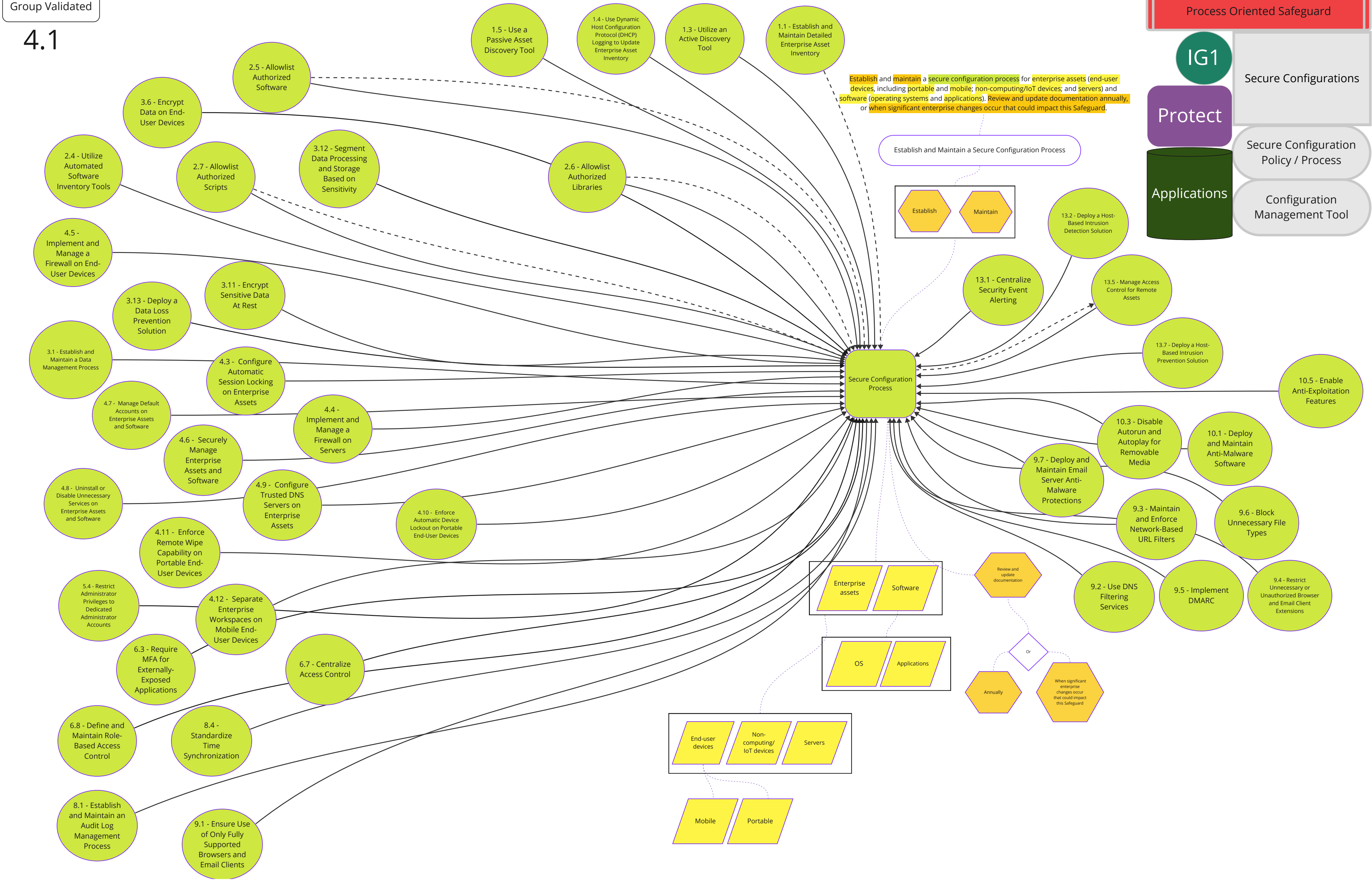
SAFEGUARDS TOTAL 12 | IG1 7/12 | IG2 11/12 | IG3 12/12

Overview

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).

Group Validated

4.1



Process Oriented Safeguard

IG1

Secure Configurations

Protect

Applications

Secure Configuration Policy / Process

Configuration Management Tool

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.

Establish and Maintain a Secure Configuration Process

Establish

Maintain

Secure Configuration Process

Enterprise assets

Software

OS

Applications

End-user devices

Non-computing/ IoT devices

Servers

Mobile

Portable

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

1.5 - Use a Passive Asset Discovery Tool

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

1.3 - Utilize an Active Discovery Tool

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.5 - Allowlist Authorized Software

3.6 - Encrypt Data on End-User Devices

2.4 - Utilize Automated Software Inventory Tools

2.7 - Allowlist Authorized Scripts

3.12 - Segment Data Processing and Storage Based on Sensitivity

2.6 - Allowlist Authorized Libraries

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

3.13 - Deploy a Data Loss Prevention Solution

3.11 - Encrypt Sensitive Data At Rest

3.1 - Establish and Maintain a Data Management Process

4.3 - Configure Automatic Session Locking on Enterprise Assets

4.7 - Manage Default Accounts on Enterprise Assets and Software

4.4 - Implement and Manage a Firewall on Servers

4.6 - Securely Manage Enterprise Assets and Software

4.8 - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

4.9 - Configure Trusted DNS Servers on Enterprise Assets

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

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

5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts

4.12 - Separate Enterprise Workspaces on Mobile End-User Devices

6.3 - Require MFA for Externally-Exposed Applications

6.7 - Centralize Access Control

6.8 - Define and Maintain Role-Based Access Control

8.4 - Standardize Time Synchronization

8.1 - Establish and Maintain an Audit Log Management Process

9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients

13.2 - Deploy a Host-Based Intrusion Detection Solution

13.1 - Centralize Security Event Alerting

13.5 - Manage Access Control for Remote Assets

13.7 - Deploy a Host-Based Intrusion Prevention Solution

10.5 - Enable Anti-Exploitation Features

10.3 - Disable Autorun and Autoplay for Removable Media

10.1 - Deploy and Maintain Anti-Malware Software

9.7 - Deploy and Maintain Email Server Anti-Malware Protections

9.3 - Maintain and Enforce Network-Based URL Filters

9.6 - Block Unnecessary File Types

9.2 - Use DNS Filtering Services

9.5 - Implement DMARC

9.4 - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Group Validated

4.2

Process Oriented Safeguard

IG1

Secure Configurations

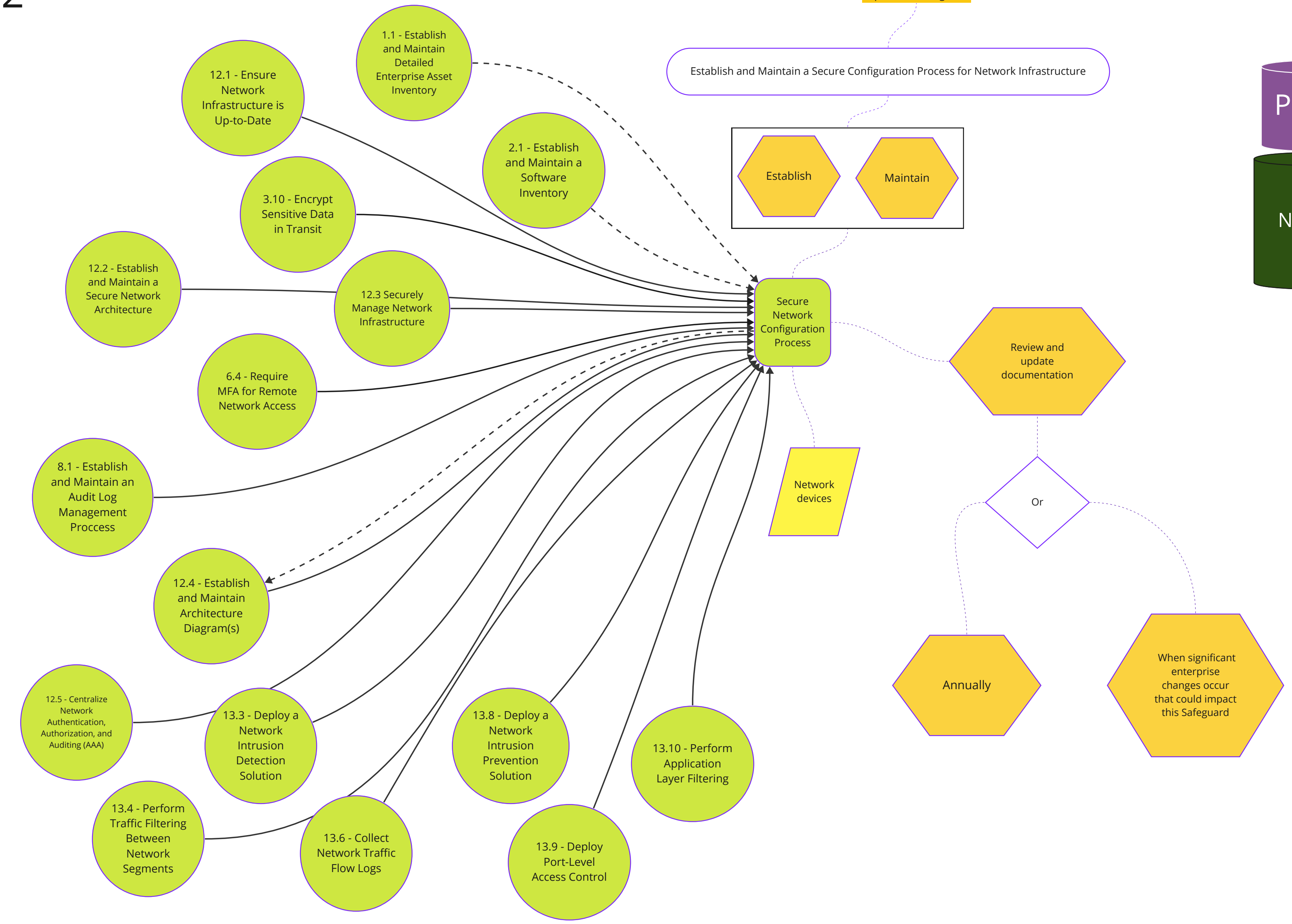
Protect

Network

Secure Configuration Policy / Process

Configuration Management Tool

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.



Establish and Maintain a Secure Configuration Process for Network Infrastructure

Establish

Maintain

Secure Network Configuration Process

Network devices

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

12.1 - Ensure Network Infrastructure is Up-to-Date

2.1 - Establish and Maintain a Software Inventory

3.10 - Encrypt Sensitive Data in Transit

12.2 - Establish and Maintain a Secure Network Architecture

12.3 Securely Manage Network Infrastructure

6.4 - Require MFA for Remote Network Access

8.1 - Establish and Maintain an Audit Log Management Proccess

12.4 - Establish and Maintain Architecture Diagram(s)

12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA)

13.3 - Deploy a Network Intrusion Detection Solution

13.8 - Deploy a Network Intrusion Prevention Solution

13.10 - Perform Application Layer Filtering

13.4 - Perform Traffic Filtering Between Network Segments

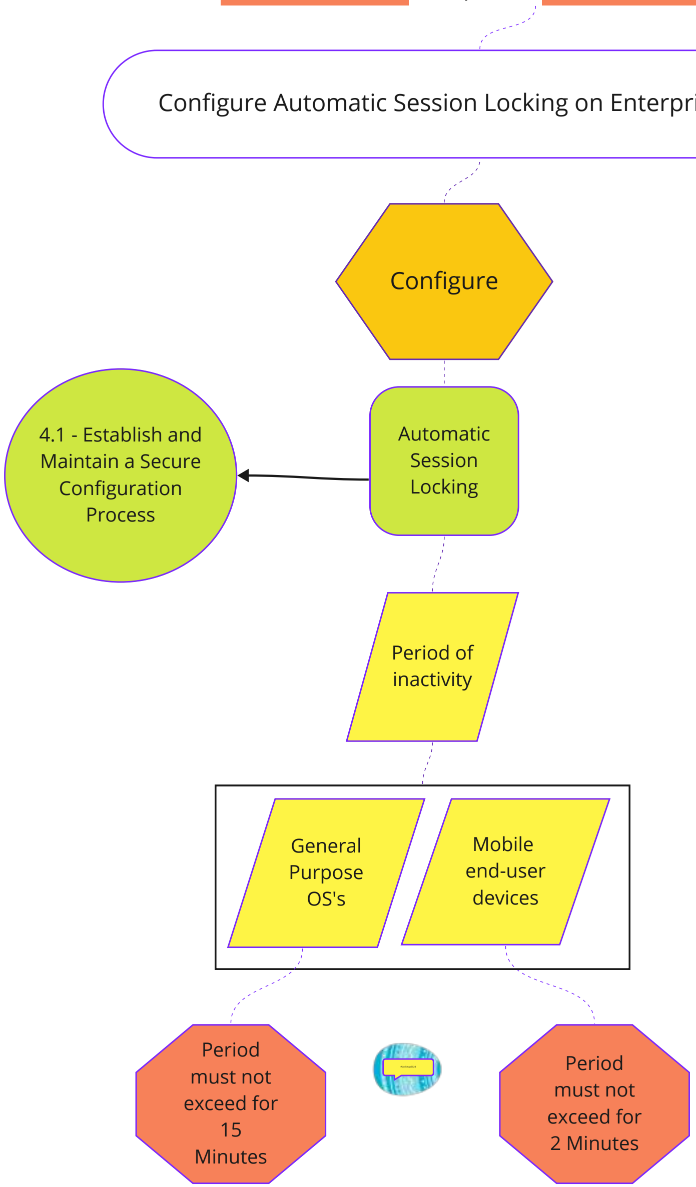
13.6 - Collect Network Traffic Flow Logs

13.9 - Deploy Port-Level Access Control

Group Validated

4.3

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.



Configure Automatic Session Locking on Enterprise Assets

Configure

Automatic Session Locking

4.1 - Establish and Maintain a Secure Configuration Process

Period of inactivity

General Purpose OS's

Mobile end-user devices

Period must not exceed for 15 Minutes

Period must not exceed for 2 Minutes

IG1

Secure Configurations

Protect

Configuration Management Tool

Users

OS Dependent

Group Validated

4.4

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

IG1

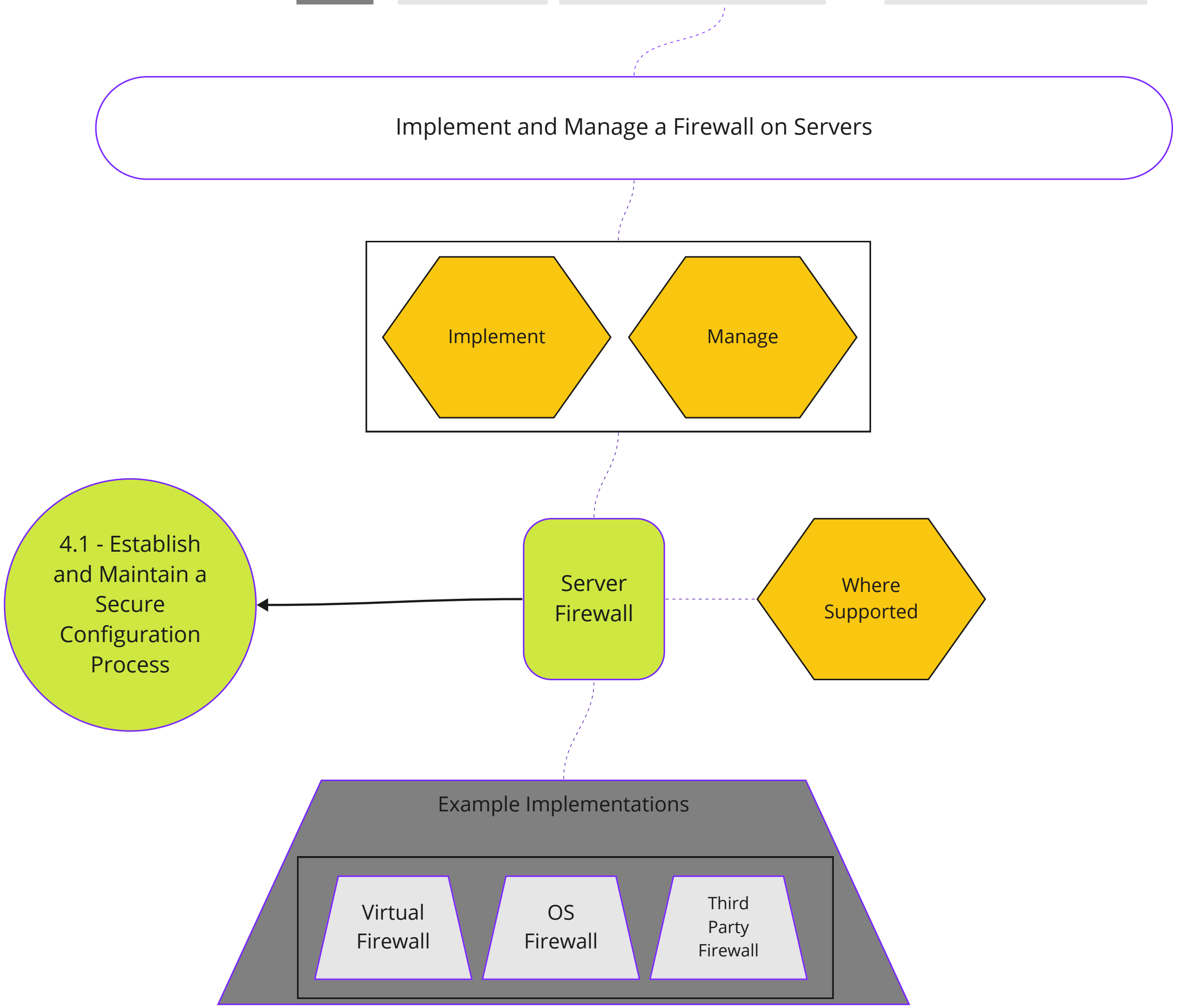
Secure Configurations

Protect

Devices

Firewall

Potentially OS Dependent



Implement and Manage a Firewall on Servers

Implement

Manage

4.1 - Establish and Maintain a Secure Configuration Process

Server Firewall

Where Supported

Example Implementations

Virtual Firewall

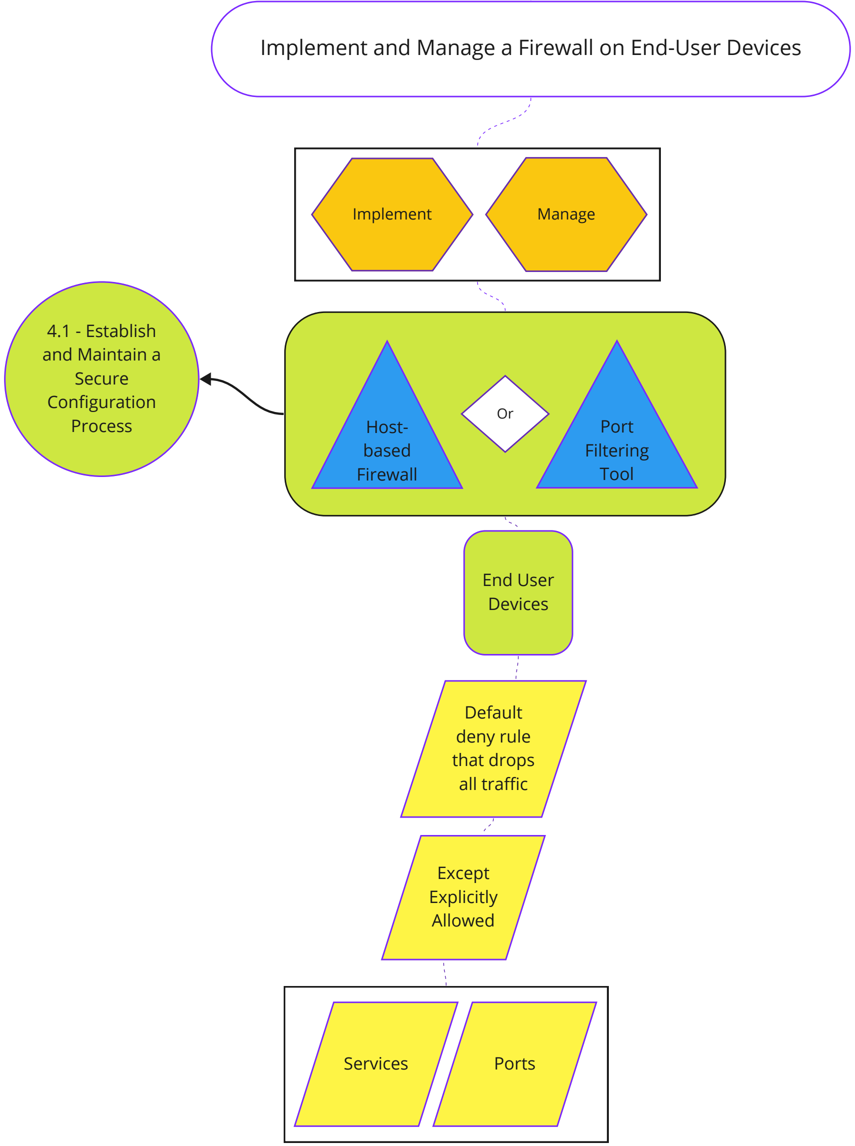
OS Firewall

Third Party Firewall

Group Validated

4.5

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.



Implement and Manage a Firewall on End-User Devices

Implement

Manage

Host-based Firewall

Or

Port Filtering Tool

4.1 - Establish and Maintain a Secure Configuration Process

End User Devices

Default deny rule that drops all traffic

Except Explicitly Allowed

Services

Ports

IG1

Secure Configurations

Protect

Devices

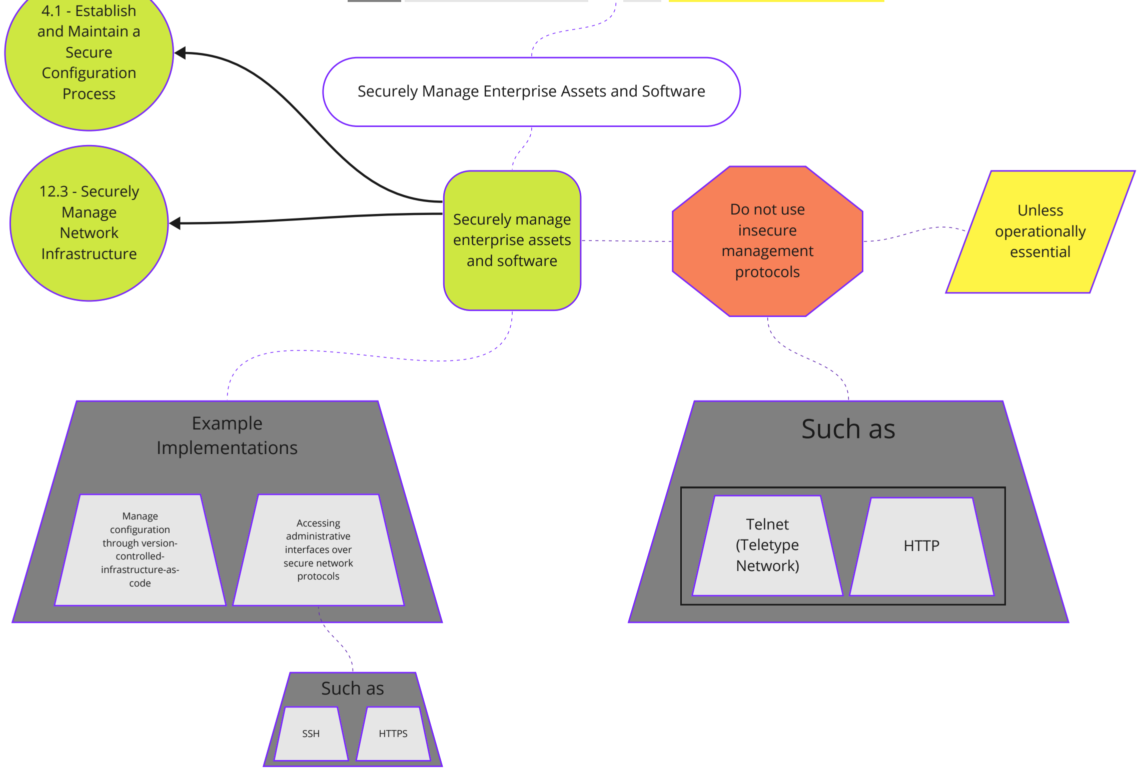
Firewall

OS Dependent

Group Validated

4.6

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.



Securely Manage Enterprise Assets and Software

4.1 - Establish and Maintain a Secure Configuration Process

12.3 - Securely Manage Network Infrastructure

Securely manage enterprise assets and software

Do not use insecure management protocols

Unless operationally essential

Example Implementations

Manage configuration through version-controlled-infrastructure-as-code

Accessing administrative interfaces over secure network protocols

Such as

SSH

HTTPS

Such as

Telnet (Teletype Network)

HTTP

IG1

Secure Configurations

Protect

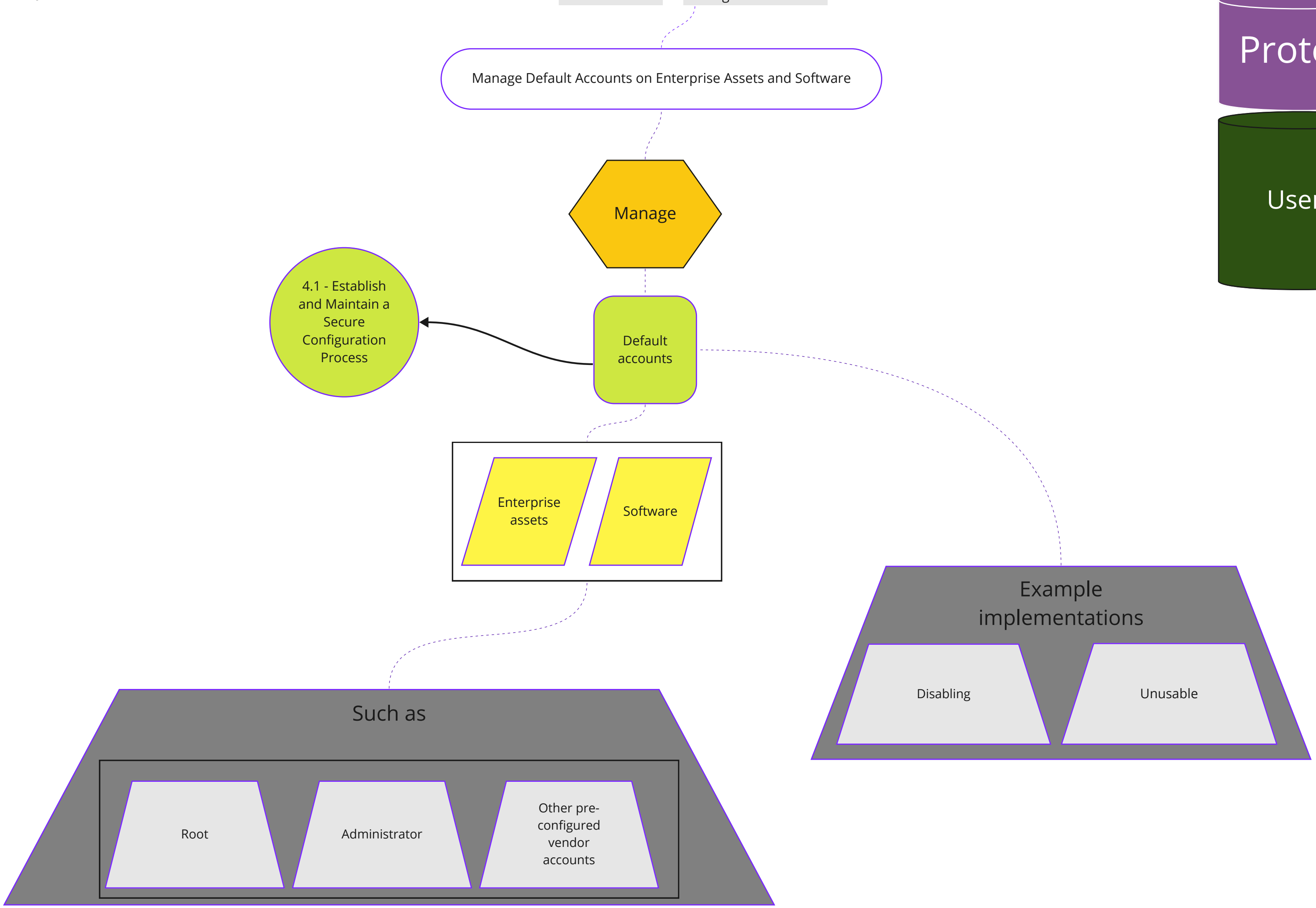
Configuration Management Tool

Network

Group Validated

4.7

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.



Manage Default Accounts on Enterprise Assets and Software

Manage

Default accounts

4.1 - Establish and Maintain a Secure Configuration Process

Enterprise assets

Software

Such as

Root

Administrator

Other pre-configured vendor accounts

Example implementations

Disabling

Unusable

IG1

Secure Configurations

Protect

Users

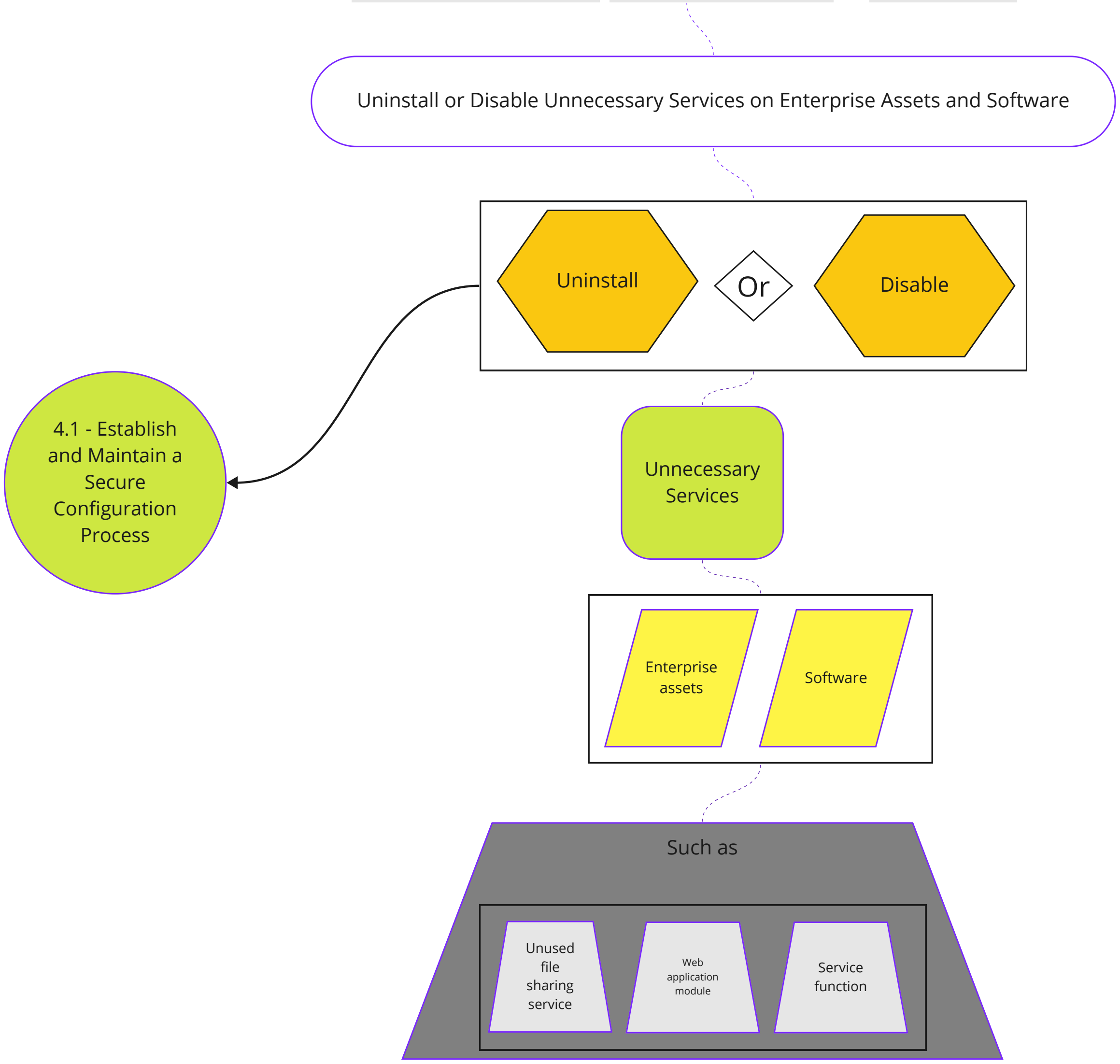
Configuration Management Tool

OS Dependent

Group Validated

4.8

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



Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Uninstall

Or

Disable

4.1 - Establish and Maintain a Secure Configuration Process

Unnecessary Services

Enterprise assets

Software

Such as

Unused file sharing service

Web application module

Service function

IG2

Secure Configurations

Protect

Configuration Management Tool

Devices

OS Dependent

Group Validated

4.9

IG2

Secure Configurations

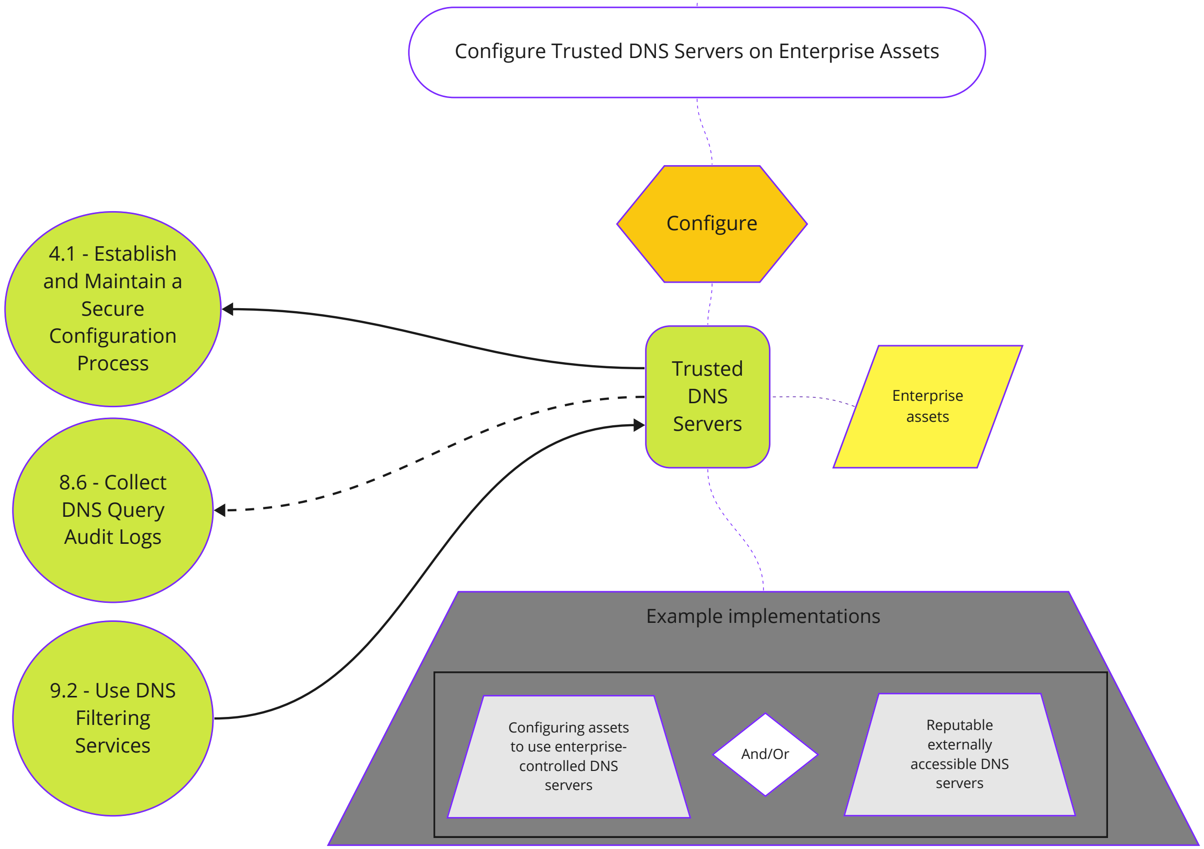
Protect

Configuration Management Tool

Devices

OS Dependent

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.



Configure Trusted DNS Servers on Enterprise Assets

Configure

Trusted DNS Servers

Enterprise assets

4.1 - Establish and Maintain a Secure Configuration Process

8.6 - Collect DNS Query Audit Logs

9.2 - Use DNS Filtering Services

Example implementations

Configuring assets to use enterprise-controlled DNS servers

And/Or

Reputable externally accessible DNS servers

Group Validated

4.10

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.

IG2

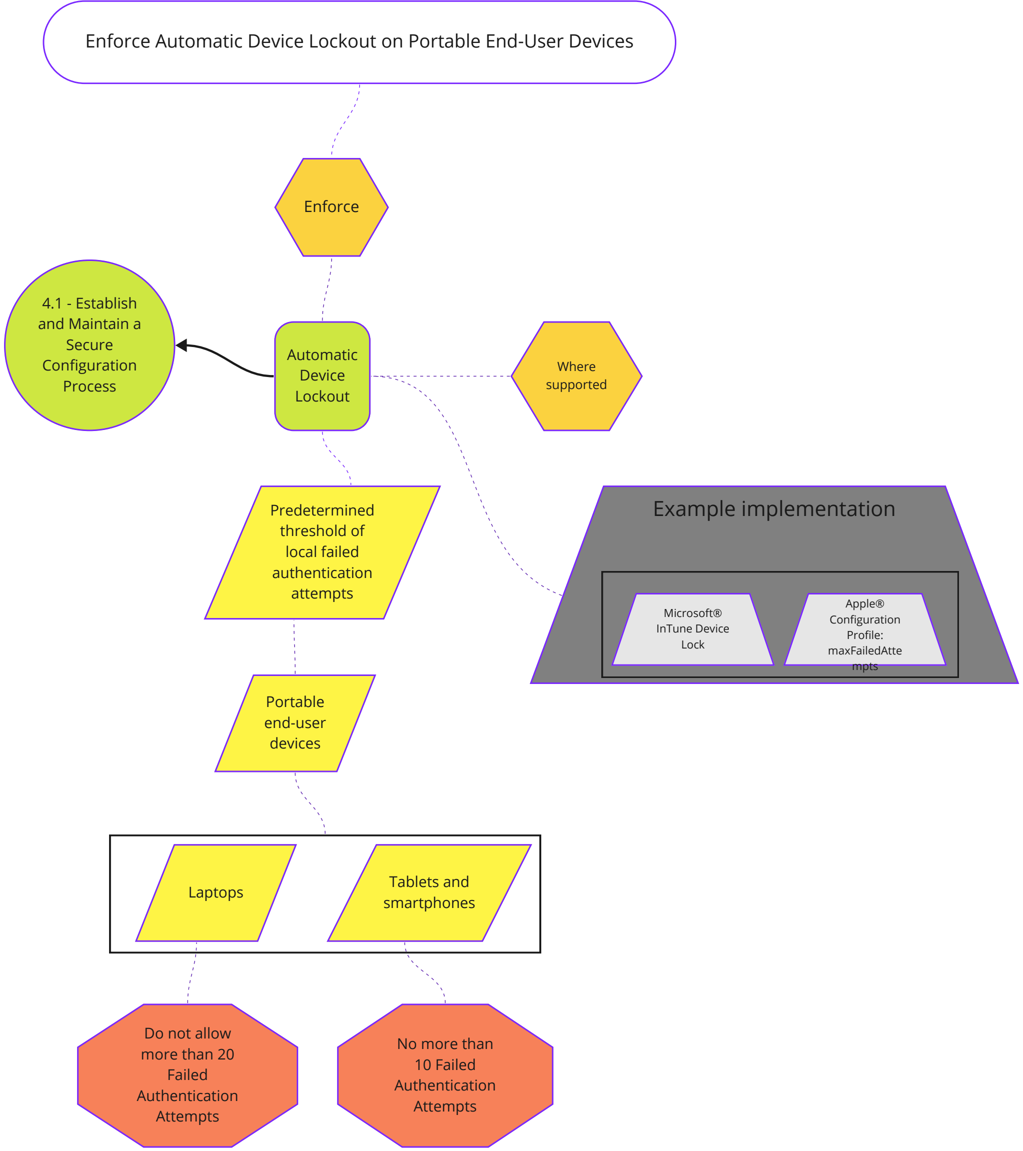
Secure Configurations

Respond

Configuration Management Tool

Devices

OS Dependent



Enforce Automatic Device Lockout on Portable End-User Devices

Enforce

Automatic Device Lockout

4.1 - Establish and Maintain a Secure Configuration Process

Where supported

Example implementation

Microsoft® InTune Device Lock

Apple® Configuration Profile: maxFailedAttempts

Predetermined threshold of local failed authentication attempts

Portable end-user devices

Laptops

Tablets and smartphones

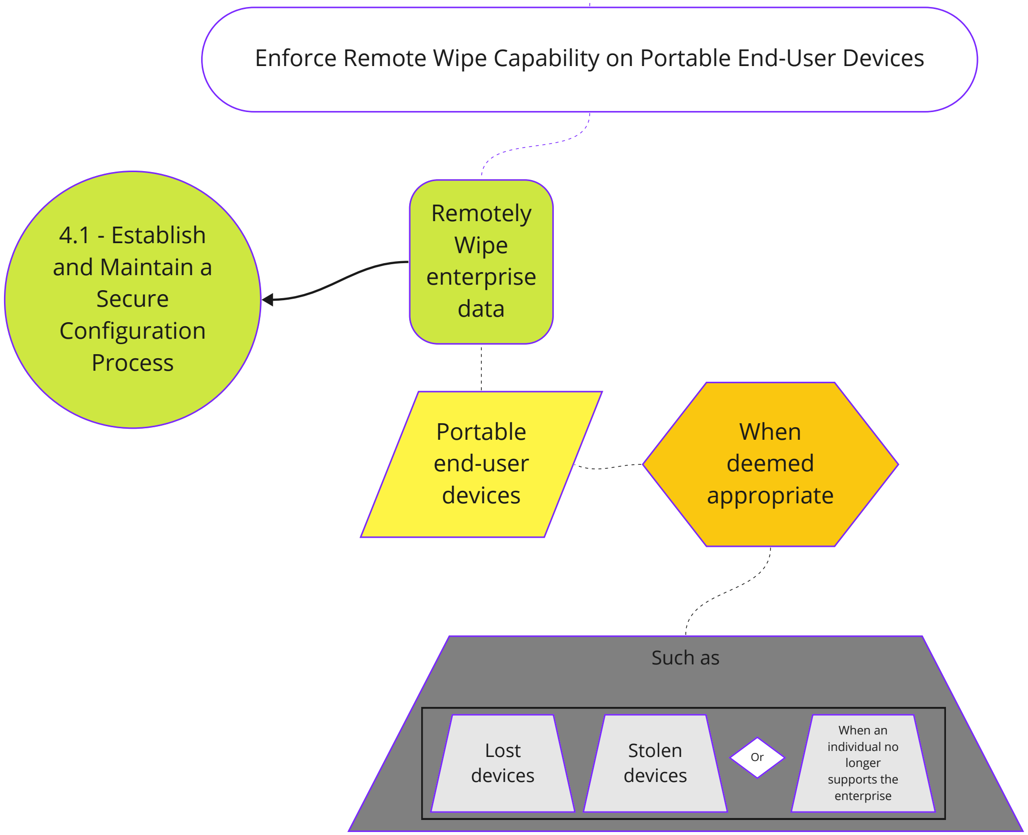
Do not allow more than 20 Failed Authentication Attempts

No more than 10 Failed Authentication Attempts

Group Validated

4.11

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.



Enforce Remote Wipe Capability on Portable End-User Devices

Remotely Wipe enterprise data

4.1 - Establish and Maintain a Secure Configuration Process

Portable end-user devices

When deemed appropriate

Such as

Lost devices

Stolen devices

Or

When an individual no longer supports the enterprise

IG2

Secure Configurations

Protect

Configuration Management Tool

Devices

OS Dependent

Group Validated

4.12

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

IG3

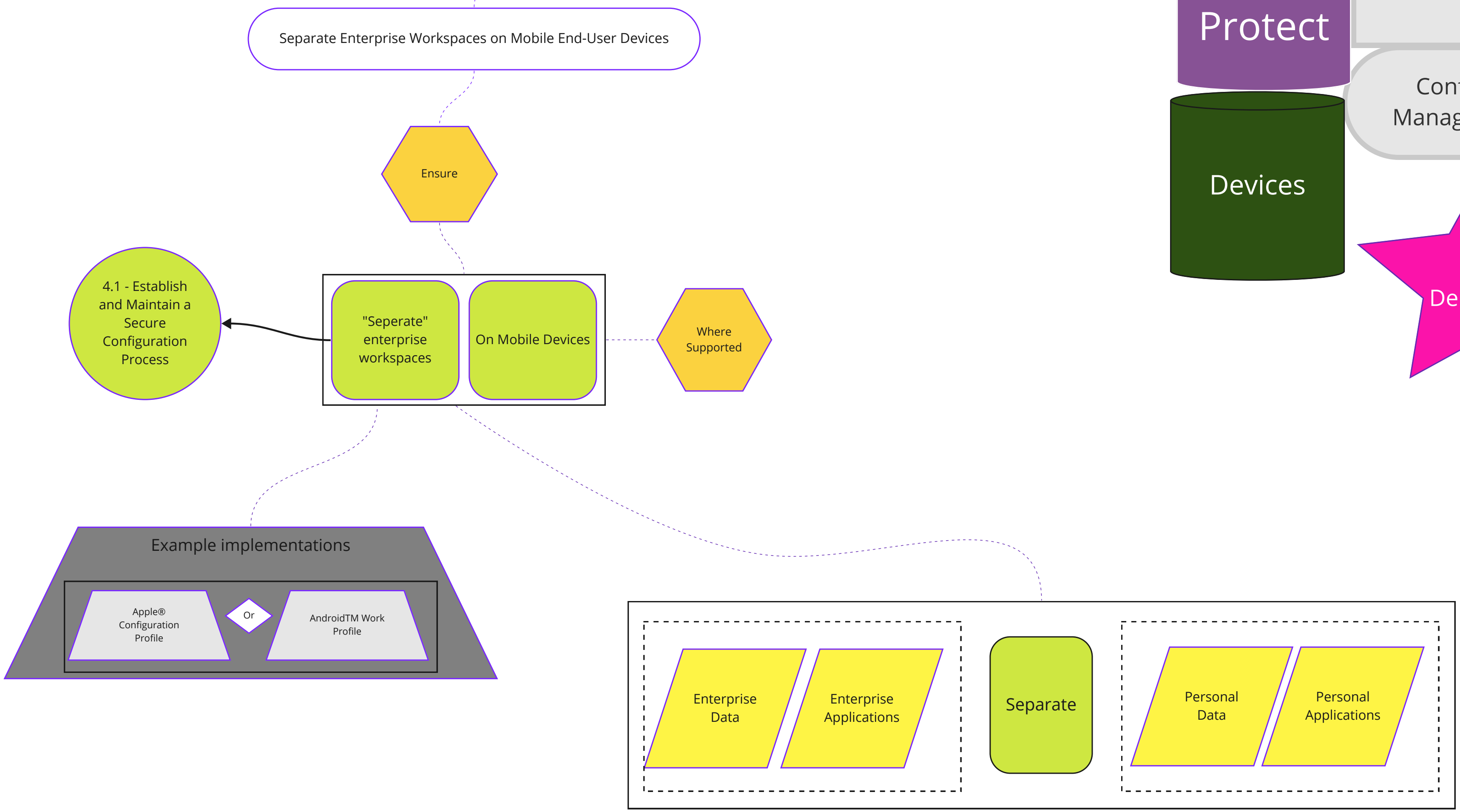
Protect

Devices

Secure Configurations

Configuration Management Tool

OS Dependent



Separate Enterprise Workspaces on Mobile End-User Devices

Ensure

4.1 - Establish and Maintain a Secure Configuration Process

"Seperate" enterprise workspaces

On Mobile Devices

Where Supported

Example implementations

Apple® Configuration Profile

Or

AndroidTM Work Profile

Enterprise Data

Enterprise Applications

Separate

Personal Data

Personal Applications

CONTROL 05

Account Management

SAFEGUARDS TOTAL 6 | IG1 4/6 | IG2 6/6 | IG3 6/6

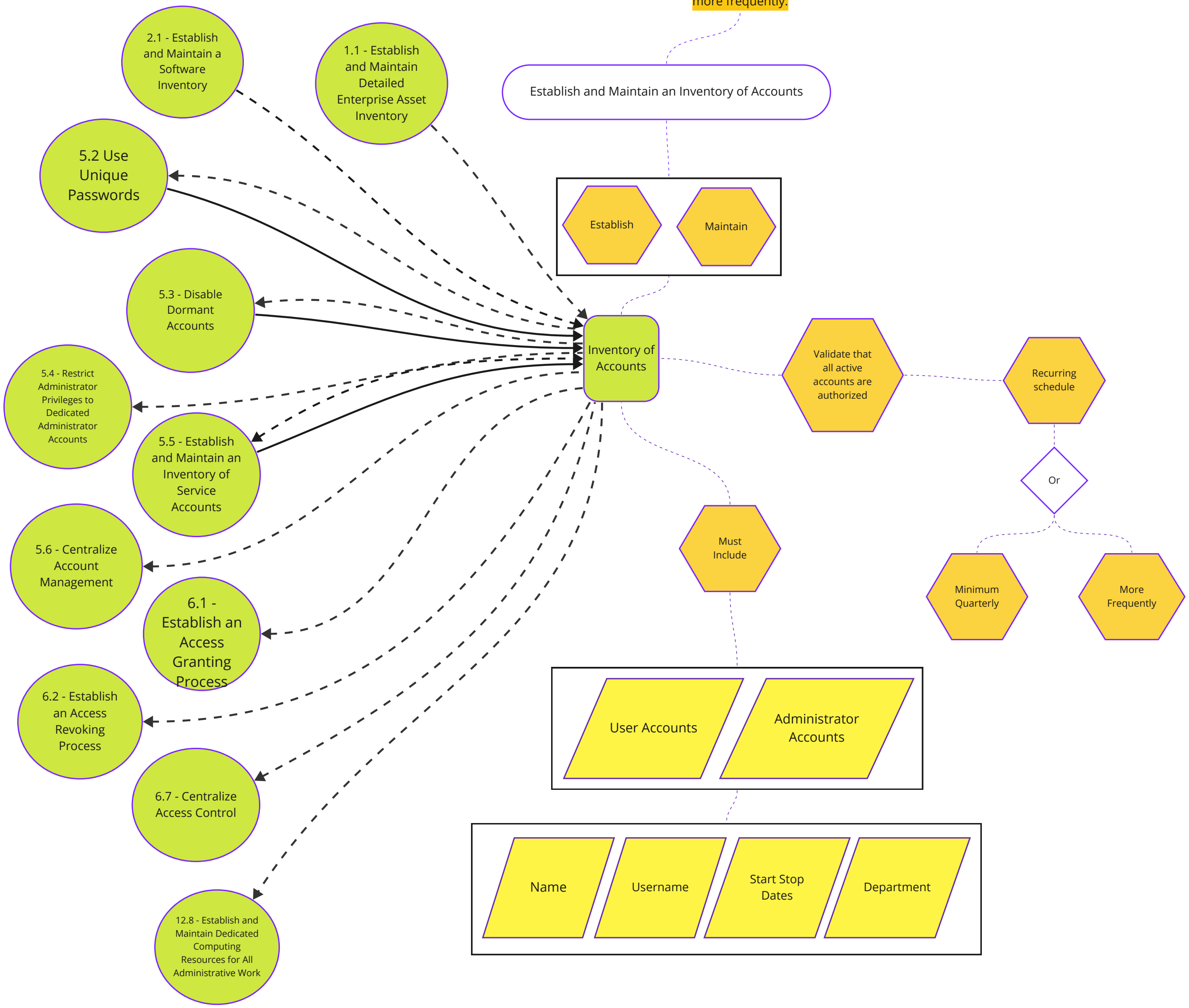
Overview

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.

Group Validated

5.1

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.



Establish and Maintain an Inventory of Accounts

Establish

Maintain

Inventory of Accounts

Validate that all active accounts are authorized

Recurring schedule

Or

Minimum Quarterly

More Frequently

Must Include

User Accounts

Administrator Accounts

Name

Username

Start Stop Dates

Department

2.1 - Establish and Maintain a Software Inventory

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

5.2 Use Unique Passwords

5.3 - Disable Dormant Accounts

5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts

5.5 - Establish and Maintain an Inventory of Service Accounts

5.6 - Centralize Account Management

6.1 - Establish an Access Granting Process

6.2 - Establish an Access Revoking Process

6.7 - Centralize Access Control

12.8 - Establish and Maintain Dedicated Computing Resources for All Administrative Work

Process Oriented Safeguard

IG1

Account and Access Control Management

Identify

Users

Identity and Access Management Tool

Group Validated

5.2

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.

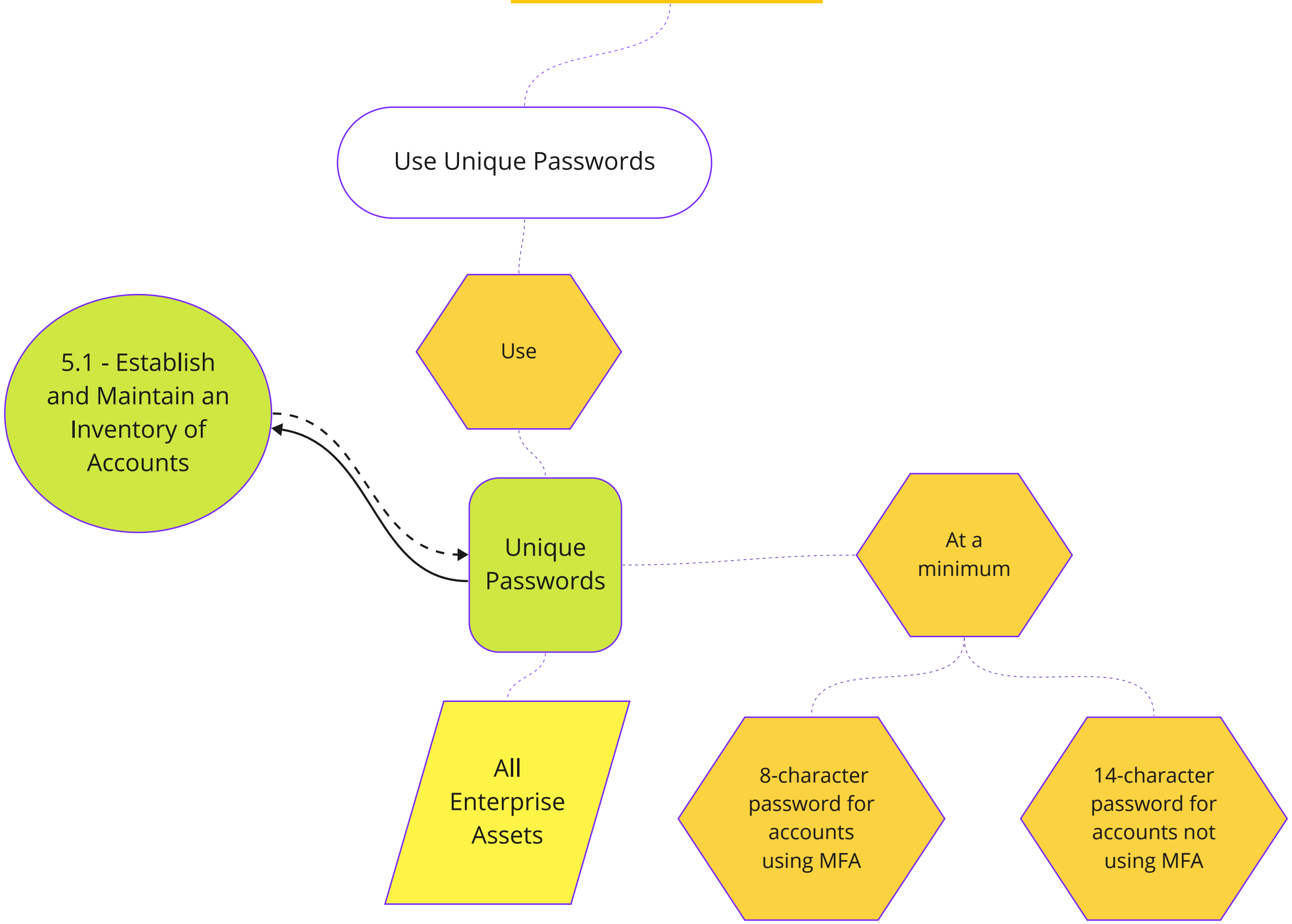
IG1

Account and Access Control Management

Protect

Password Management Tool

Users


Use Unique Passwords
Use
5.1 - Establish and Maintain an Inventory of Accounts
Unique Passwords
At a minimum
All Enterprise Assets
8-character password for accounts using MFA
14-character password for accounts not using MFA

Group Validated

5.3

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

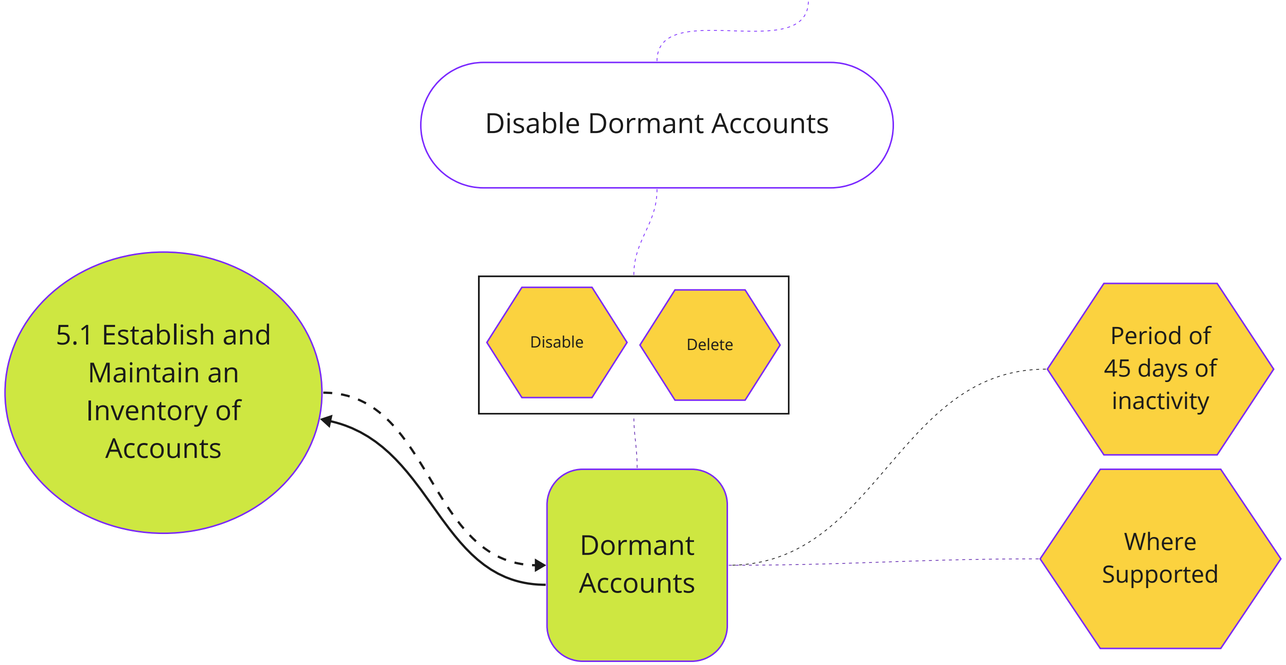
IG1

Account and Access Control Management

Respond

Identity and Access Management Tool

Users



Disable Dormant Accounts

Disable

Delete

5.1 Establish and Maintain an Inventory of Accounts

Dormant Accounts

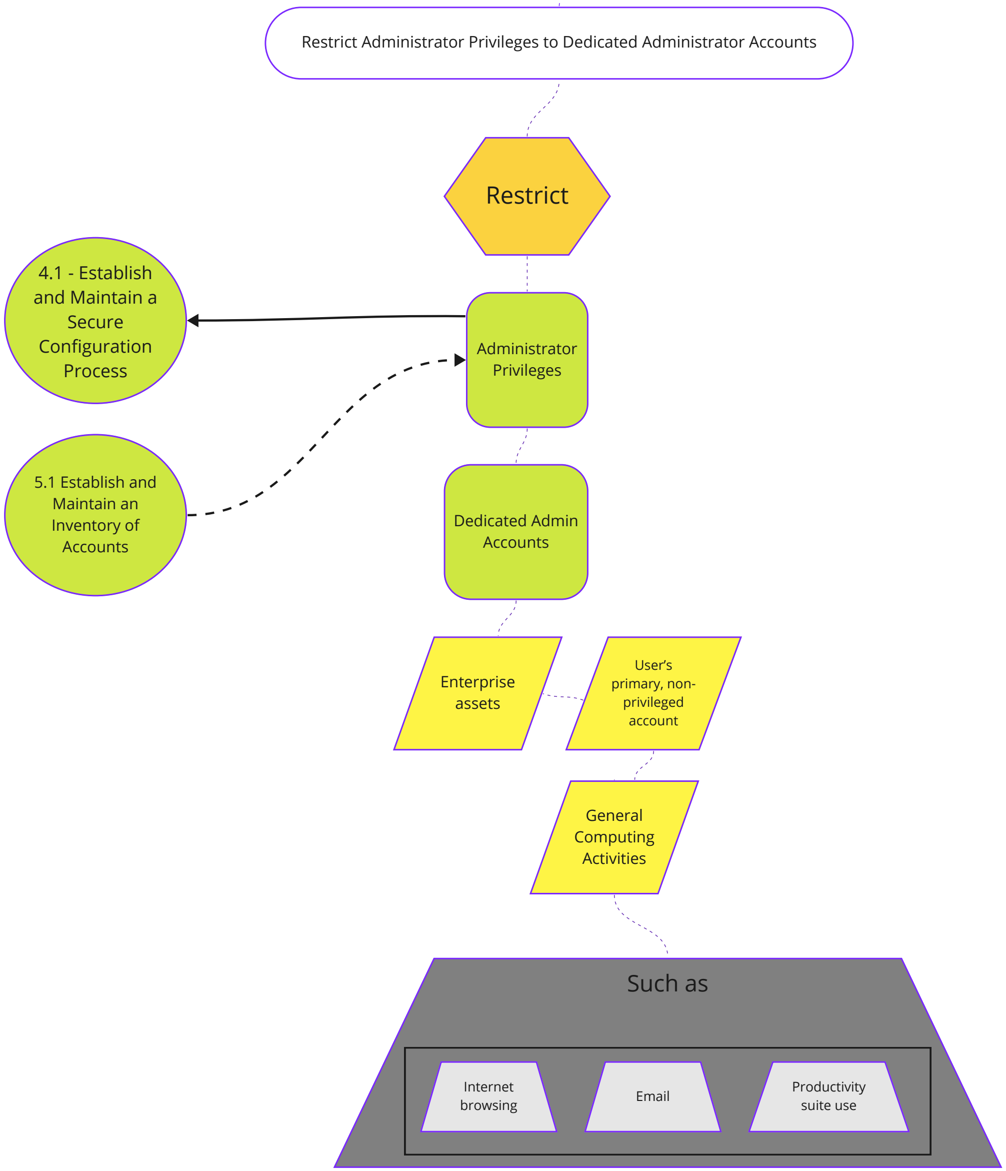
Period of 45 days of inactivity

Where Supported

Group Validated

5.4

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.



Restrict Administrator Privileges to Dedicated Administrator Accounts

Restrict

Administrator Privileges

4.1 - Establish and Maintain a Secure Configuration Process

5.1 Establish and Maintain an Inventory of Accounts

Dedicated Admin Accounts

Enterprise assets

User’s primary, non-privileged account

General Computing Activities

Such as

Internet browsing

Email

Productivity suite use

IG1

Protect

Users

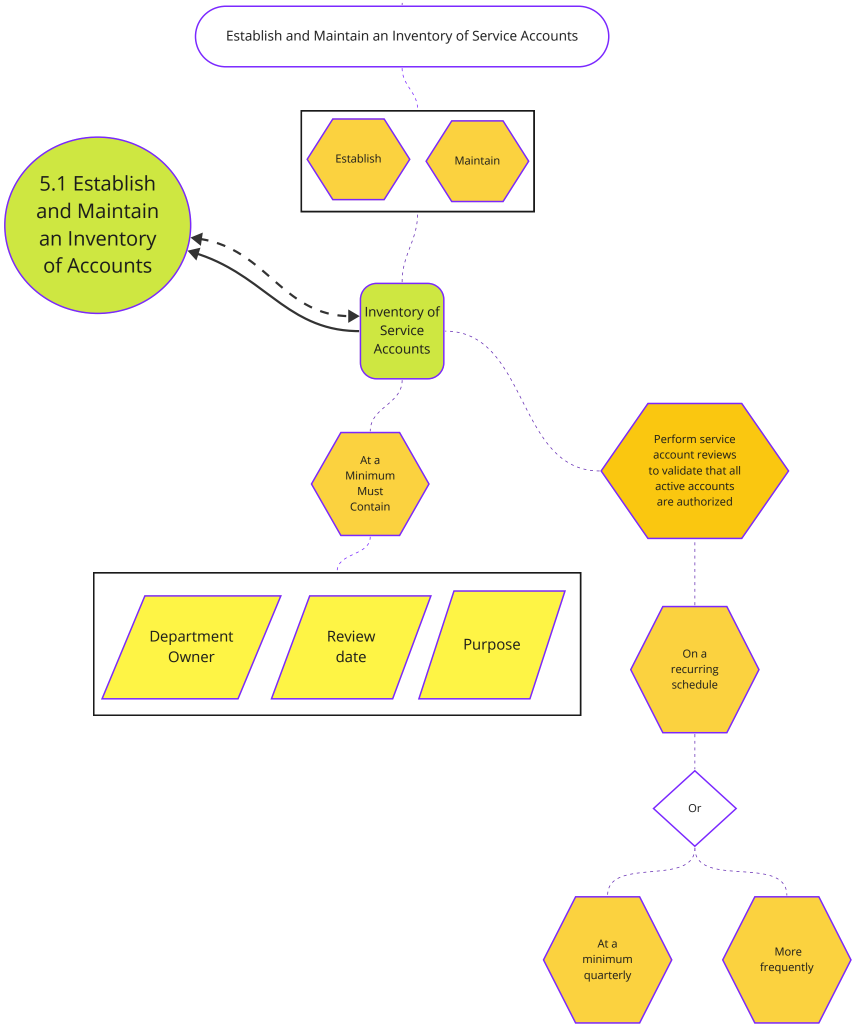
Account and Access Control Management

Identity and Access Management Tool

Group Validated

5.5

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.



Establish and Maintain an Inventory of Service Accounts
Establish
Maintain
5.1 Establish and Maintain an Inventory of Accounts
Inventory of Service Accounts
At a Minimum Must Contain
Department Owner
Review date
Purpose
Perform service account reviews to validate that all active accounts are authorized
On a recurring schedule
Or
At a minimum quarterly
More frequently

Process Oriented Safeguard

IG2

Account and Access Control Management

Identify

Users

Identity and Access Management Tool

Group Validated

5.6

Centralize account management through a directory or identity service.

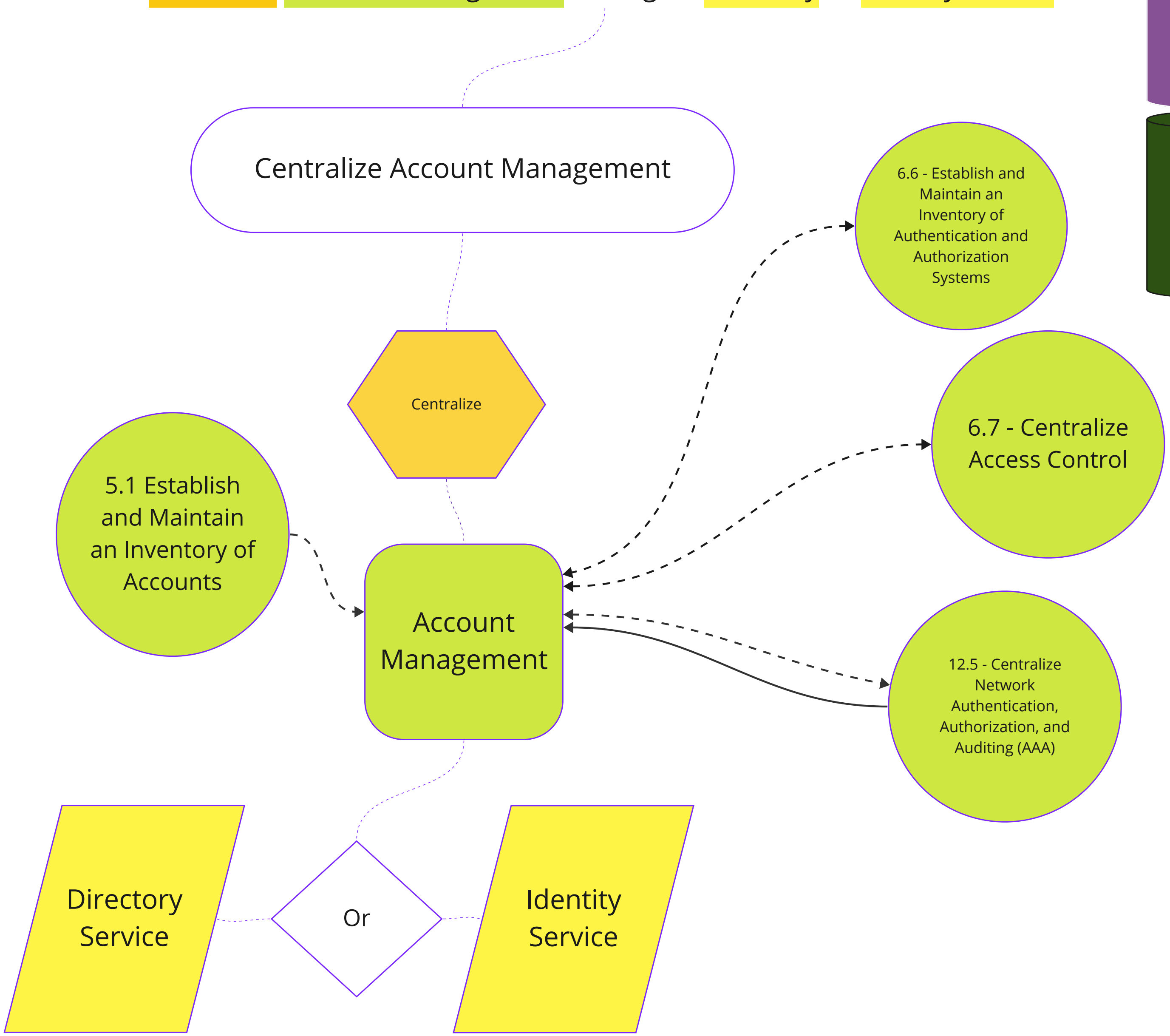
IG2

Protect

Users

Account and Access Control Management

Identity and Access Management Tool



Centralize Account Management

Centralize

Account Management

5.1 Establish and Maintain an Inventory of Accounts

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

6.7 - Centralize Access Control

12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA)

Directory Service

Or

Identity Service

CONTROL 06

Access Control Management

SAFEGUARDS TOTAL	IG1	IG2	IG3
8	5/8	7/8	8/8

Overview

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.

Group Validated

6.1

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

Process Oriented Safeguard

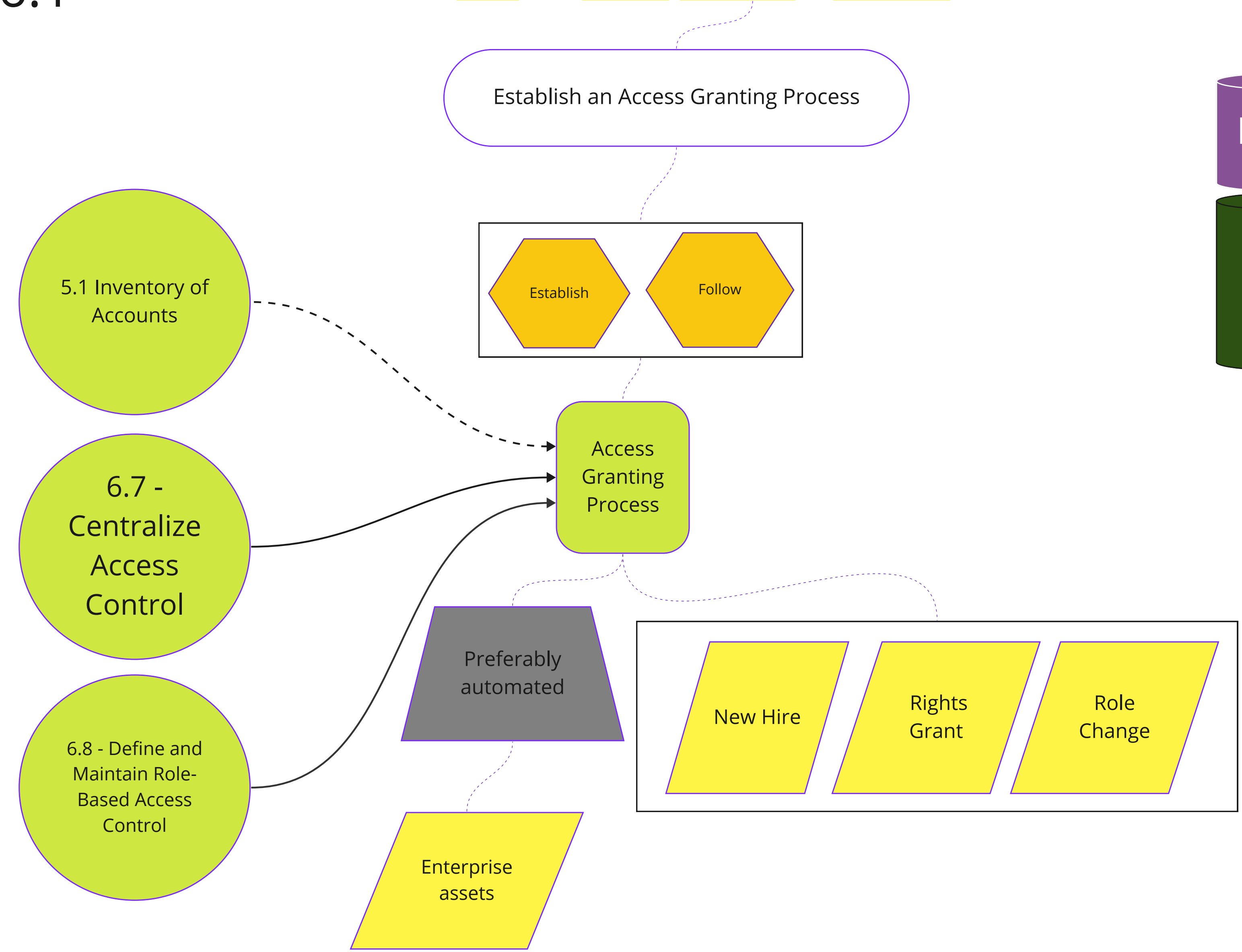
IG1

Account and Access Control Management

Protect

Account and Credential Management Policy/Process

Users



Establish an Access Granting Process

Establish

Follow

5.1 Inventory of Accounts

6.7 - Centralize Access Control

6.8 - Define and Maintain Role-Based Access Control

Access Granting Process

Preferably automated

New Hire

Rights Grant

Role Change

Enterprise assets

Group Validated

6.2

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.

Process Oriented Safeguard

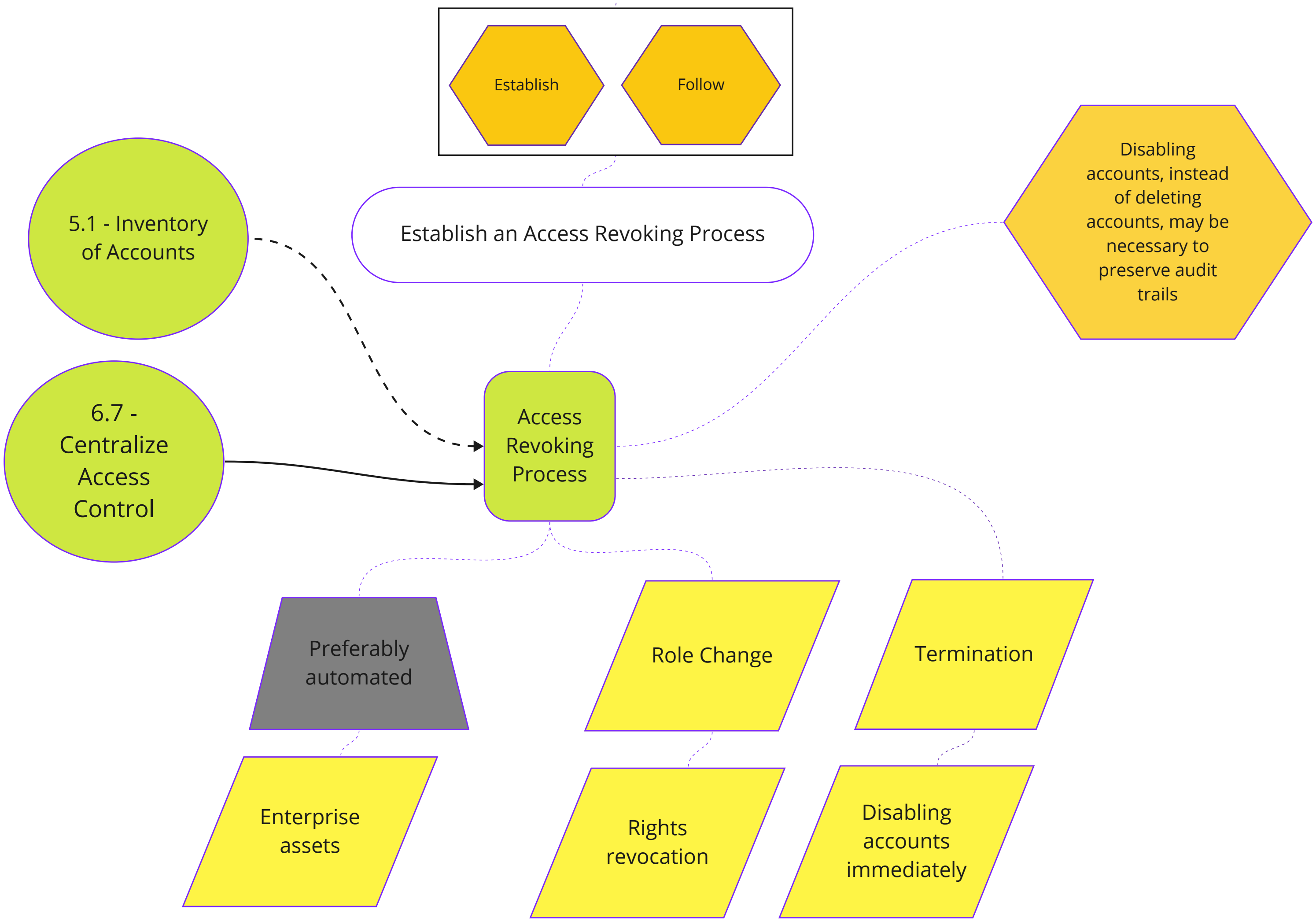
IG1

Account and Access Control Management

Protect

Account and Credential Management Policy/Process

Users



Establish

Follow

Establish an Access Revoking Process

Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails

5.1 - Inventory of Accounts

6.7 - Centralize Access Control

Access Revoking Process

Preferably automated

Role Change

Termination

Enterprise assets

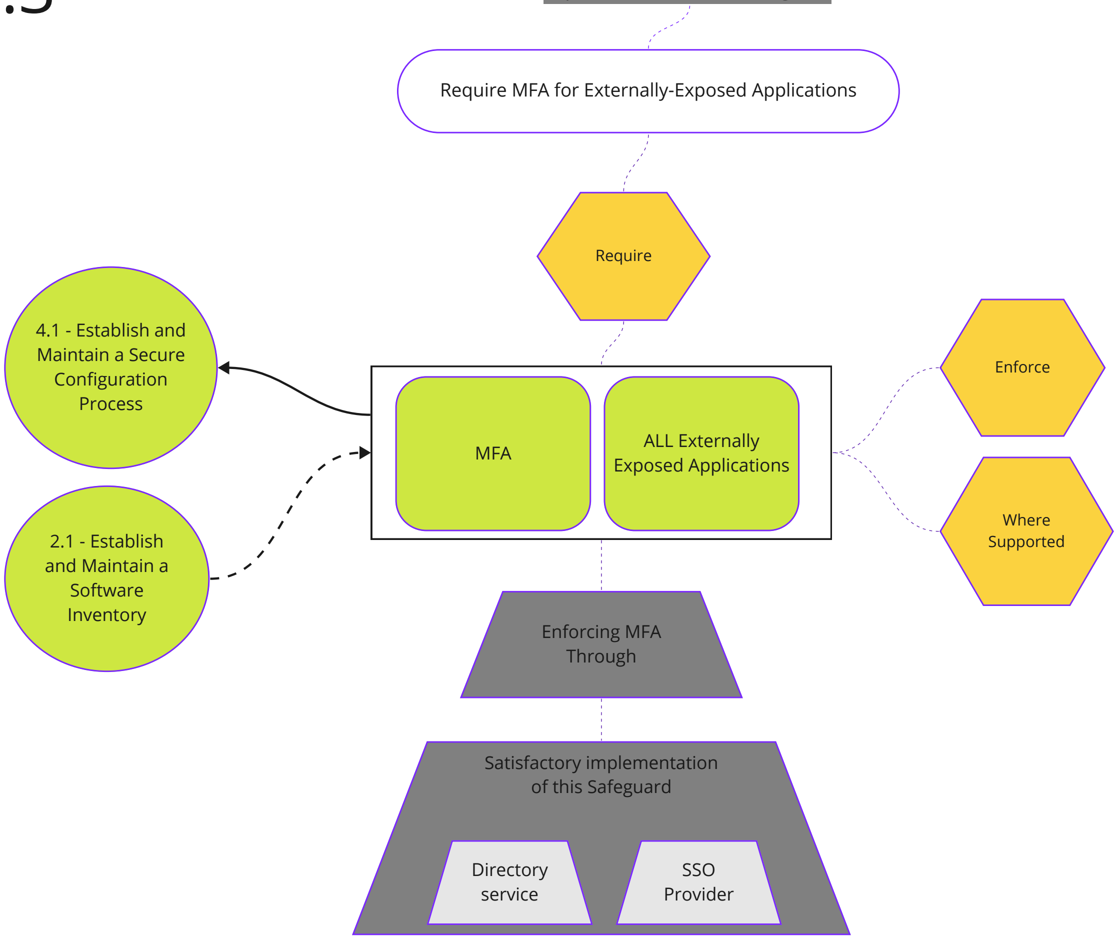
Rights revocation

Disabling accounts immediately

Group Validated

6.3

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.



Require MFA for Externally-Exposed Applications

Require

4.1 - Establish and Maintain a Secure Configuration Process

2.1 - Establish and Maintain a Software Inventory

MFA

ALL Externally Exposed Applications

Enforce

Where Supported

Enforcing MFA Through

Satisfactory implementation of this Safeguard

Directory service

SSO Provider

IG1

Account and Access Control Management

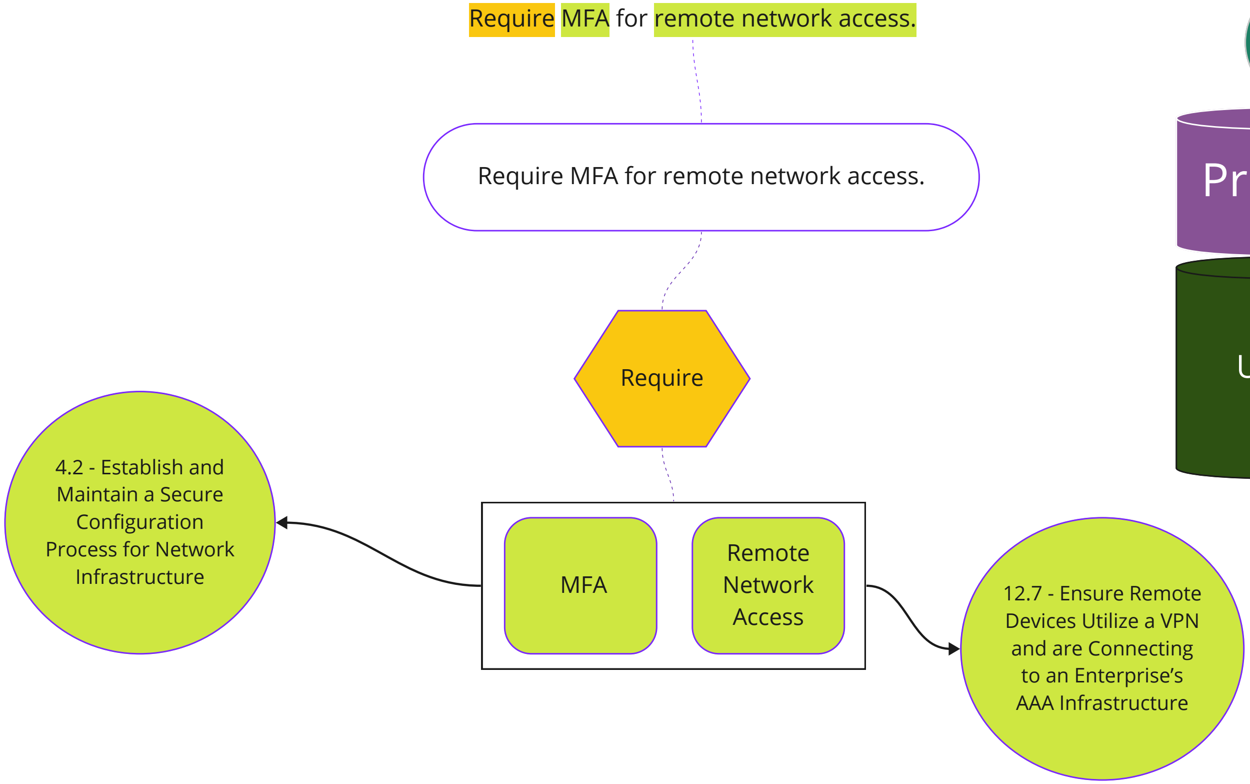
Protect

Multi-Factor Authentication Tool

Users

Group Validated

6.4



Require MFA for remote network access.

Require MFA for remote network access.

Require

MFA

Remote Network Access

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

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

IG1

Account and Access Control Management

Protect

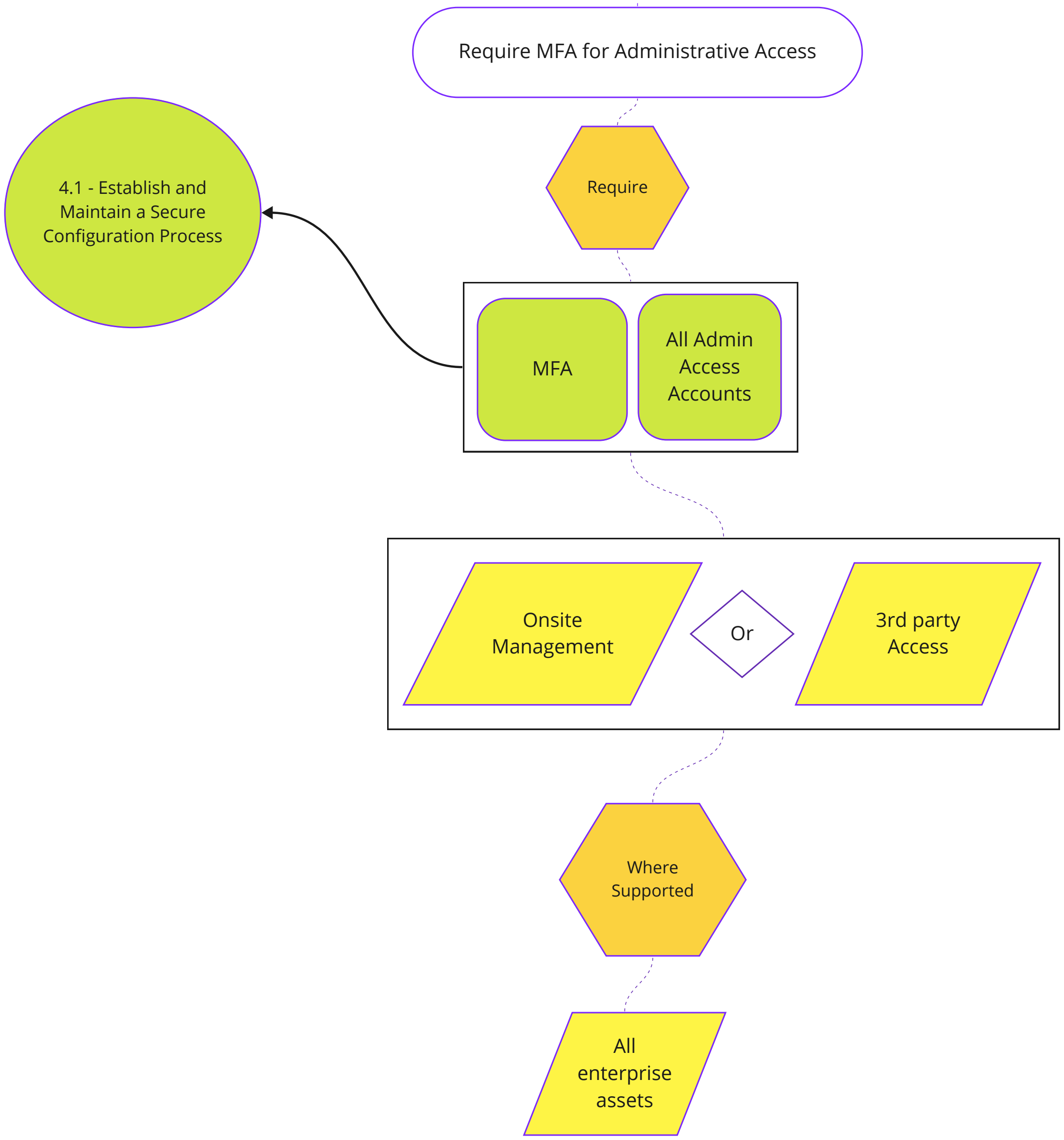
Multi-Factor Authentication Tool

Users

Group Validated

6.5

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



Require MFA for Administrative Access

Require

MFA

All Admin Access Accounts

4.1 - Establish and Maintain a Secure Configuration Process

Onsite Management

Or

3rd party Access

Where Supported

All enterprise assets

IG1

Account and Access Control Management

Protect

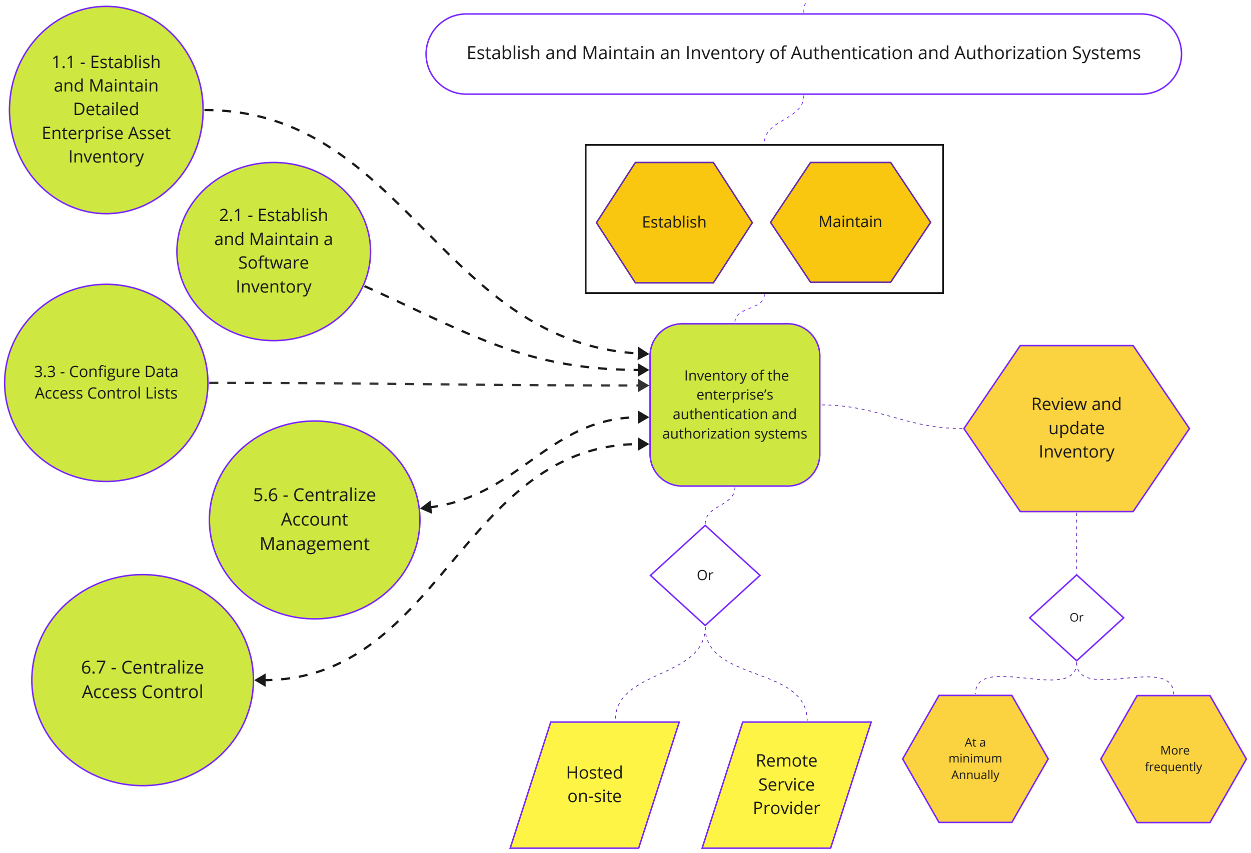
Multi-Factor Authentication Tool

Users

Group Validated

6.6

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.



Establish and Maintain an Inventory of Authentication and Authorization Systems

Establish

Maintain

Inventory of the enterprise's authentication and authorization systems

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

3.3 - Configure Data Access Control Lists

5.6 - Centralize Account Management

6.7 - Centralize Access Control

Or

Hosted on-site

Remote Service Provider

Review and update Inventory

Or

At a minimum Annually

More frequently

Process Oriented Safeguard

IG2

Account and Access Control Management

Identify

Account and Credential Management Policy/Process

Users

Group Validated

6.7

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

IG2

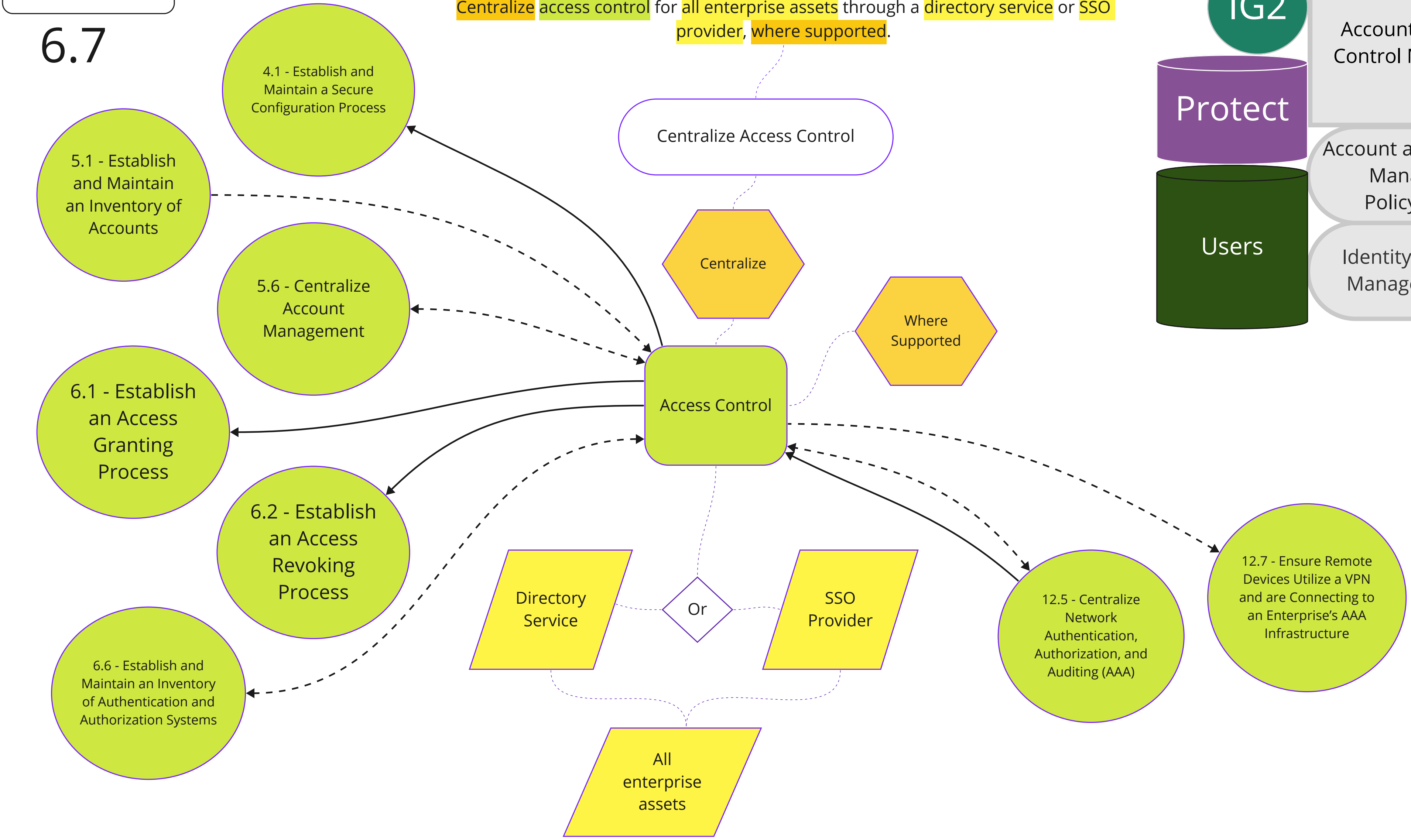
Account and Access Control Management

Protect

Users

Account and Credential Management Policy/Process

Identity and Access Management Tool



Centralize Access Control

Centralize

Where Supported

Access Control

Directory Service

Or

SSO Provider

All enterprise assets

4.1 - Establish and Maintain a Secure Configuration Process

5.1 - Establish and Maintain an Inventory of Accounts

5.6 - Centralize Account Management

6.1 - Establish an Access Granting Process

6.2 - Establish an Access Revoking Process

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

12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA)

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

Group Validated

6.8

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.

Process Oriented Safeguard

IG2

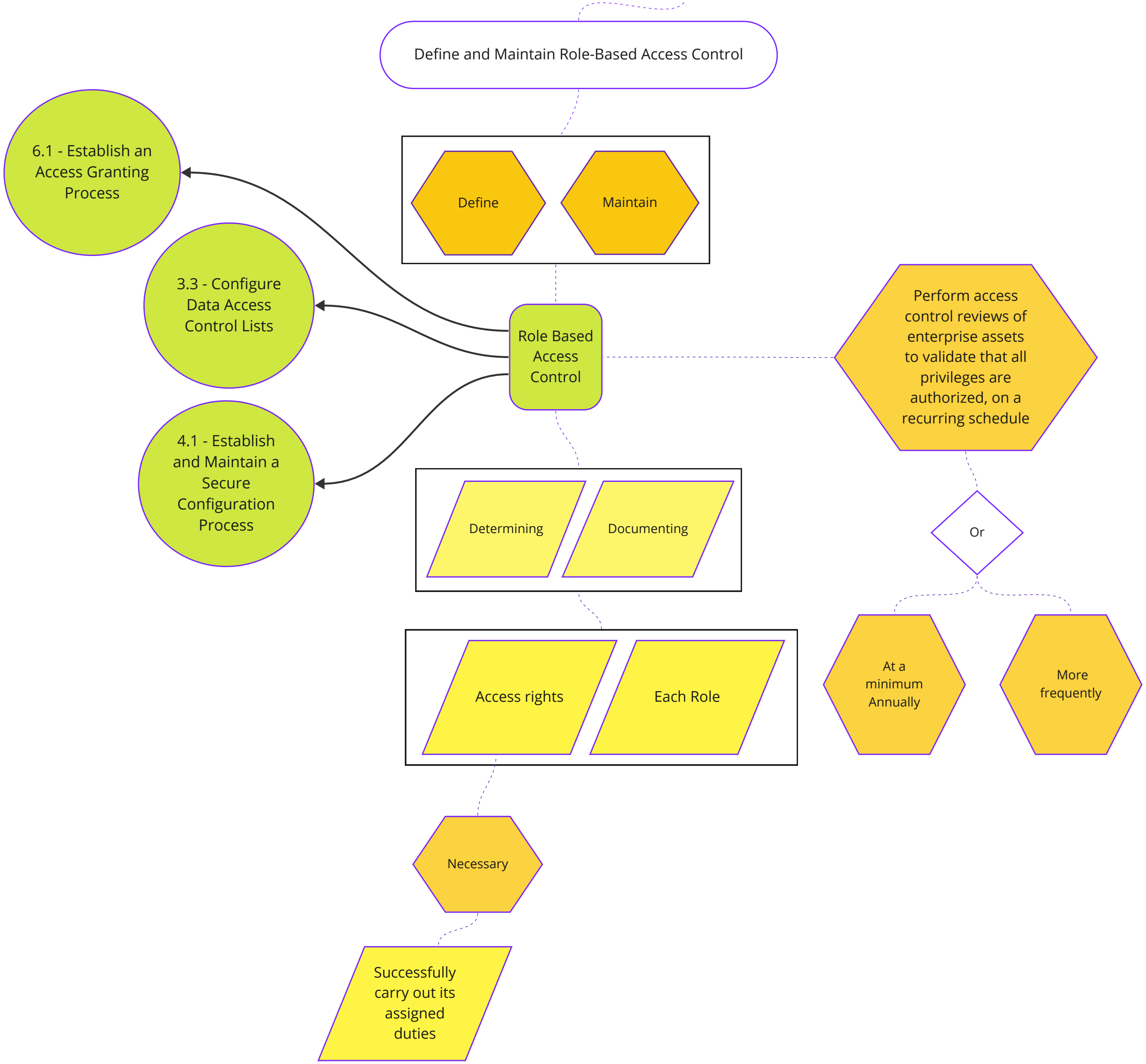
Account and Access Control Management

Protect

Users

Account and Credential Management Policy/Process

Identity and Access management Tool



Define and Maintain Role-Based Access Control

Define

Maintain

Role Based Access Control

6.1 - Establish an Access Granting Process

3.3 - Configure Data Access Control Lists

4.1 - Establish and Maintain a Secure Configuration Process

Determining

Documenting

Access rights

Each Role

Necessary

Successfully carry out its assigned duties

Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule

Or

At a minimum Annually

More frequently

CONTROL 07

Continuous Vulnerability Management

SAFEGUARDS TOTAL	7	IG1	4/7	IG2	7/7	IG3	7/7

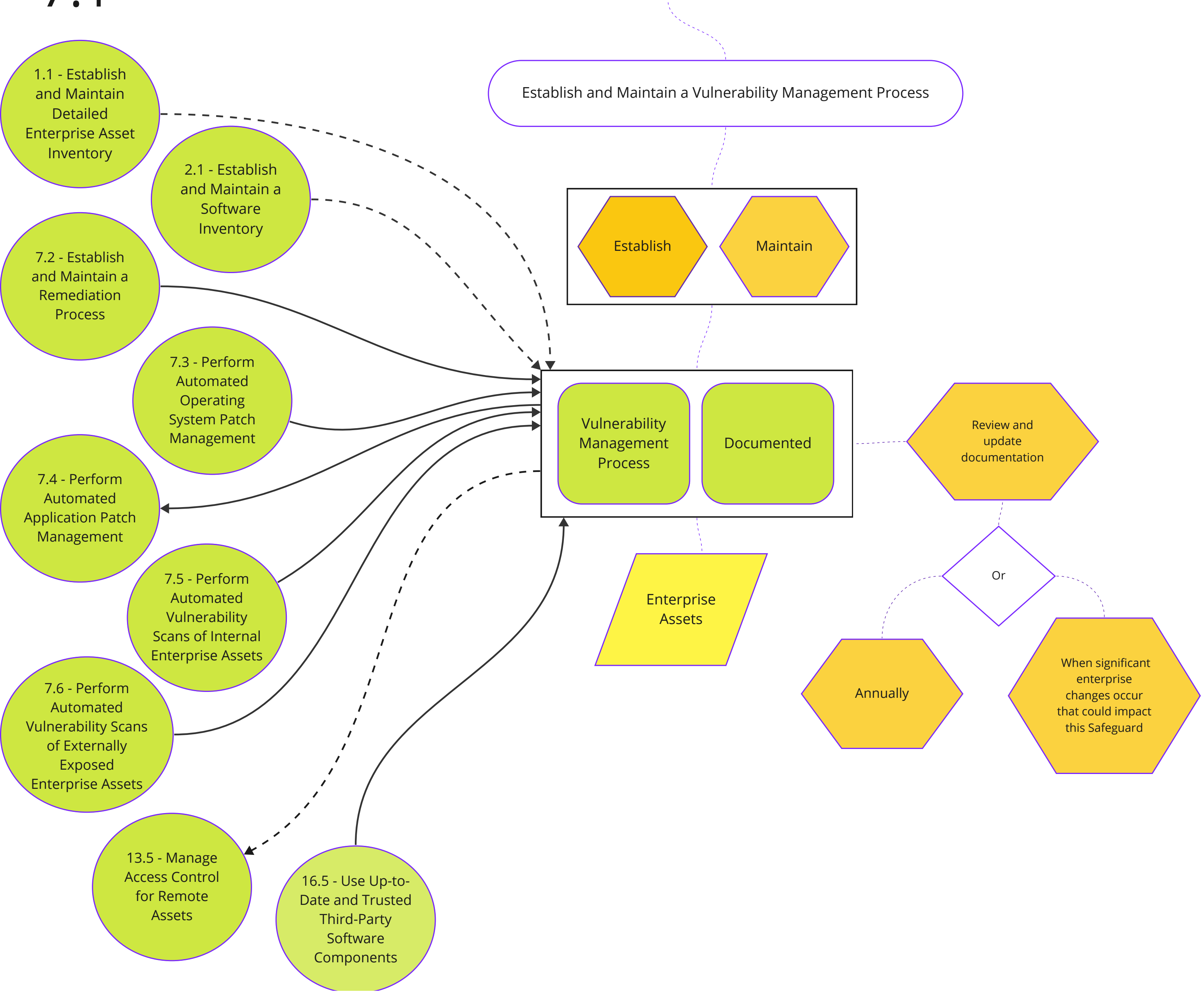
Overview

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.

Group Validated

7.1

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.



Establish and Maintain a Vulnerability Management Process

Establish

Maintain

Vulnerability Management Process

Documented

Enterprise Assets

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

7.2 - Establish and Maintain a Remediation Process

7.3 - Perform Automated Operating System Patch Management

7.4 - Perform Automated Application Patch Management

7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets

7.6 - Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets

13.5 - Manage Access Control for Remote Assets

16.5 - Use Up-to-Date and Trusted Third-Party Software Components

Process Oriented Safeguard

IG1

Vulnerability Management

Protect

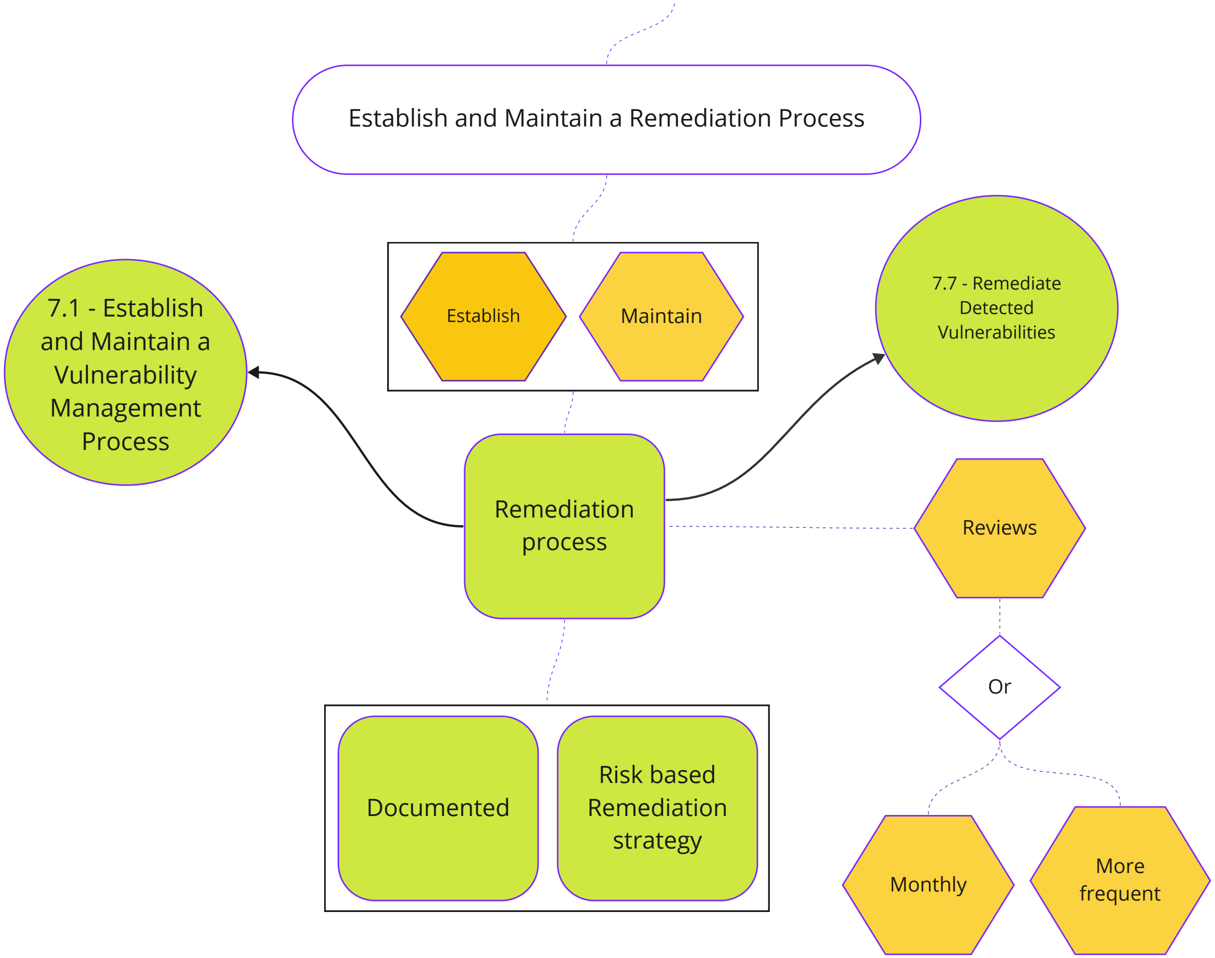
Applications

Vulnerability/Patch Management Policy/Process

Group Validated

7.2

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


Establish and Maintain a Remediation Process

Establish

Maintain

7.1 - Establish and Maintain a Vulnerability Management Process

7.7 - Remediate Detected Vulnerabilities

Remediation process

Reviews

Or

Monthly

More frequent

Documented

Risk based Remediation strategy

Process Oriented Safeguard

IG1

Vulnerability Management

Respond

Vulnerability/Patch Management Tool

Applications

Group Validated

7.3

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

IG1

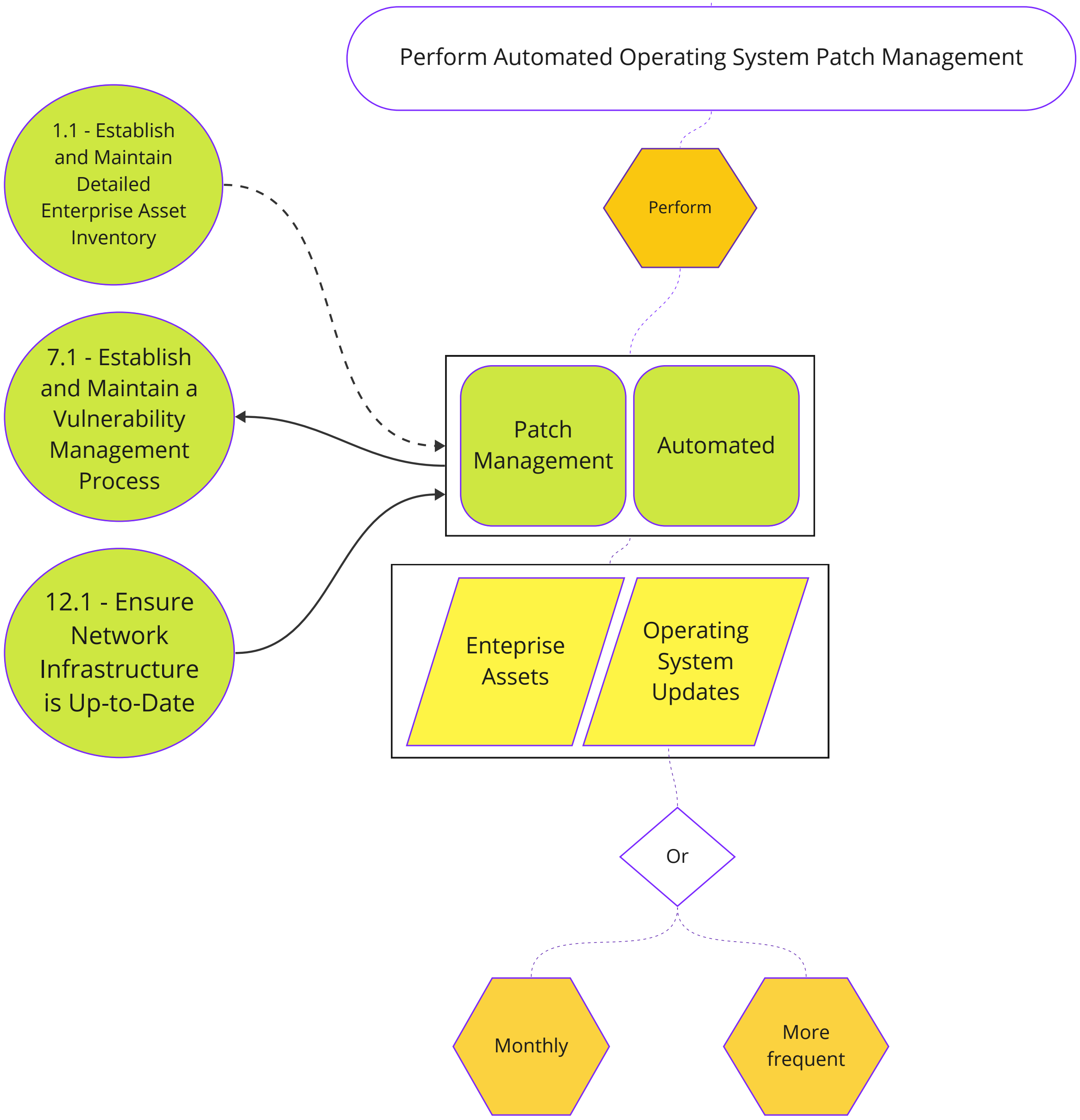
Protect

Vulnerability Management

Applications

Vulnerability/Patch Management Tool

OS Dependent



Perform Automated Operating System Patch Management

Perform

Patch Management

Automated

Enteprise Assets

Operating System Updates

Or

Monthly

More frequent

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

7.1 - Establish and Maintain a Vulnerability Management Process

12.1 - Ensure Network Infrastructure is Up-to-Date

Group Validated

7.4

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

IG1

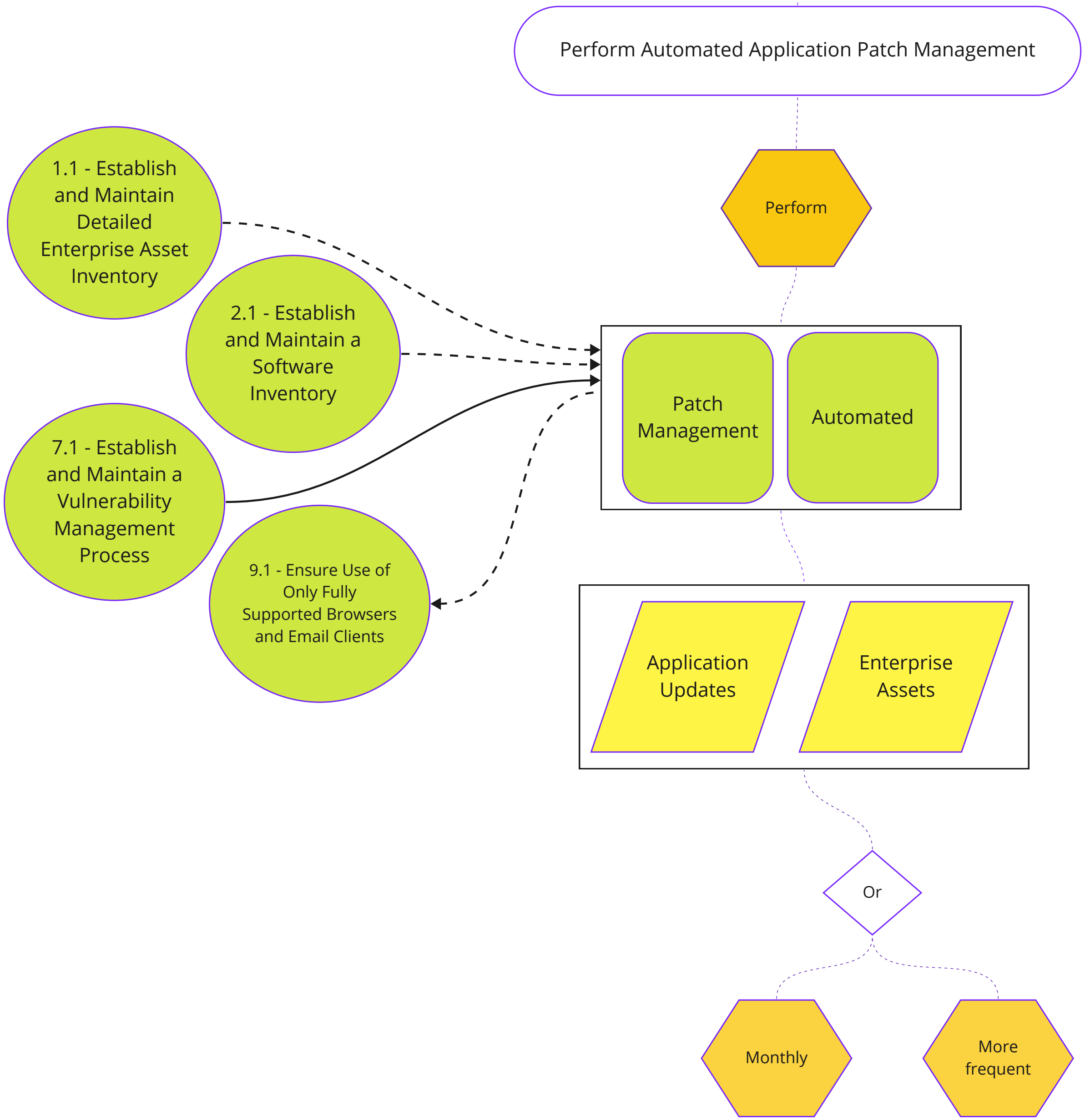
Vulnerability Management

Protect

Vulnerability/Patch Management Tool

Applications

OS Dependent



Perform Automated Application Patch Management

Perform

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

7.1 - Establish and Maintain a Vulnerability Management Process

9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients

Patch Management

Automated

Application Updates

Enterprise Assets

Or

Monthly

More frequent

Group Validated

7.5

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.

IG2

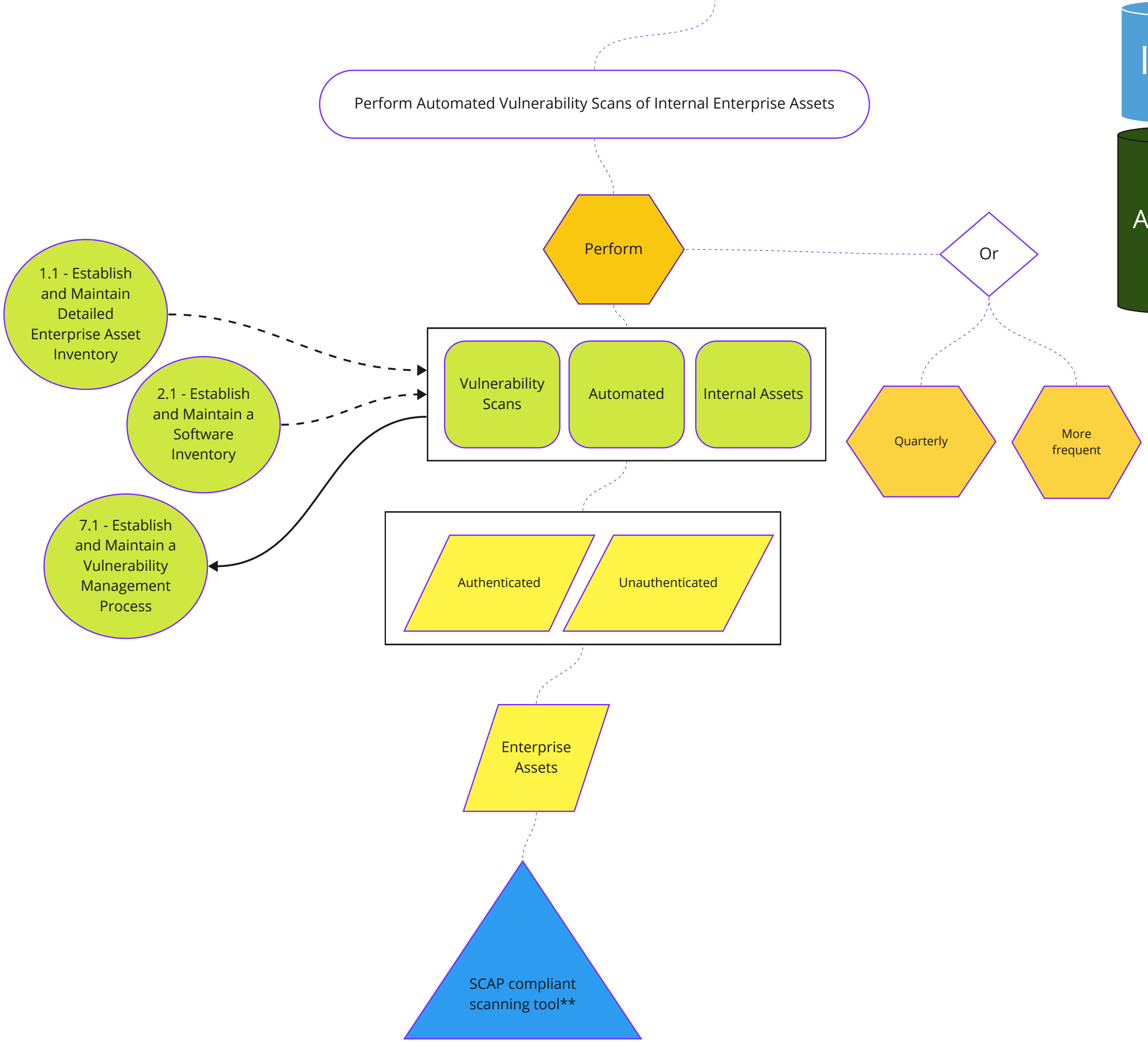
Vulnerability Management

Identify

Applications

Vulnerability Scanning Tool

OS Dependent



Perform Automated Vulnerability Scans of Internal Enterprise Assets

Perform

Or

Quarterly

More frequent

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

7.1 - Establish and Maintain a Vulnerability Management Process

Vulnerability Scans

Automated

Internal Assets

Authenticated

Unauthenticated

Enterprise Assets

SCAP compliant scanning tool**

Group Validated

7.6

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.

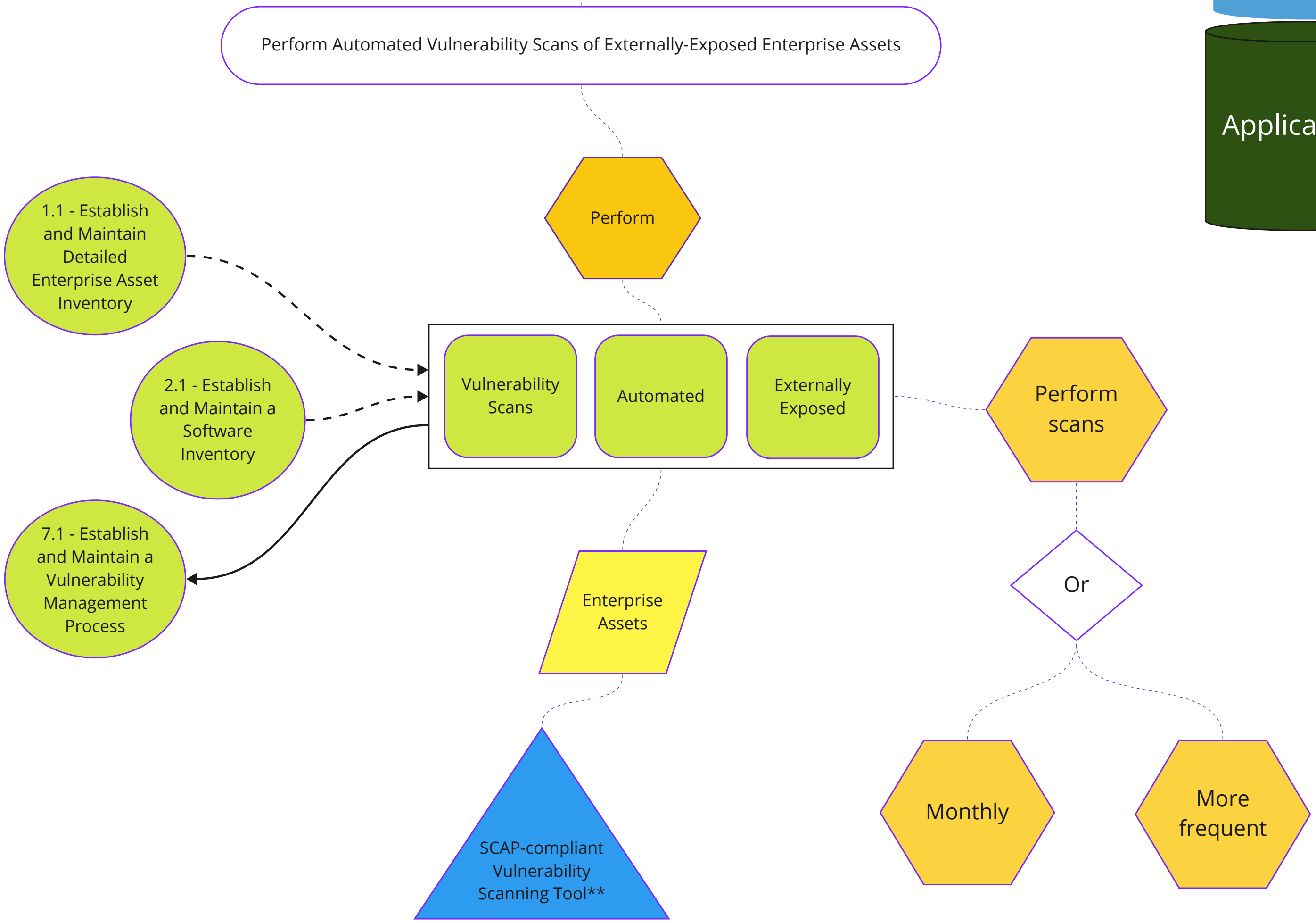
IG2

Vulnerability Management

Identify

Vulnerability Scanning Tool

Applications



Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Perform

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

7.1 - Establish and Maintain a Vulnerability Management Process

Vulnerability Scans

Automated

Externally Exposed

Perform scans

Or

Monthly

More frequent

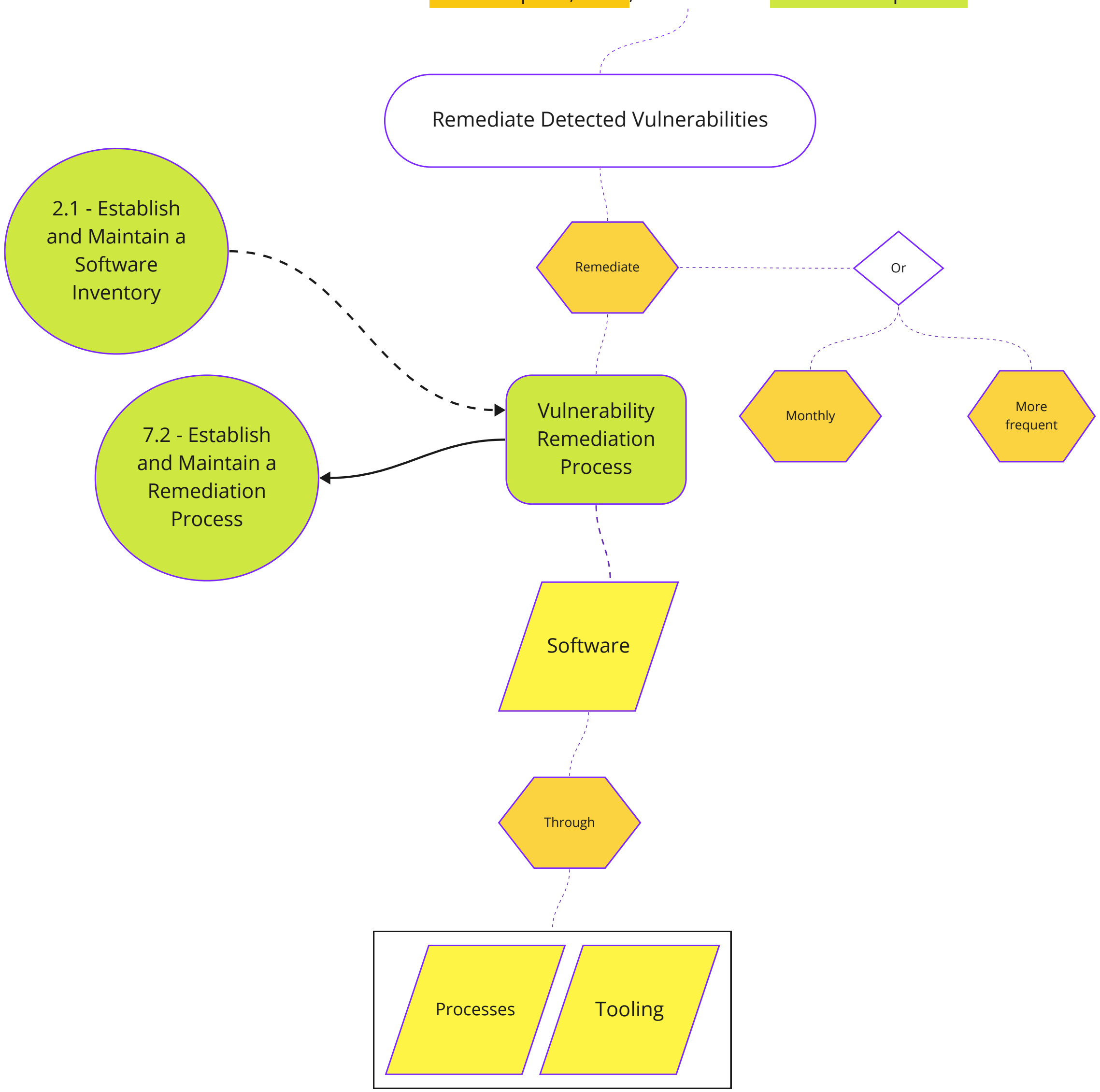
Enterprise Assets

SCAP-compliant Vulnerability Scanning Tool**

Group Validated

7.7

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



Remediate Detected Vulnerabilities

Remediate

Or

Monthly

More frequent

2.1 - Establish and Maintain a Software Inventory

Vulnerability Remediation Process

7.2 - Establish and Maintain a Remediation Process

Software

Through

Processes

Tooling

Process Oriented Safeguard

IG2

Vulnerability Management

Respond

Vulnerability/Patch Management Policy/Process

Applications

CONTROL 08

Audit Log Management

Safeguards Total	12	IG1	3/12	IG2	11/12	IG3	12/12

Overview

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

Group Validated

8.1

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.

Process Oriented Safeguard

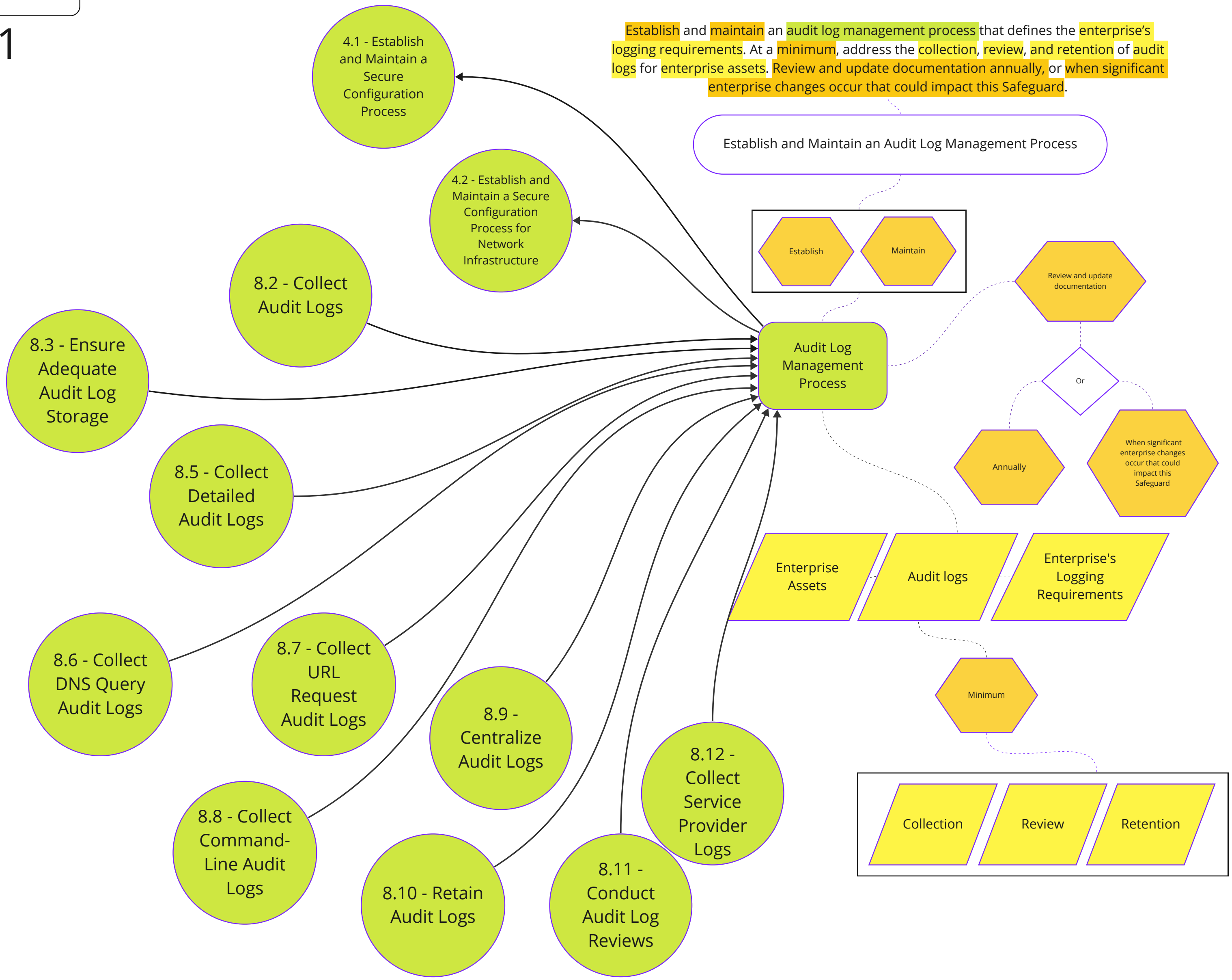
IG1

Log Management

Protect

Log Management Policy/Process

Network



Establish and Maintain an Audit Log Management Process

Establish

Maintain

Audit Log Management Process

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Enterprise Assets

Audit logs

Enterprise's Logging Requirements

Minimum

Collection

Review

Retention

4.1 - Establish and Maintain a Secure Configuration Process

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

8.2 - Collect Audit Logs

8.3 - Ensure Adequate Audit Log Storage

8.5 - Collect Detailed Audit Logs

8.6 - Collect DNS Query Audit Logs

8.7 - Collect URL Request Audit Logs

8.8 - Collect Command-Line Audit Logs

8.9 - Centralize Audit Logs

8.10 - Retain Audit Logs

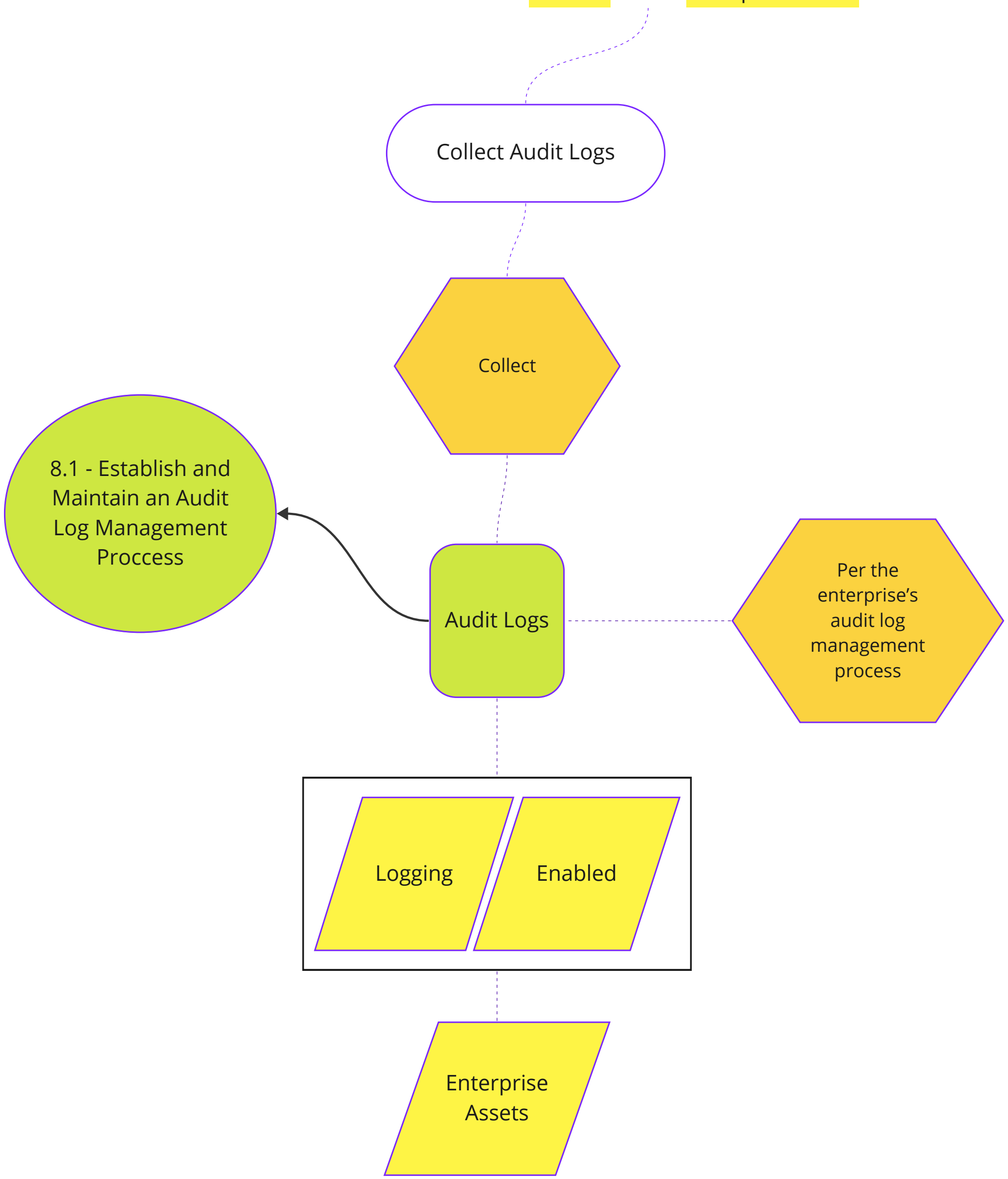
8.11 - Conduct Audit Log Reviews

8.12 - Collect Service Provider Logs

Group Validated

8.2

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



Collect Audit Logs

Collect

8.1 - Establish and Maintain an Audit Log Management Proccess

Audit Logs

Per the enterprise's audit log management process

Logging

Enabled

Enterprise Assets

IG1

Log Management

Detect

Log Management Tool

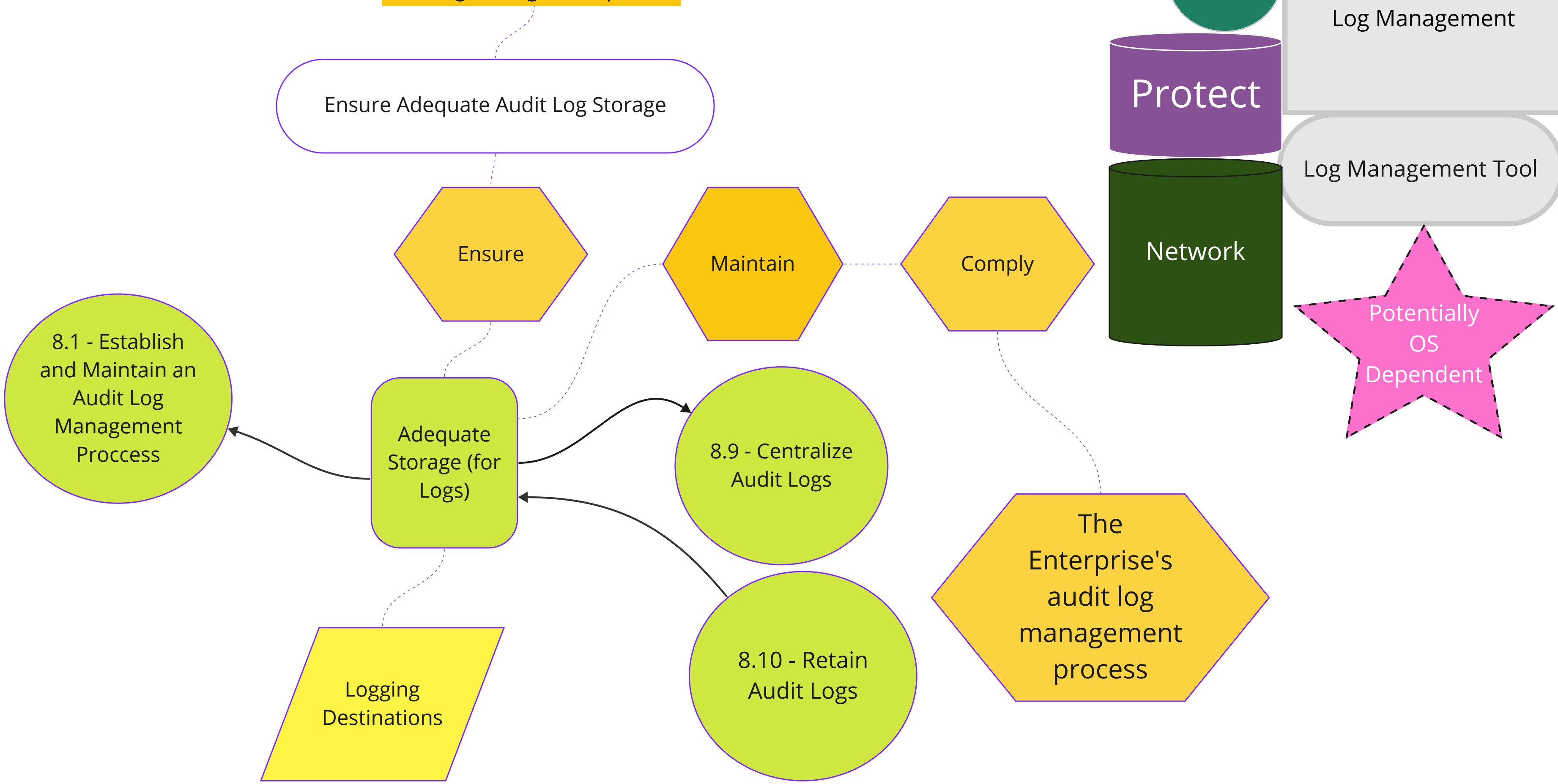
Network

OS Dependent

Group Validated

8.3

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



IG1

Log Management

Protect

Log Management Tool

Network

Potentially OS Dependent

Ensure Adequate Audit Log Storage

Ensure

Maintain

Comply

8.1 - Establish and Maintain an Audit Log Management Proccess

Adequate Storage (for Logs)

8.9 - Centralize Audit Logs

8.10 - Retain Audit Logs

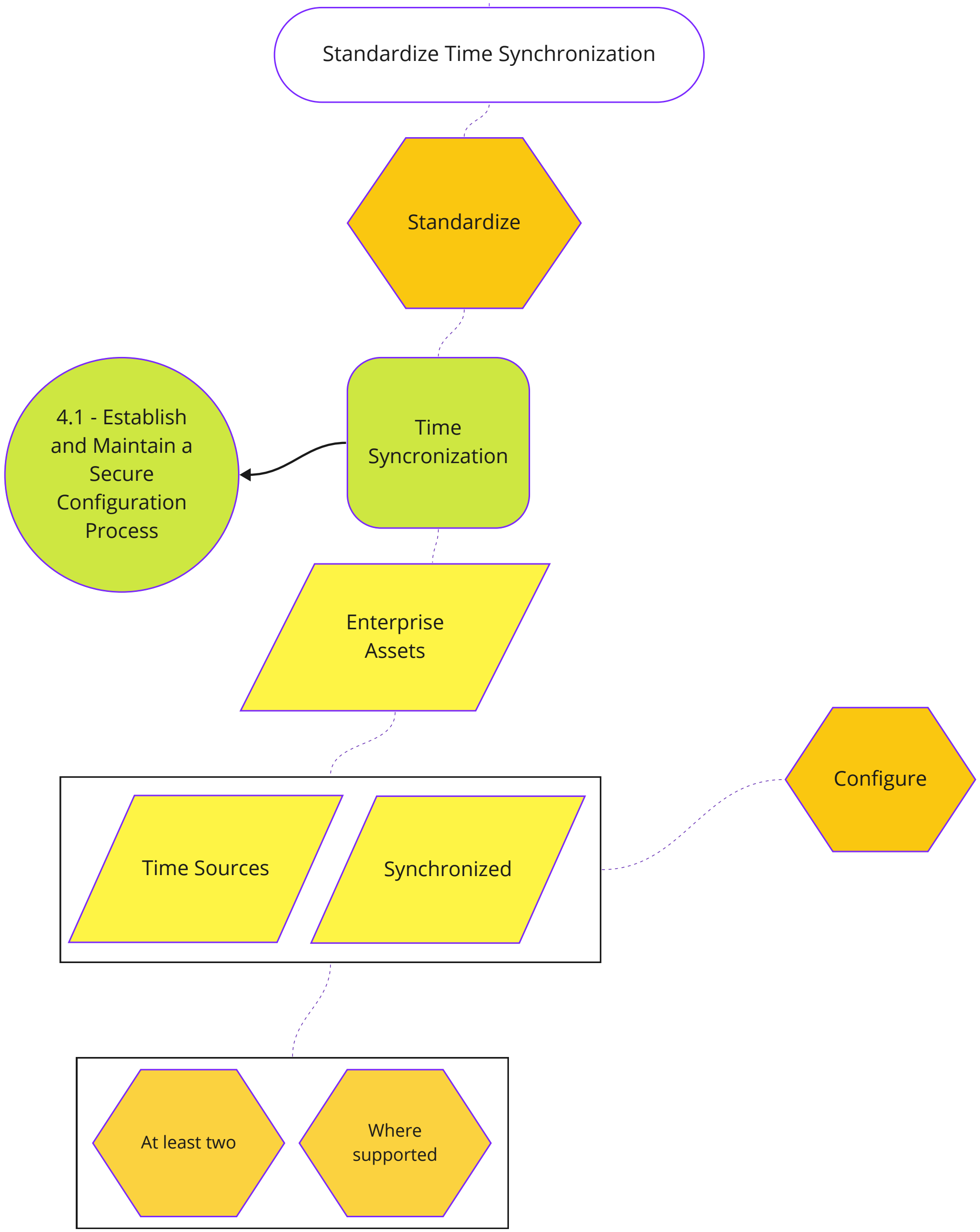
The Enterprise's audit log management process

Logging Destinations

Group Validated

8.4

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



Standardize Time Synchronization

Standardize

Time Syncronization

4.1 - Establish and Maintain a Secure Configuration Process

Enterprise Assets

Time Sources

Synchronized

Configure

At least two

Where supported

IG2

Secure Configurations

Protect

Network

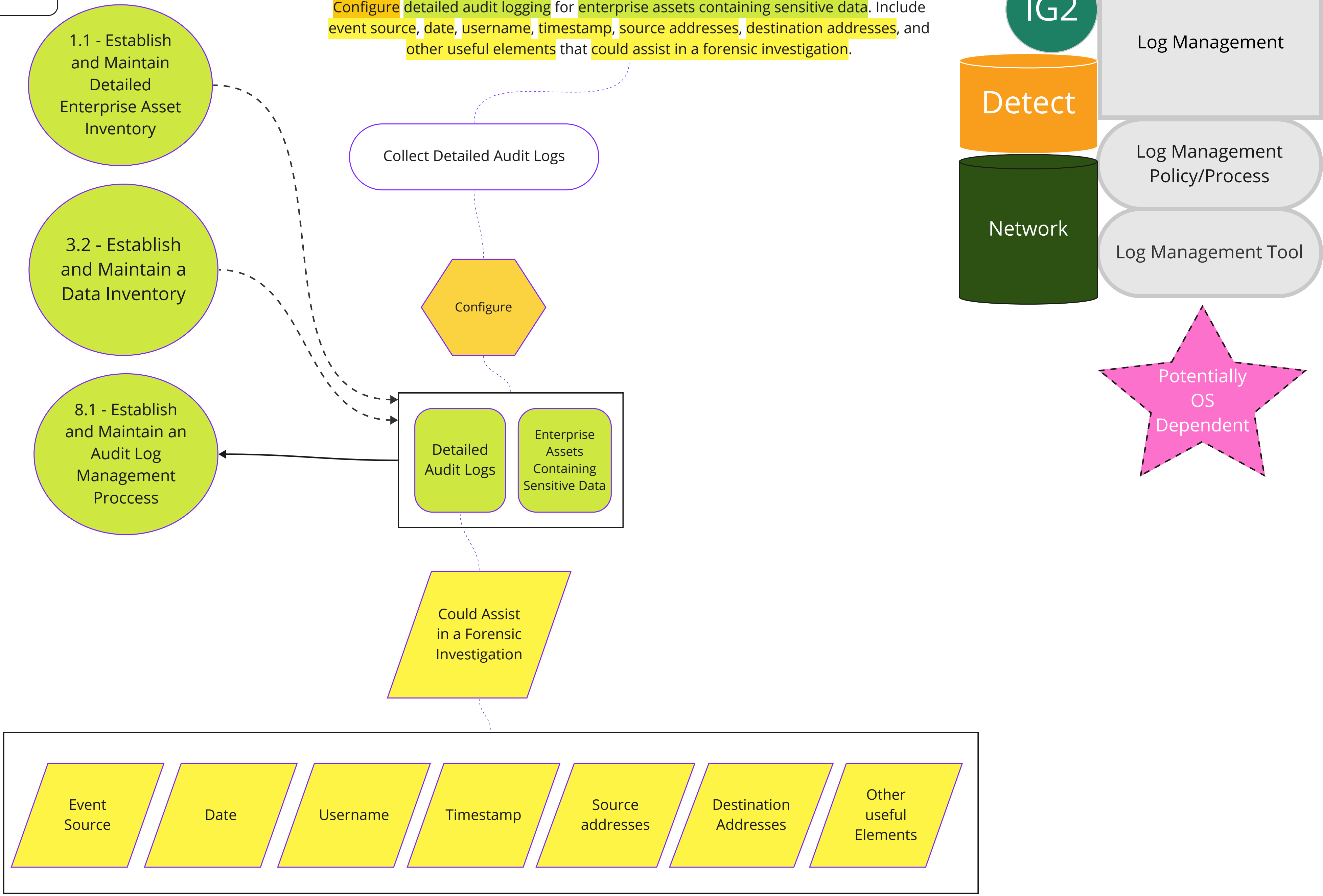
Secure Configuration Policy/Process

Potentially OS Dependent

Group Validated

8.5

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.



1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

3.2 - Establish and Maintain a Data Inventory

8.1 - Establish and Maintain an Audit Log Management Proccess

Collect Detailed Audit Logs

Configure

Detailed Audit Logs

Enterprise Assets Containing Sensitive Data

Could Assist in a Forensic Investigation

Event Source

Date

Username

Timestamp

Source addresses

Destination Addresses

Other useful Elements

IG2

Detect

Network

Log Management

Log Management Policy/Process

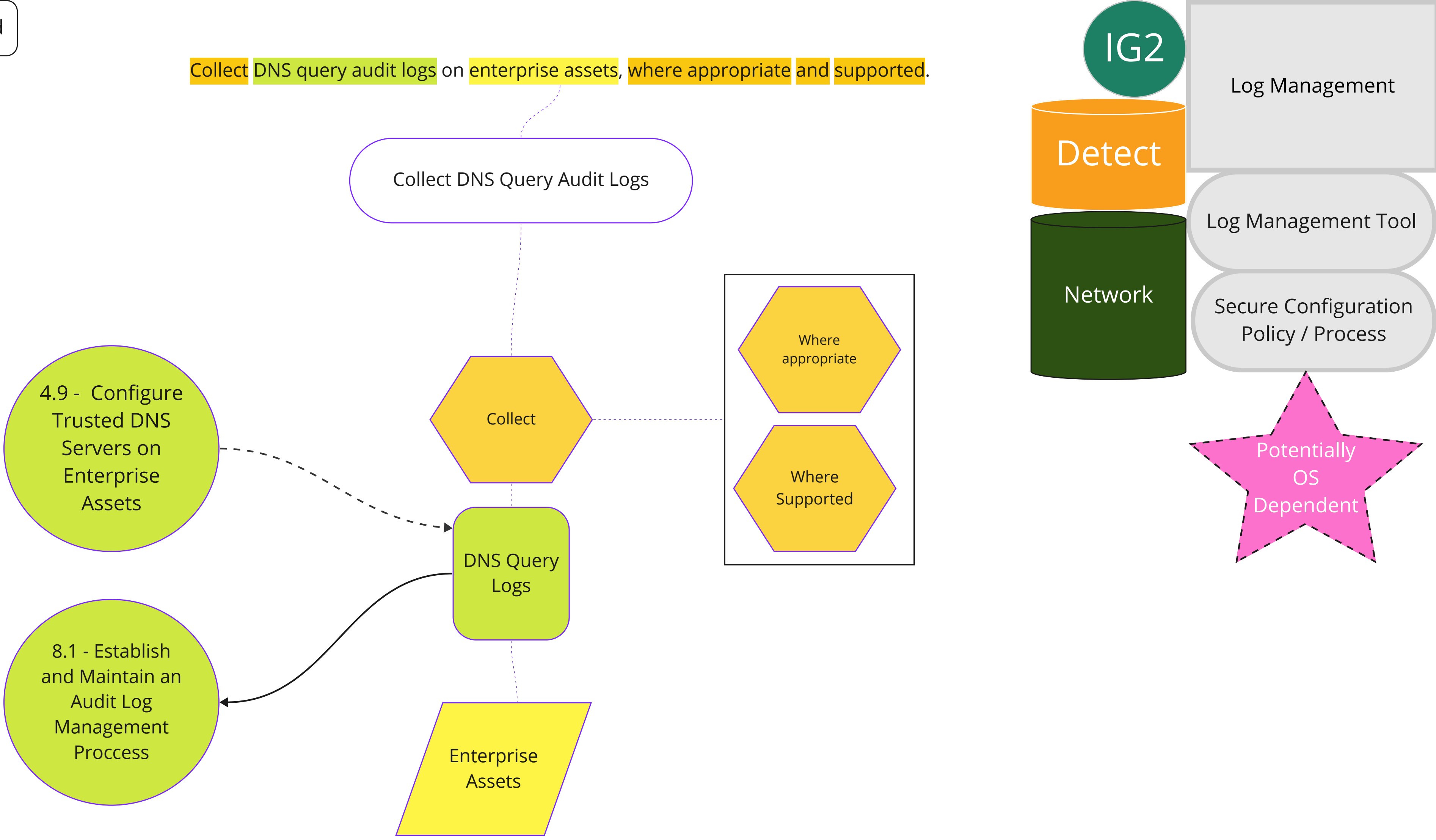
Log Management Tool

Potentially OS Dependent

Group Validated

8.6

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



IG2

Detect

Network

Log Management

Log Management Tool

Secure Configuration Policy / Process

Potentially OS Dependent

Collect DNS Query Audit Logs

Collect

Where appropriate

Where Supported

DNS Query Logs

Enterprise Assets

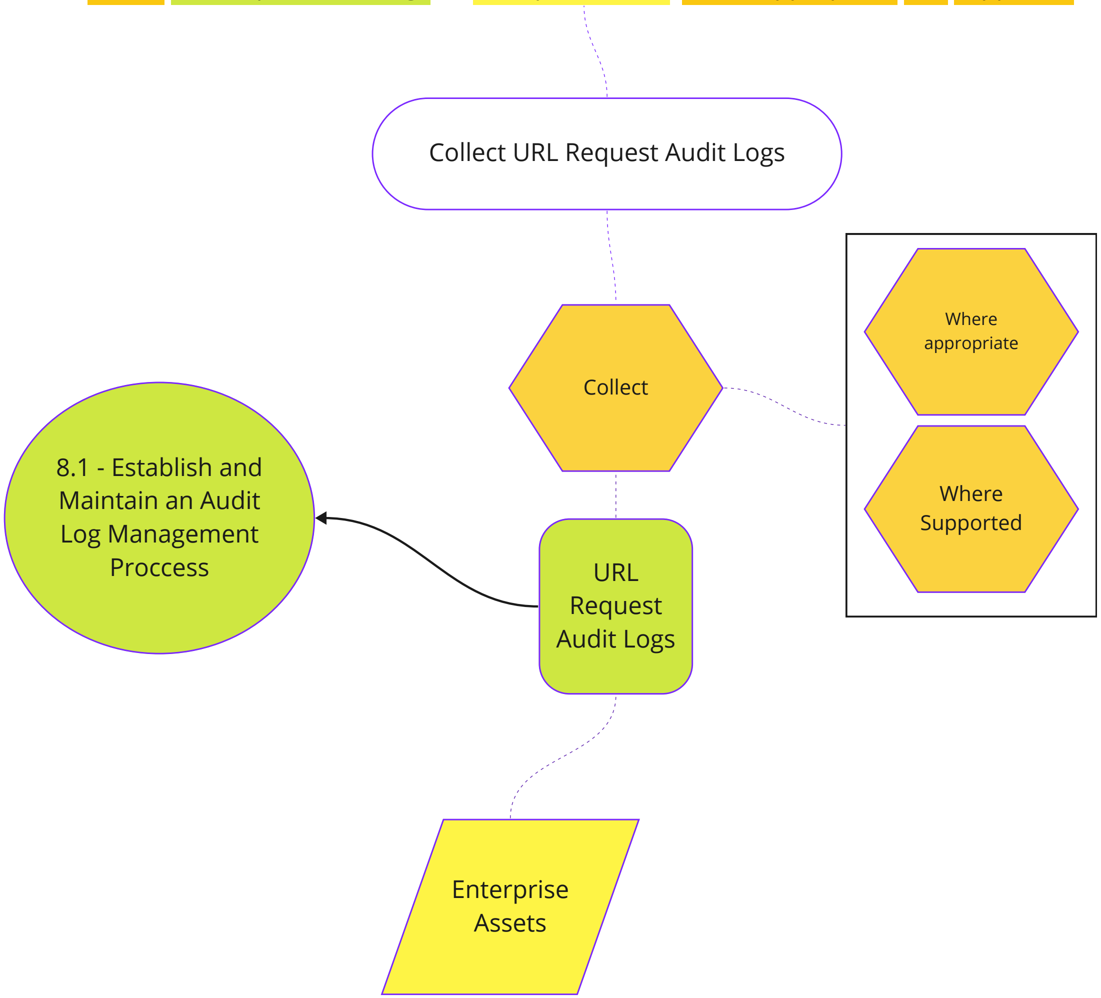
4.9 - Configure Trusted DNS Servers on Enterprise Assets

8.1 - Establish and Maintain an Audit Log Management Proccess

Group Validated

8.7

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



Collect URL Request Audit Logs

Collect

Where appropriate

Where Supported

URL Request Audit Logs

8.1 - Establish and Maintain an Audit Log Management Proccess

Enterprise Assets

IG2

Log Management

Detect

Network

Log Management Tool

Secure Configuration Policy / Process

Potentially OS Dependent

Group Validated

8.8

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

IG2

Log Management

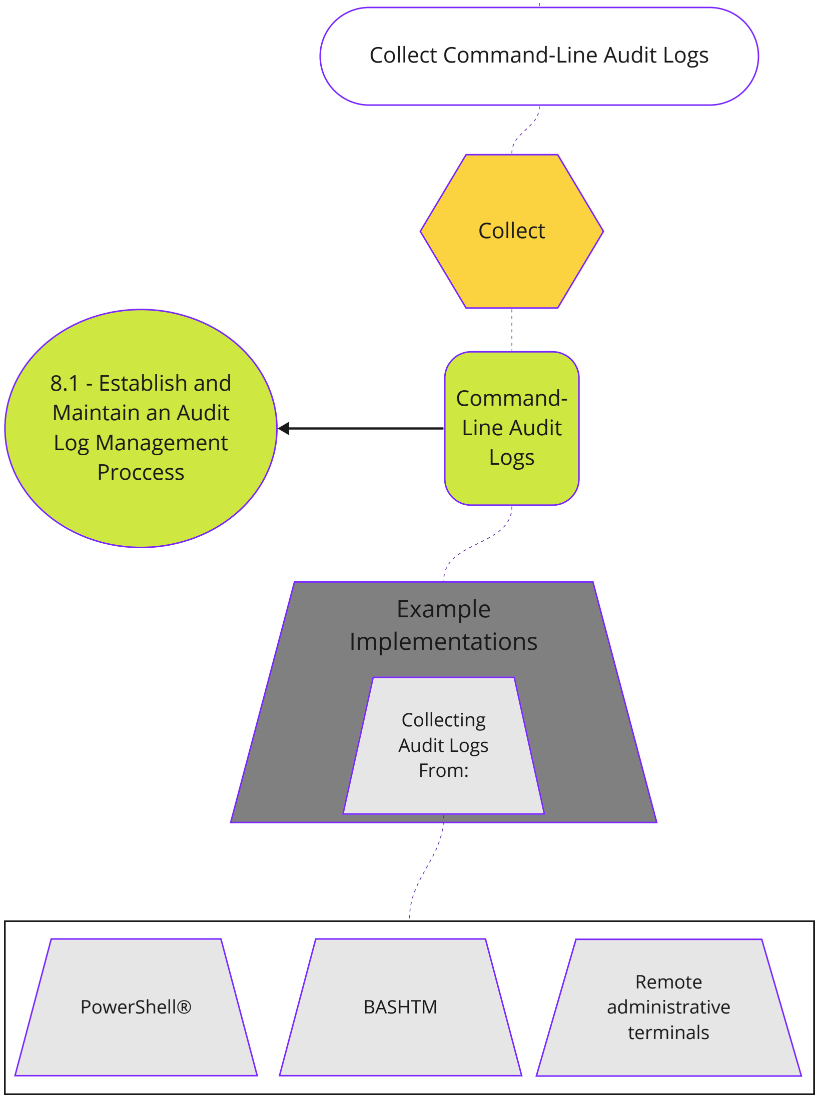
Detect

Devices

Log Management Tool

Secure Configuration Policy / Process

OS Dependent



Collect Command-Line Audit Logs

Collect

Command-Line Audit Logs

8.1 - Establish and Maintain an Audit Log Management Proccess

Example Implementations

Collecting Audit Logs From:

PowerShell®

BASHTM

Remote administrative terminals

Group Validated

8.9

IG2

Detect

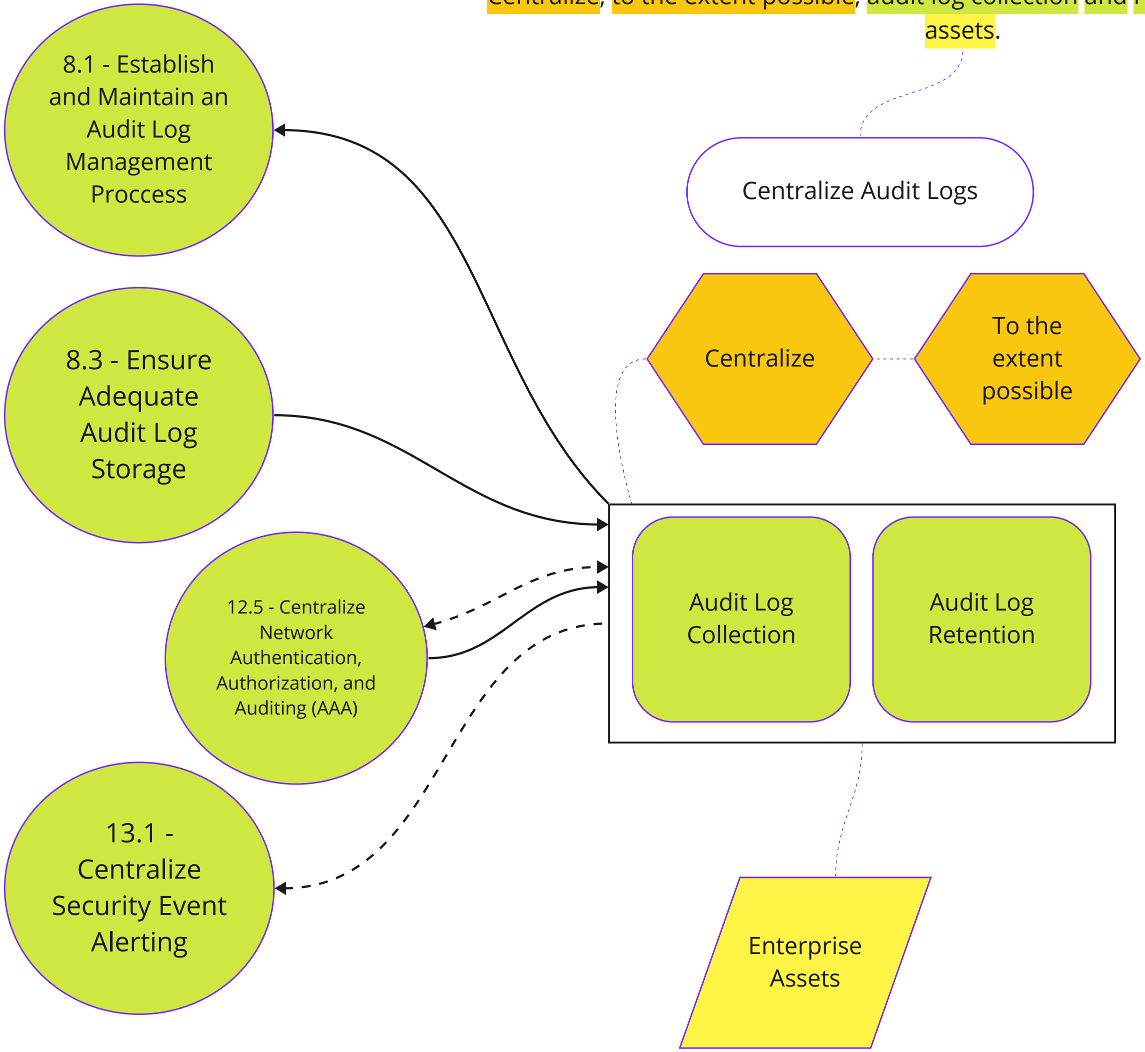
Network

Log Management

Log Analytics and Centralization Tool

OS Dependent

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



Centralize Audit Logs

Centralize

To the extent possible

Audit Log Collection

Audit Log Retention

Enterprise Assets

8.1 - Establish and Maintain an Audit Log Management Proccess

8.3 - Ensure Adequate Audit Log Storage

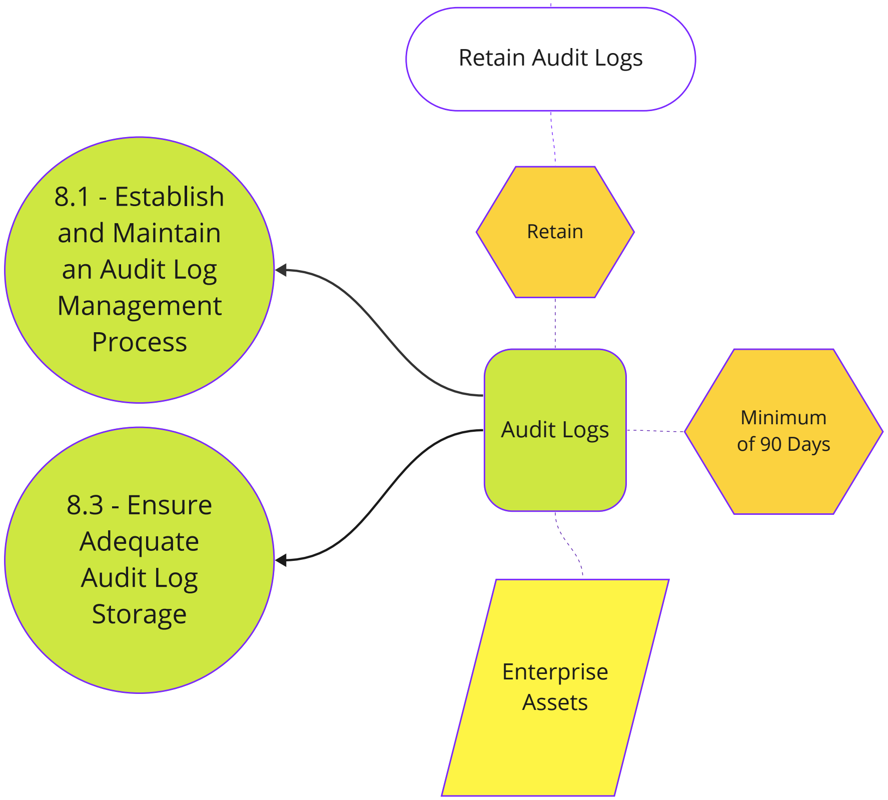
12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA)

13.1 - Centralize Security Event Alerting

Group Validated

8.10

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



Retain Audit Logs

Retain

Audit Logs

Minimum of 90 Days

Enterprise Assets

8.1 - Establish and Maintain an Audit Log Management Process

8.3 - Ensure Adequate Audit Log Storage

IG2

Log Management

Protect

Log Analytics and Centralization Tool

Network

OS Dependent

Group Validated

8.11

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.

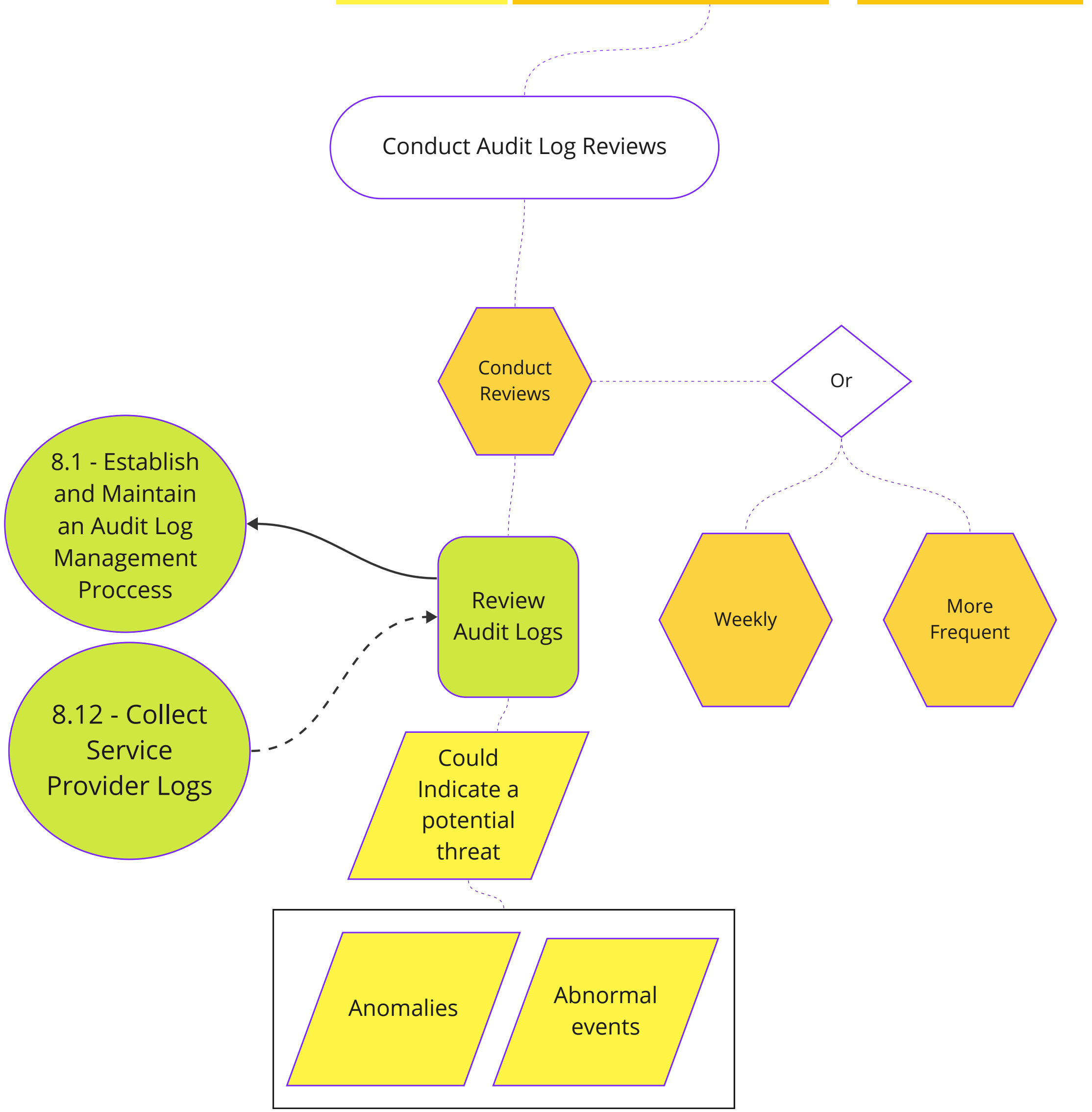
IG2

Log Management

Detect

Log Analytics and Centralization Tool

Network



Conduct Audit Log Reviews

Conduct Reviews

Or

Weekly

More Frequent

8.1 - Establish and Maintain an Audit Log Management Proccess

Review Audit Logs

8.12 - Collect Service Provider Logs

Could Indicate a potential threat

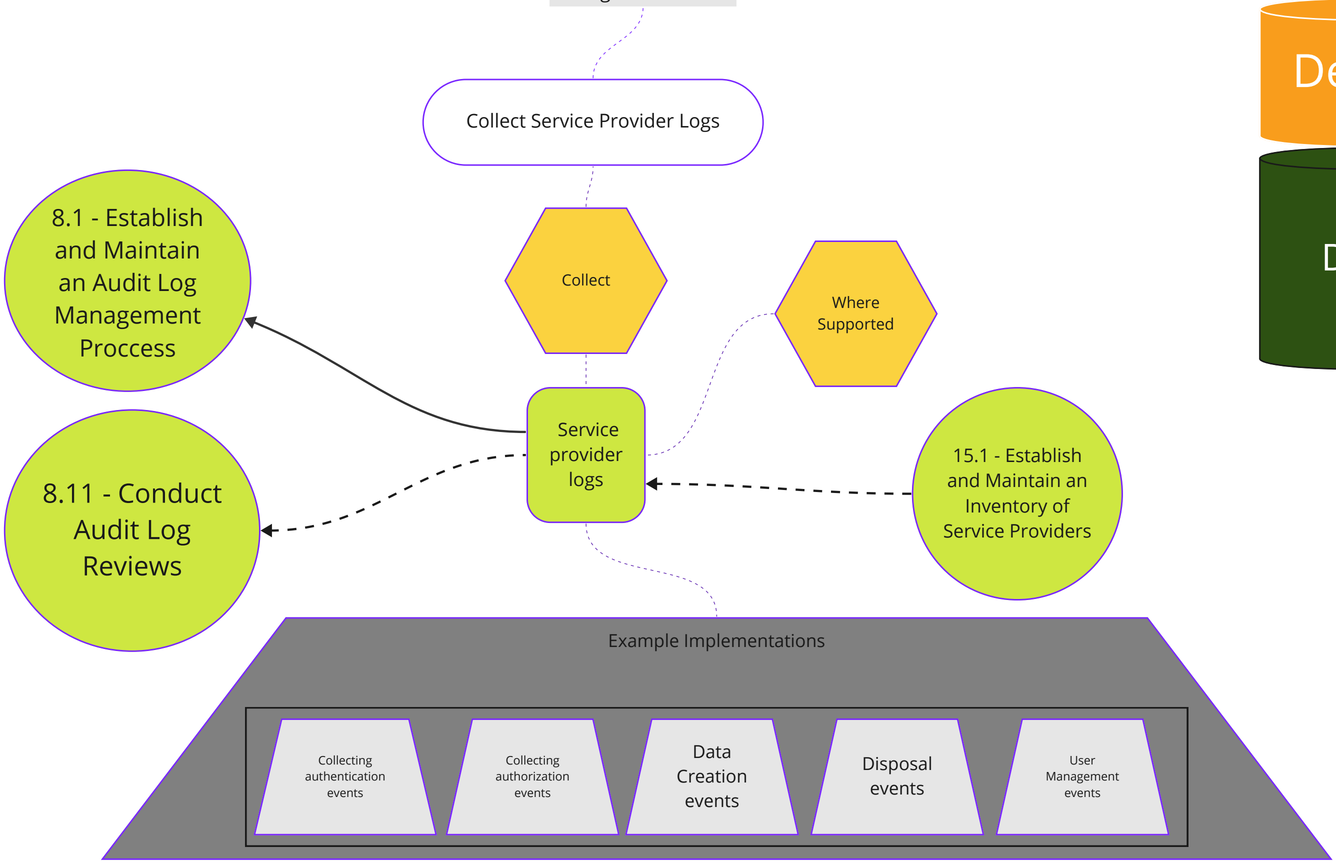
Anomalies

Abnormal events

Group Validated

8.12

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


Collect Service Provider Logs
Collect
Where Supported
8.1 - Establish and Maintain an Audit Log Management Proccess
Service provider logs
8.11 - Conduct Audit Log Reviews
15.1 - Establish and Maintain an Inventory of Service Providers
Example Implementations
Collecting authentication events
Collecting authorization events
Data Creation events
Disposal events
User Management events

IG3

Log Management

Detect

Data

Log Analytics and Centralization Tool

Secure Configuration Policy / Process

CONTROL 09

Email and Web Browser Protections

Safeguards Total 7 — IG1 2/7 — IG2 6/7 — IG3 7/7

Overview

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

Group Validated

9.1

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.

IG1

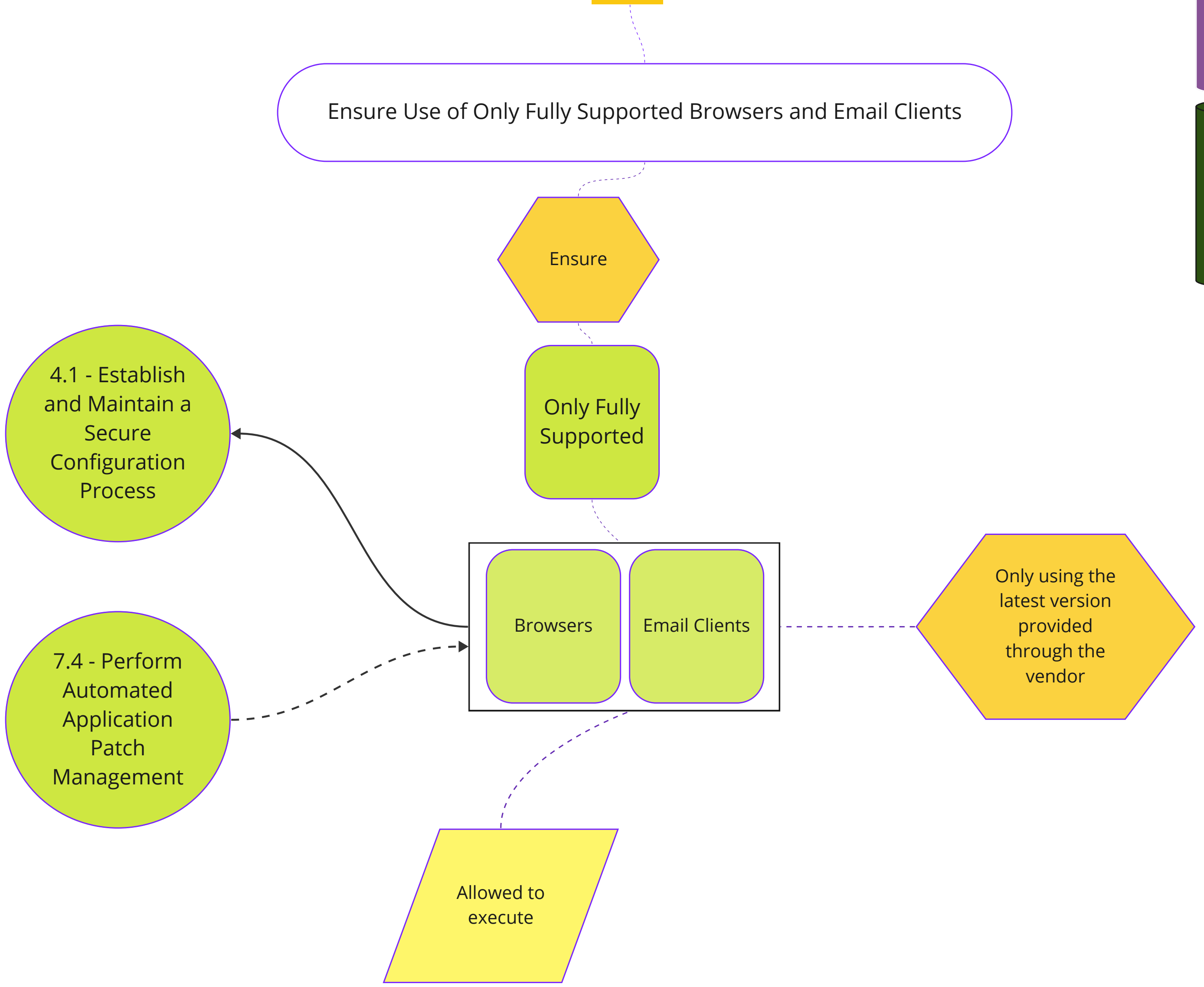
Protect

Applications

Asset Management

Enterprise and Software Asset Management Tool

Potentially OS Dependent



Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure

Only Fully Supported

Browsers

Email Clients

Only using the latest version provided through the vendor

Allowed to execute

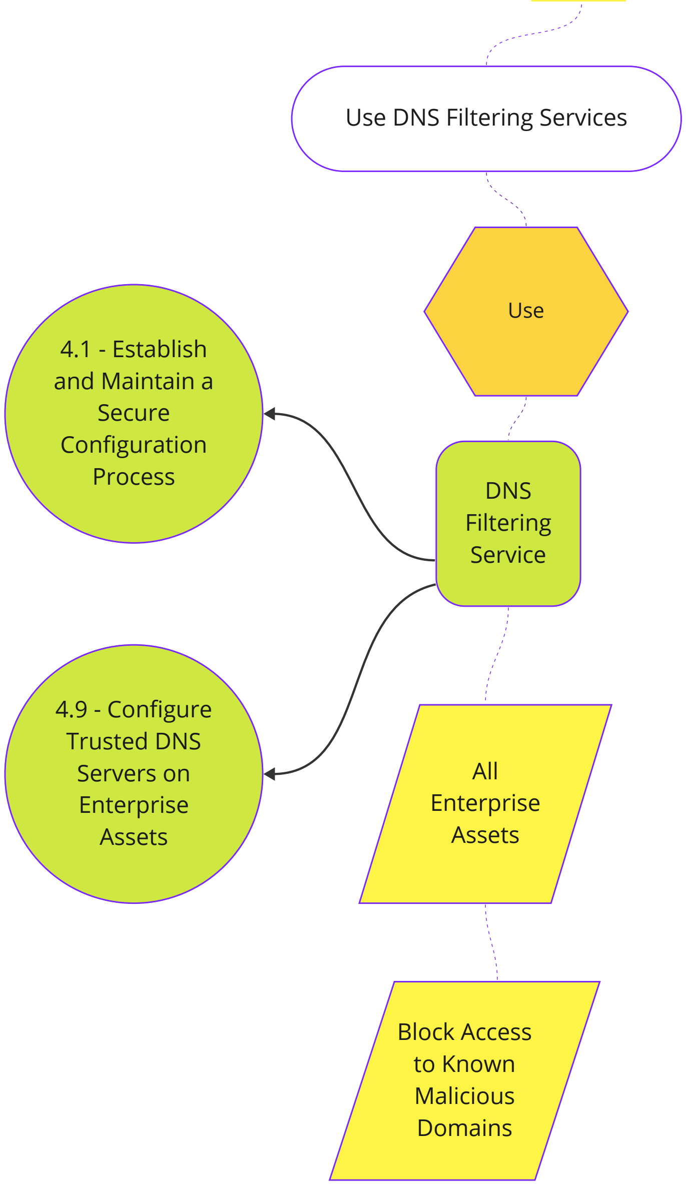
4.1 - Establish and Maintain a Secure Configuration Process

7.4 - Perform Automated Application Patch Management

Group Validated

9.2

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



Use DNS Filtering Services

Use

DNS Filtering Service

4.1 - Establish and Maintain a Secure Configuration Process

4.9 - Configure Trusted DNS Servers on Enterprise Assets

All Enterprise Assets

Block Access to Known Malicious Domains

IG1

Malware Defense

Protect

DNS Service/Server

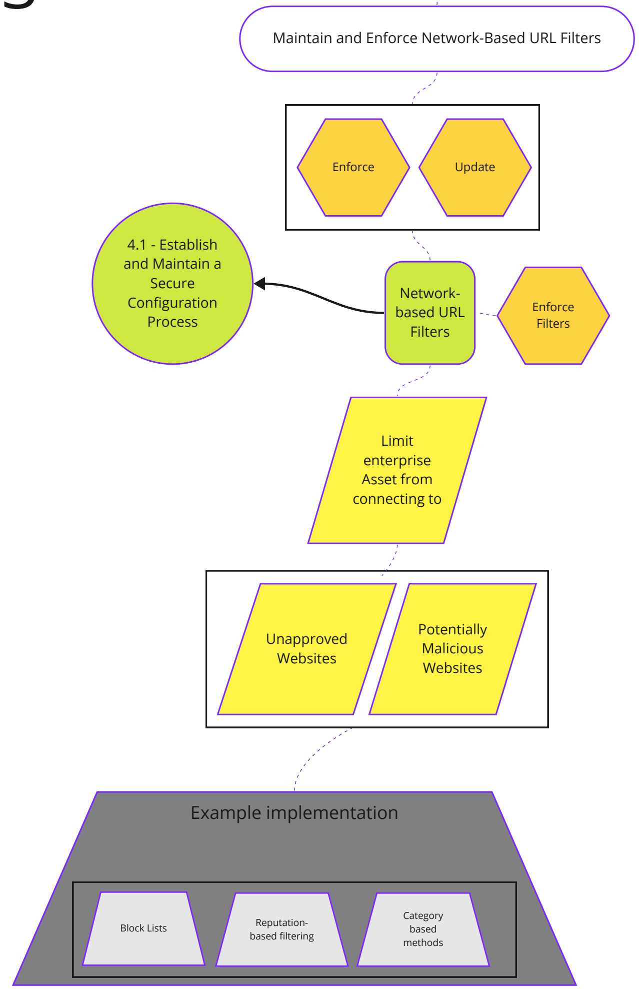
Network

Potentially OS Dependent

Group Validated

9.3

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.



Maintain and Enforce Network-Based URL Filters

Enforce

Update

4.1 - Establish and Maintain a Secure Configuration Process

Network-based URL Filters

Enforce Filters

Limit enterprise Asset from connecting to

Unapproved Websites

Potentially Malicious Websites

Example implementation

Block Lists

Reputation-based filtering

Category based methods

IG2

Malware Defense

Protect

URL Filtering Tool

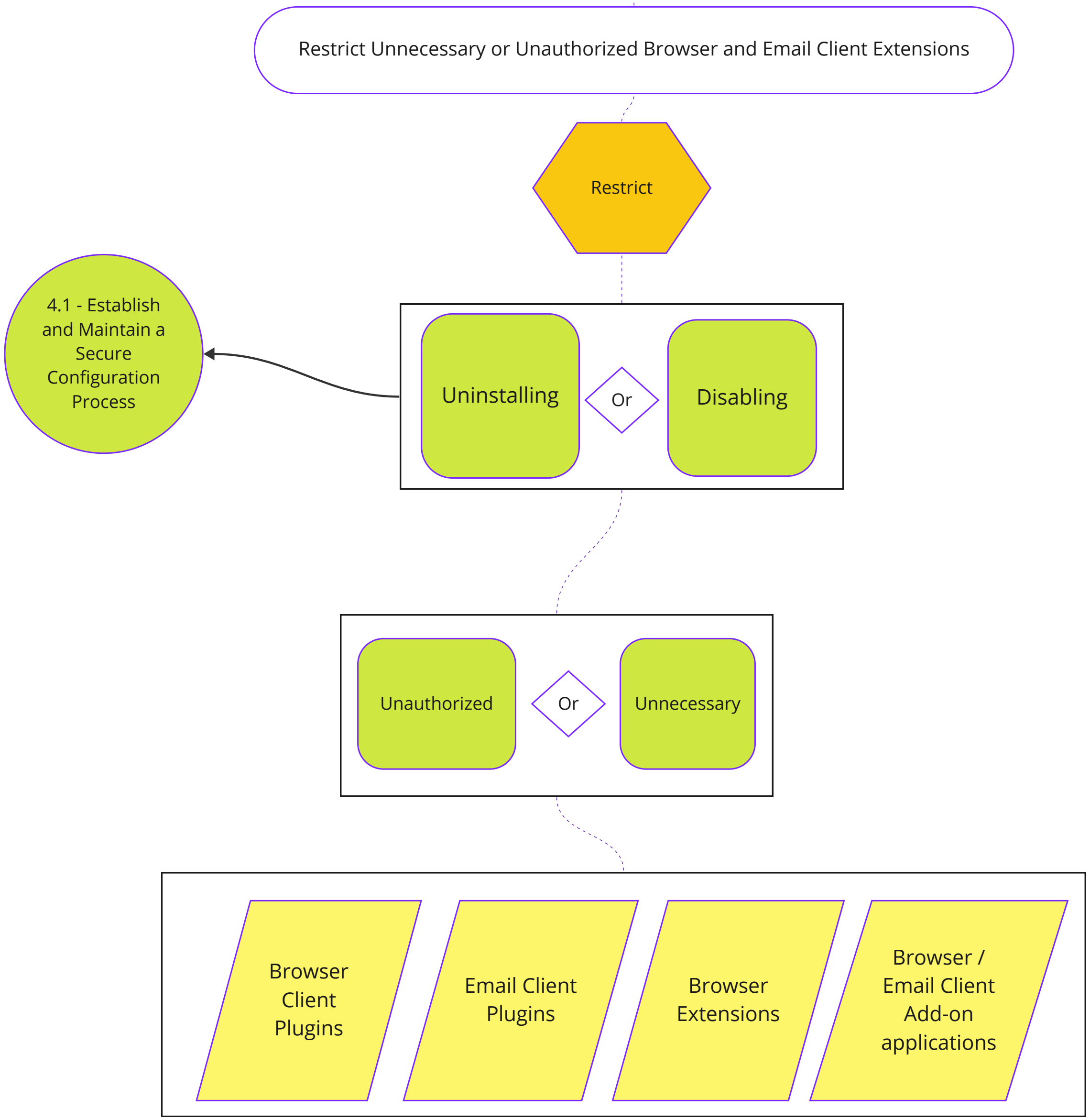
Network

Potentially OS Dependent

Group Validated

9.4

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



Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Restrict

Uninstalling

Or

Disabling

4.1 - Establish and Maintain a Secure Configuration Process

Unauthorized

Or

Unnecessary

Browser Client Plugins

Email Client Plugins

Browser Extensions

Browser / Email Client Add-on applications

IG2

Secure Configurations

Protect

Configuration Management Tool

Applications

Potentially OS Dependent

Group Validated

9.5

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.

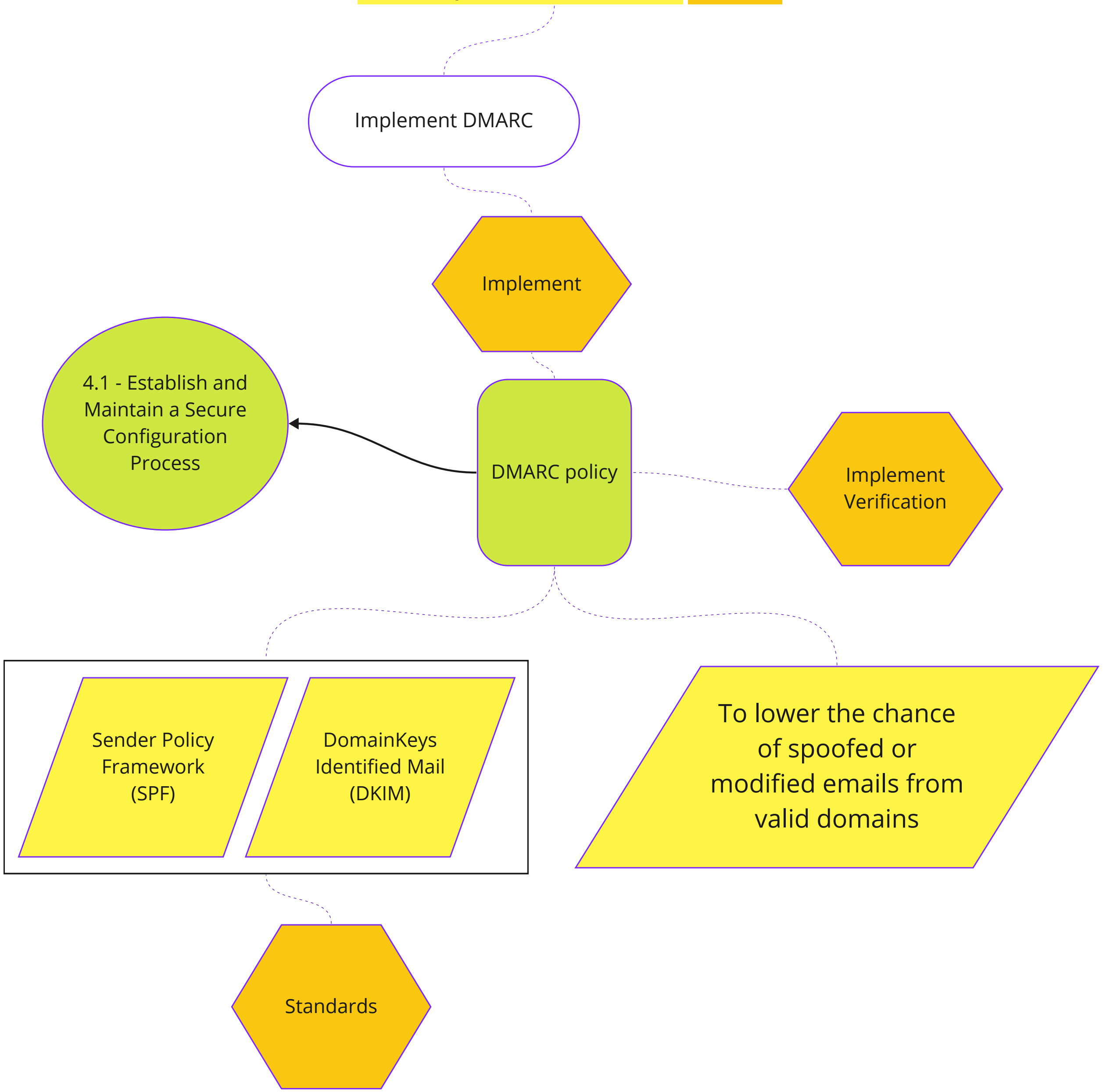
IG2

Protect

Network

Malware Defense

DMARC Management Tool



Implement DMARC

Implement

4.1 - Establish and Maintain a Secure Configuration Process

DMARC policy

Implement Verification

Sender Policy Framework (SPF)

DomainKeys Identified Mail (DKIM)

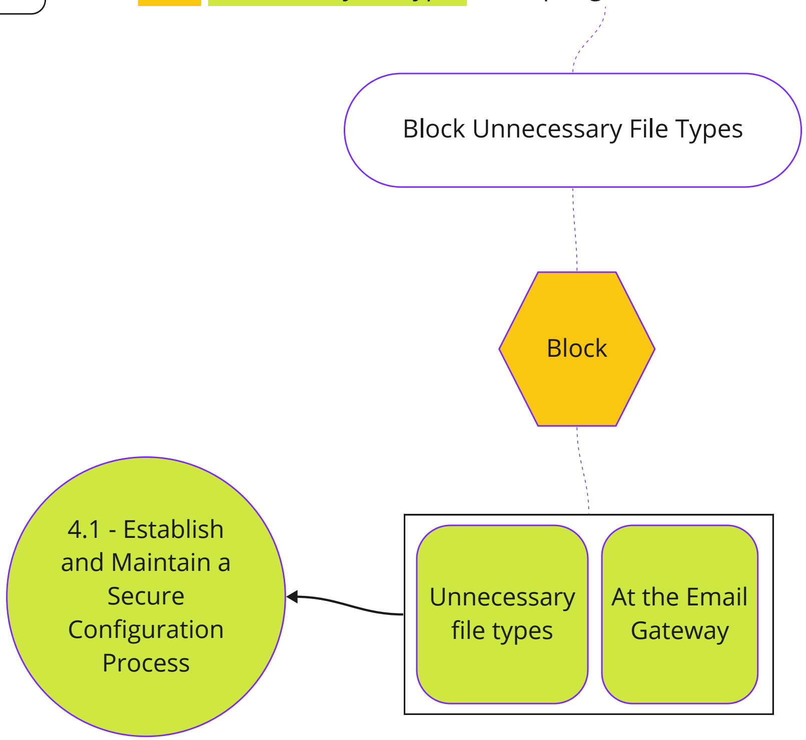
To lower the chance of spoofed or modified emails from valid domains

Standards

Group Validated

9.6

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



Block Unnecessary File Types

Block

Unnecessary file types

At the Email Gateway

4.1 - Establish and Maintain a Secure Configuration Process

IG2

Malware Defense

Protect

Network

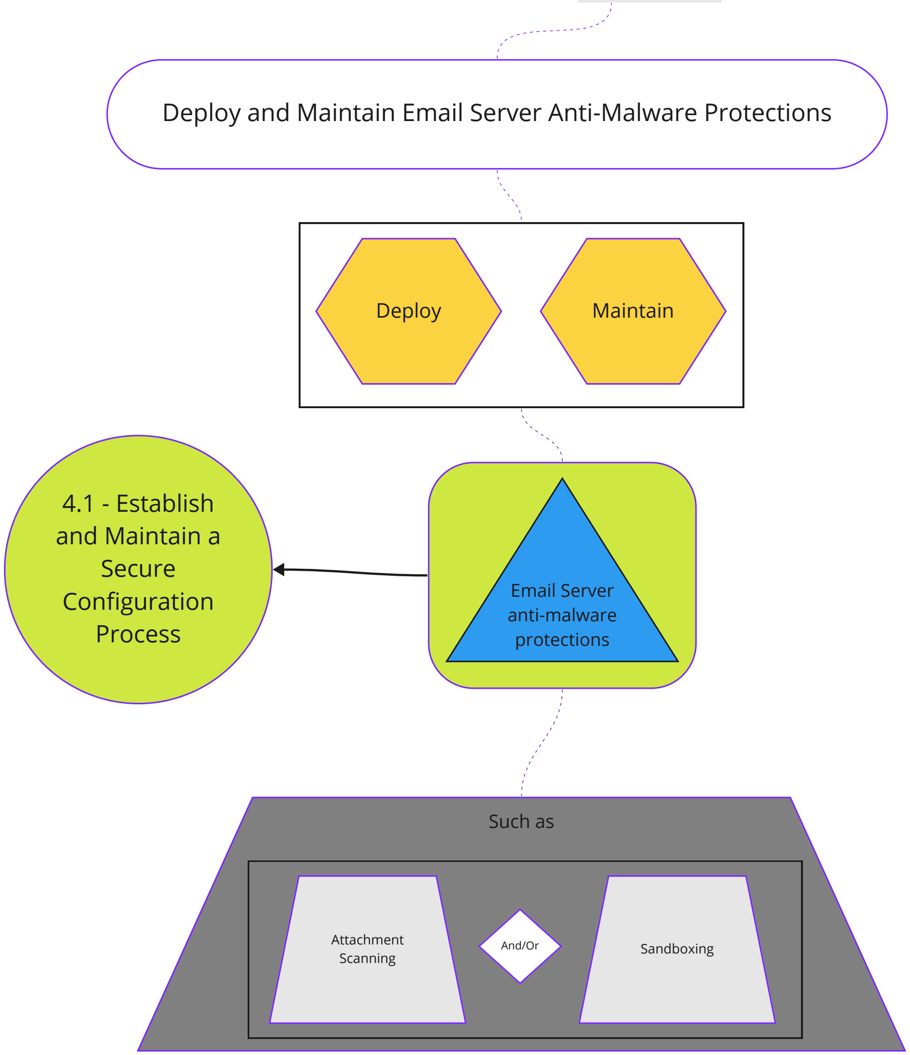
Email Security Tool

Potentially OS Dependent

Group Validated

9.7

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



Deploy and Maintain Email Server Anti-Malware Protections

Deploy

Maintain

Email Server anti-malware protections

4.1 - Establish and Maintain a Secure Configuration Process

Such as

Attachment Scanning

And/Or

Sandboxing

IG1

Malware Defense

Protect

Email Security Tool

Network

CONTROL 10

Malware Defenses

Safeguards Total 7	IG1 3/7	IG2 7/7	IG3 7/7

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

Group Validated

10.1

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

IG1

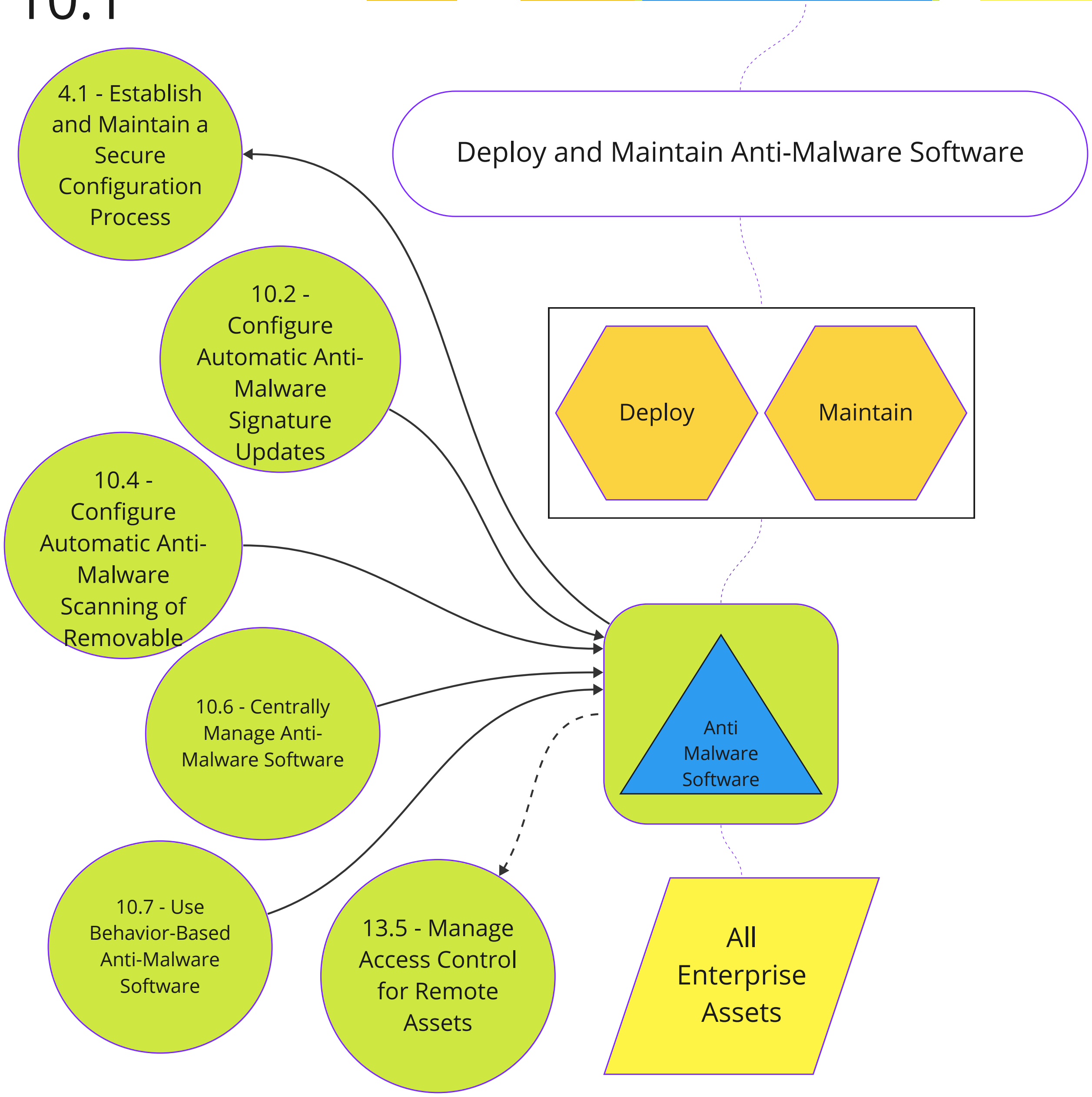
Malware Defense

Protect

Anti-Malware Software

Devices

OS Dependent



Deploy and Maintain Anti-Malware Software

Deploy

Maintain

Anti Malware Software

All Enterprise Assets

4.1 - Establish and Maintain a Secure Configuration Process

10.2 - Configure Automatic Anti-Malware Signature Updates

10.4 - Configure Automatic Anti-Malware Scanning of Removable

10.6 - Centrally Manage Anti-Malware Software

10.7 - Use Behavior-Based Anti-Malware Software

13.5 - Manage Access Control for Remote Assets

Group Validated

10.2

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

IG1

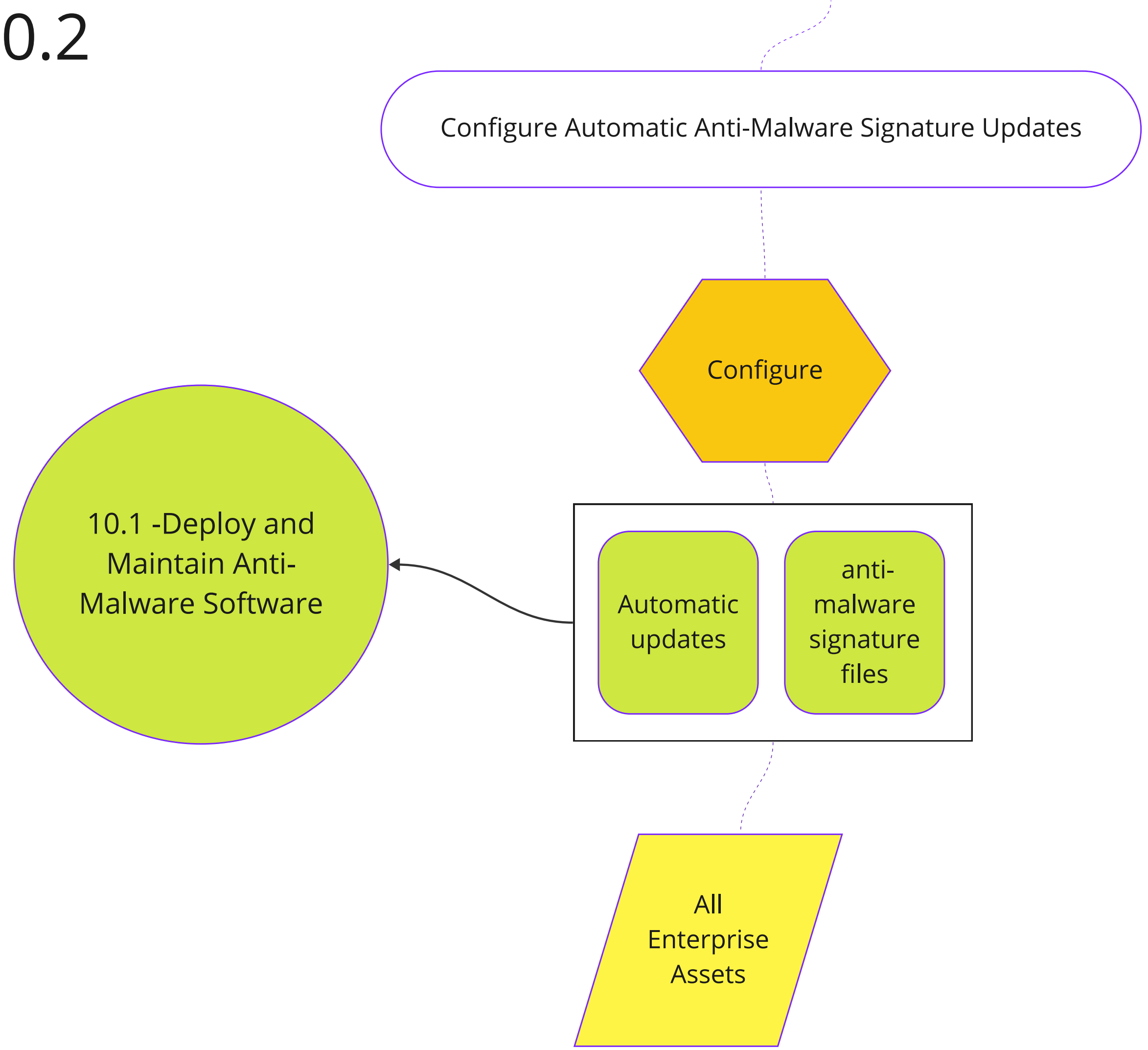
Malware Defense

Protect

Devices

Anti-Malware Software

OS Dependent



Configure Automatic Anti-Malware Signature Updates

Configure

Automatic updates

anti-malware signature files

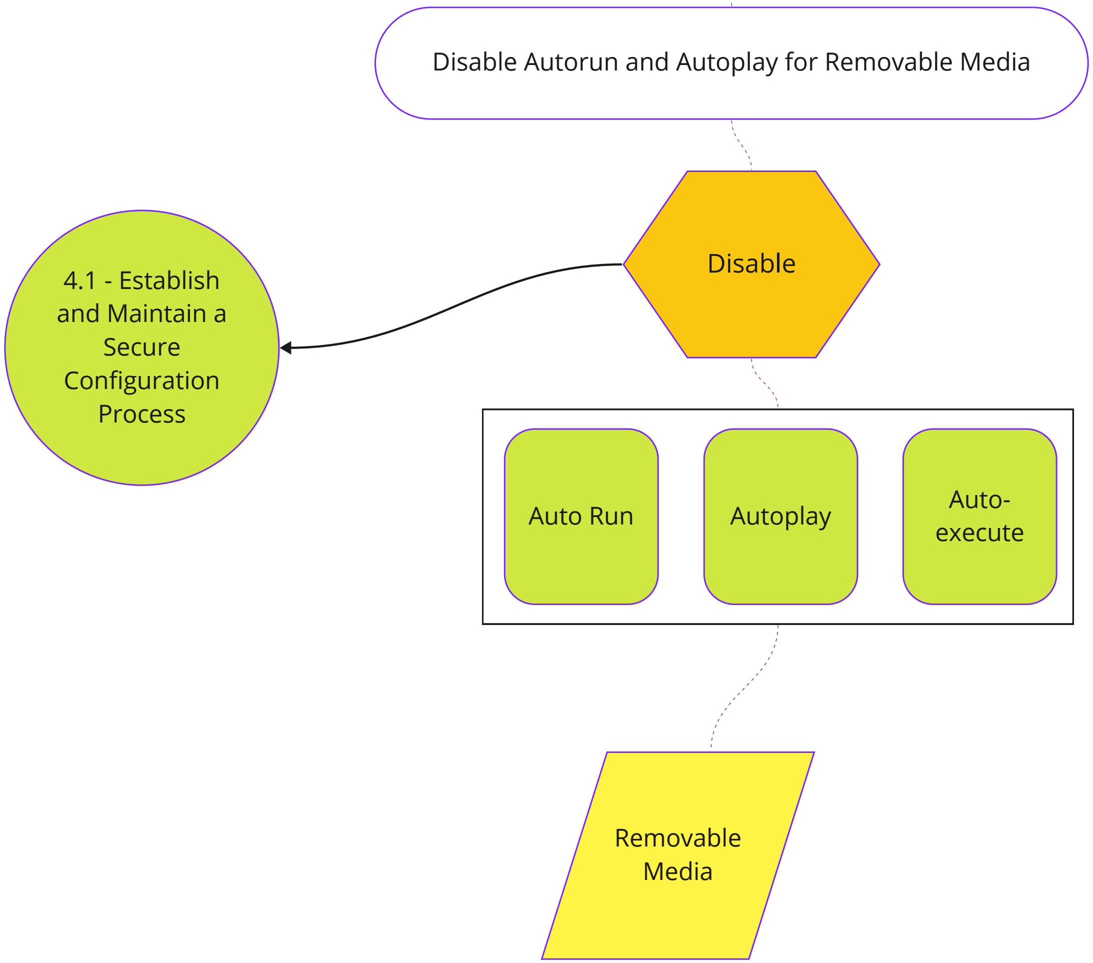
10.1 -Deploy and Maintain Anti-Malware Software

All Enterprise Assets

Group Validated

10.3

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



Disable Autorun and Autoplay for Removable Media

Disable

4.1 - Establish and Maintain a Secure Configuration Process

Auto Run

Autoplay

Auto-execute

Removable Media

IG1

Secure Configurations

Protect

Configuration Management Tool

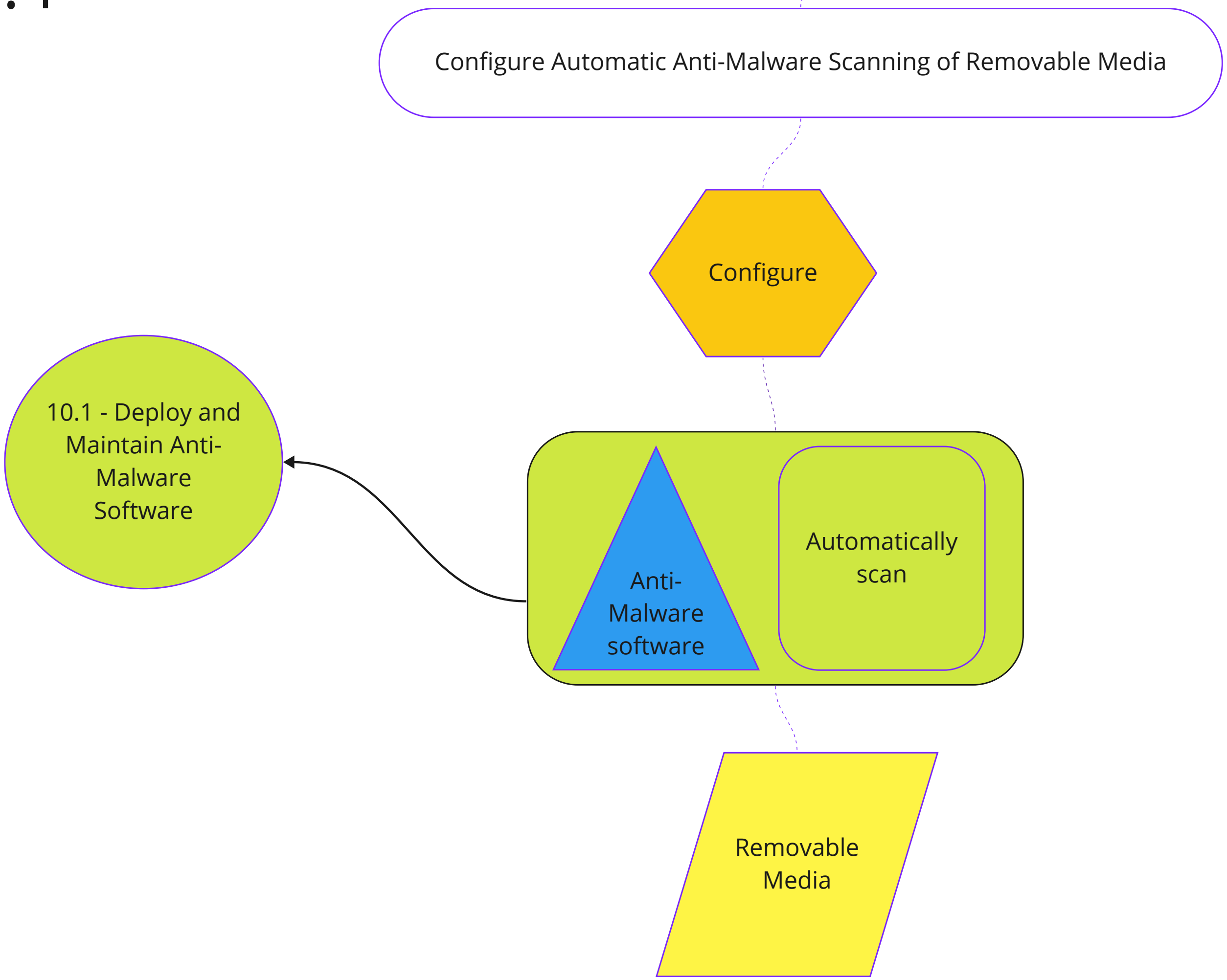
Devices

OS Dependent

Group Validated

10.4

Configure anti-malware software to automatically scan removable media.



Configure Automatic Anti-Malware Scanning of Removable Media

Configure

Anti-Malware software

Automatically scan

10.1 - Deploy and Maintain Anti-Malware Software

Removable Media

IG2

Malware Defense

Detect

Devices

Anti-Malware Software Configuration Policy / Process

Anti-Malware Software

OS Dependent

Group Validated

10.5

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 GatekeeperTM.

IG2

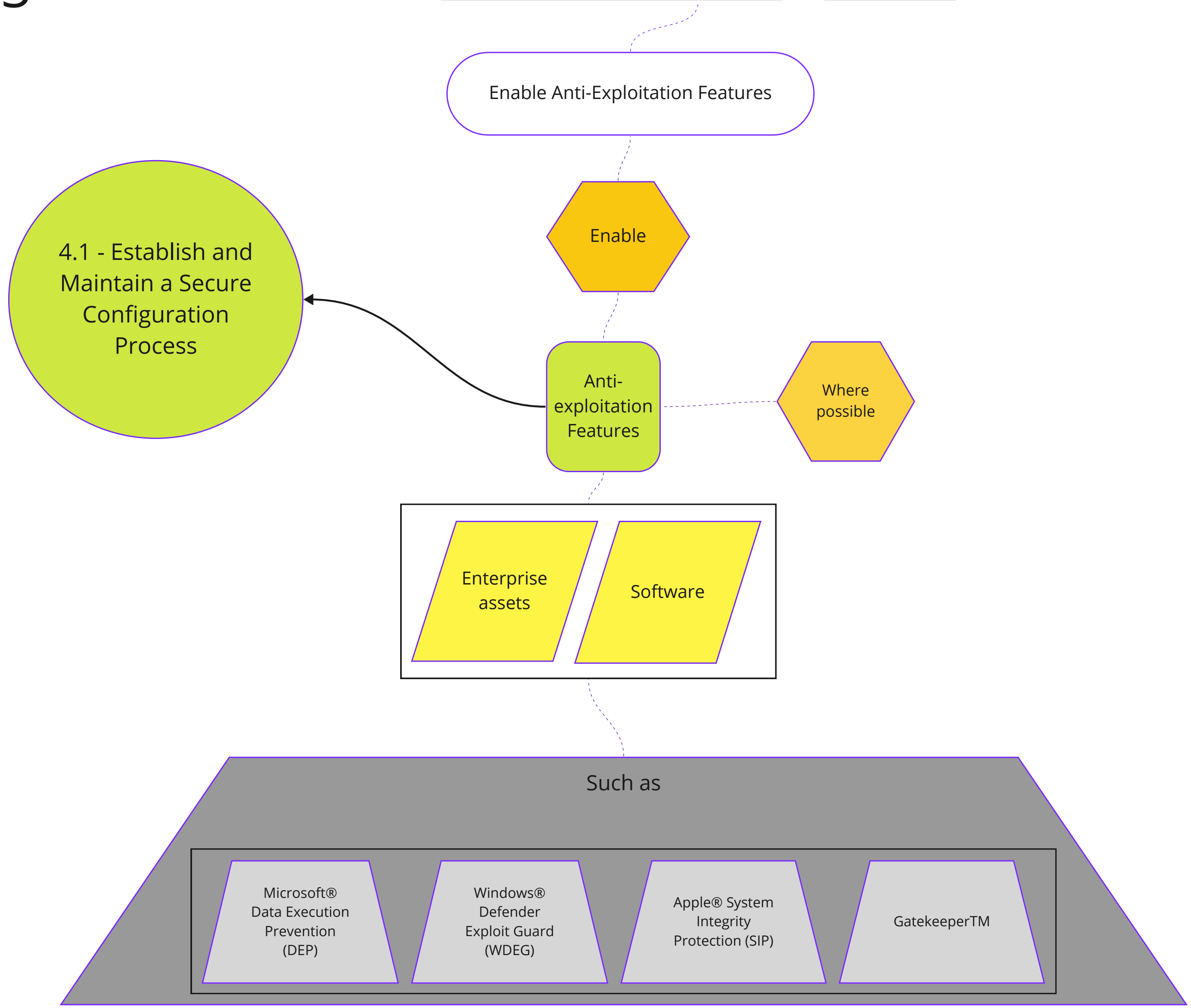
Secure Configurations

Protect

Configuration Management Tool

Devices

OS Dependent



Enable Anti-Exploitation Features

Enable

4.1 - Establish and Maintain a Secure Configuration Process

Anti-exploitation Features

Where possible

Enterprise assets

Software

Such as

Microsoft® Data Execution Prevention (DEP)

Windows® Defender Exploit Guard (WDEG)

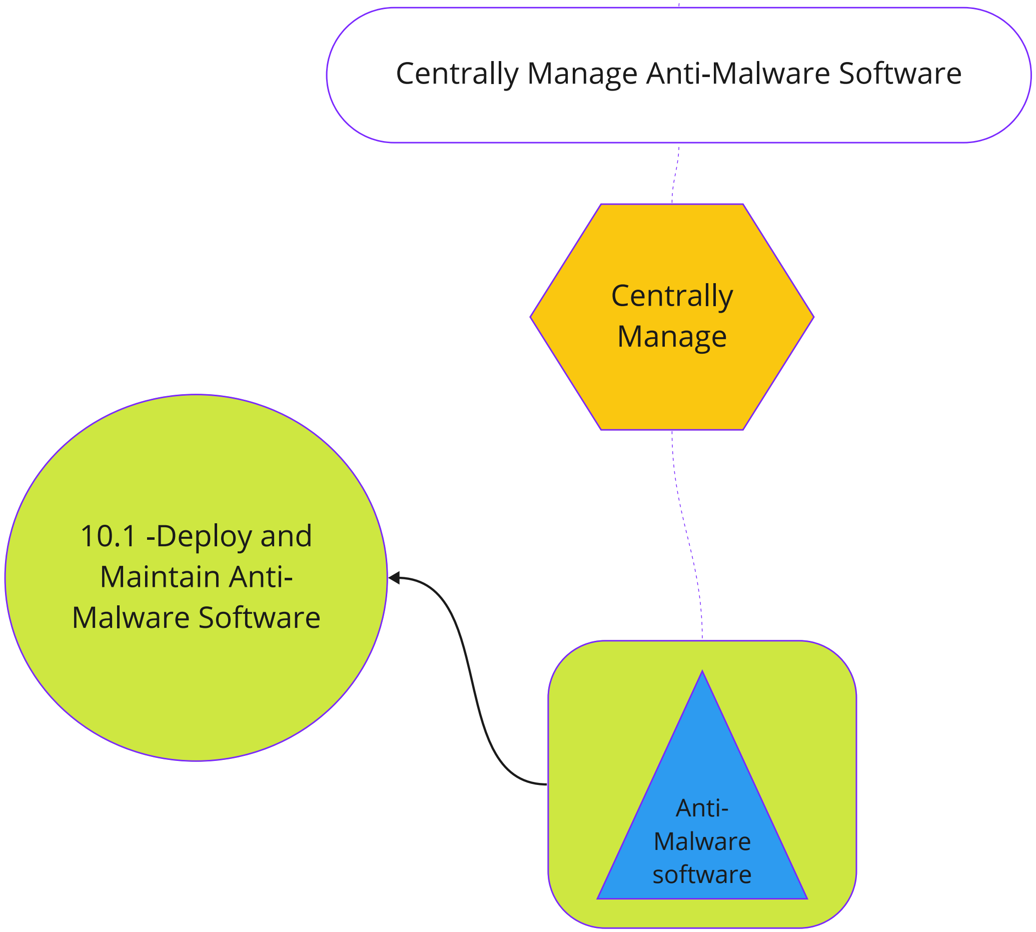
Apple® System Integrity Protection (SIP)

GatekeeperTM

Group Validated

10.6

Centrally manage anti-malware software.



Centrally Manage Anti-Malware Software

Centrally Manage

Anti-Malware software

10.1 -Deploy and Maintain Anti-Malware Software

IG2

Malware Defense

Protect

Anti-Malware Software Configuration Policy / Process

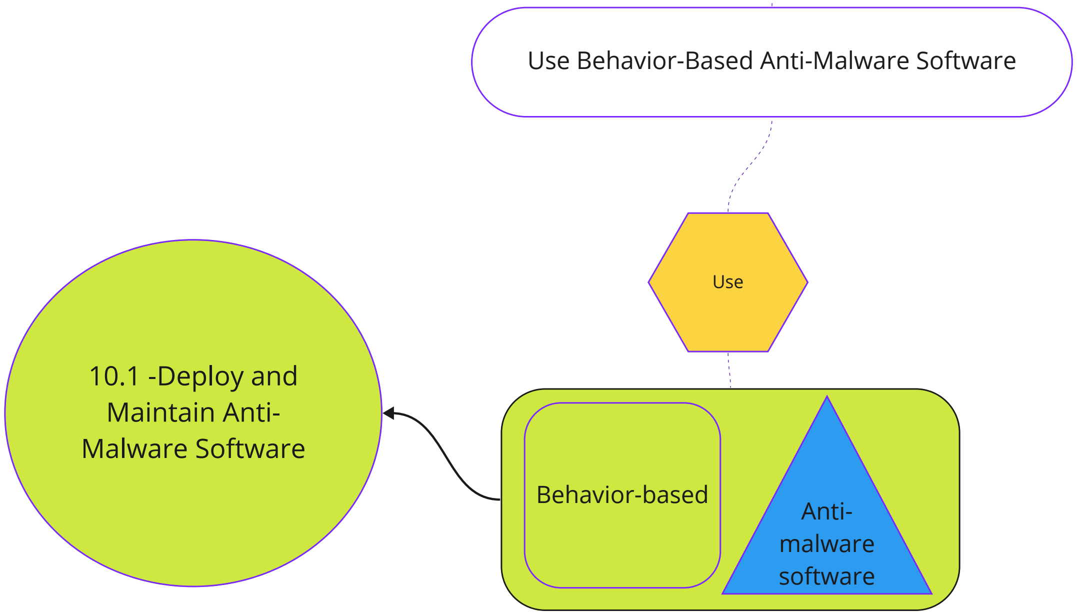
Devices

Anti-Malware Software

Group Validated

10.7

Use behavior-based anti-malware software.



Use Behavior-Based Anti-Malware Software

Use

Behavior-based

Anti-malware software

10.1 -Deploy and Maintain Anti-Malware Software

IG2

Malware Defense

Detect

Devices

Anti-Malware Software Configuration Policy / Process

Anti-Malware Software

CONTROL 11

Data Recovery

SAFEGUARDS TOTAL	IG1	IG2	IG3
5	4/5	5/5	5/5

Overview

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

Group Validated

11.1

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.

Process Oriented Safeguard

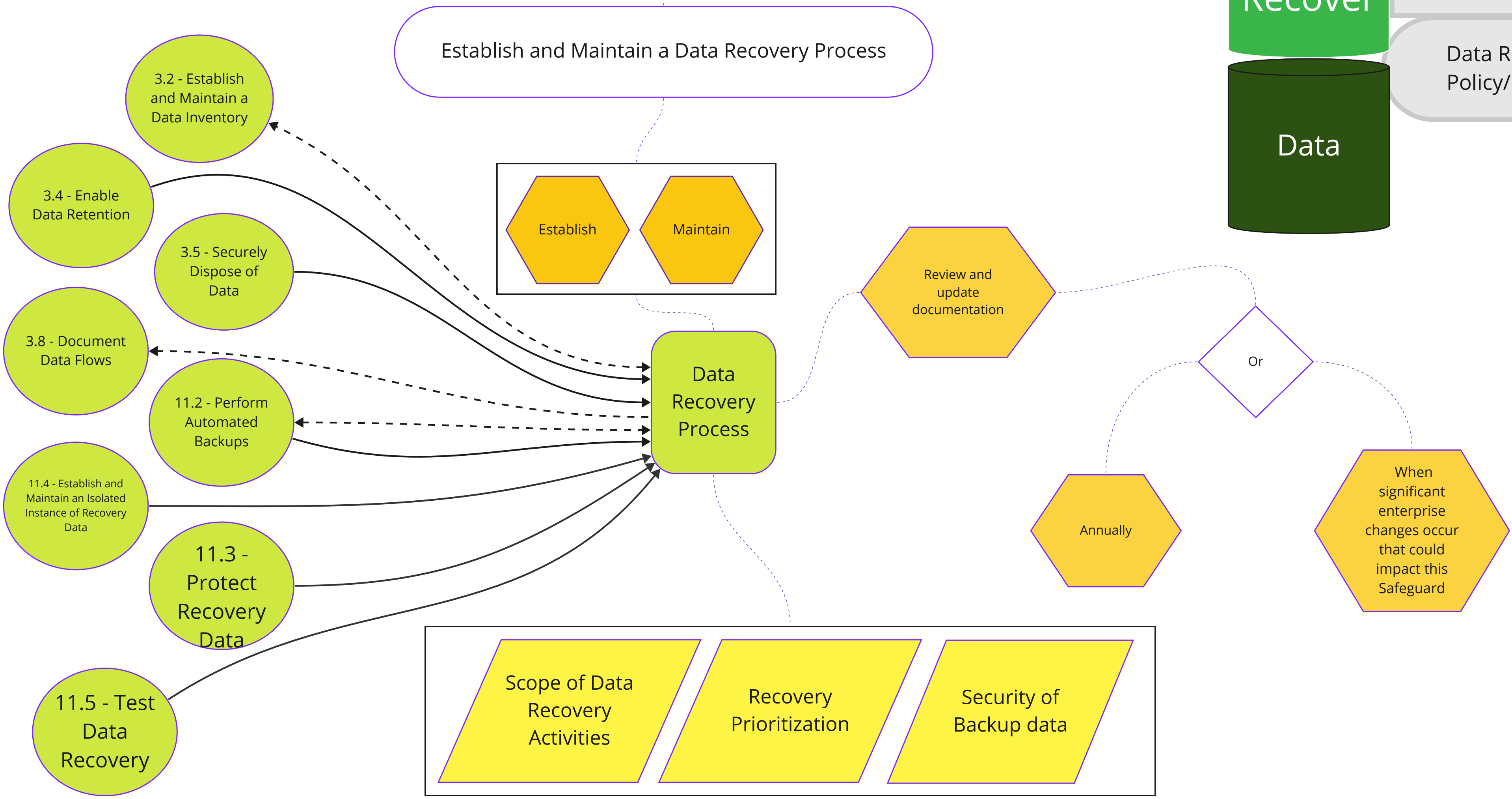
IG1

Data Recovery

Recover

Data

Data Recovery Policy/Process



Establish and Maintain a Data Recovery Process

Establish

Maintain

Data Recovery Process

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Scope of Data Recovery Activities

Recovery Prioritization

Security of Backup data

3.2 - Establish and Maintain a Data Inventory

3.4 - Enable Data Retention

3.5 - Securely Dispose of Data

3.8 - Document Data Flows

11.2 - Perform Automated Backups

11.4 - Establish and Maintain an Isolated Instance of Recovery Data

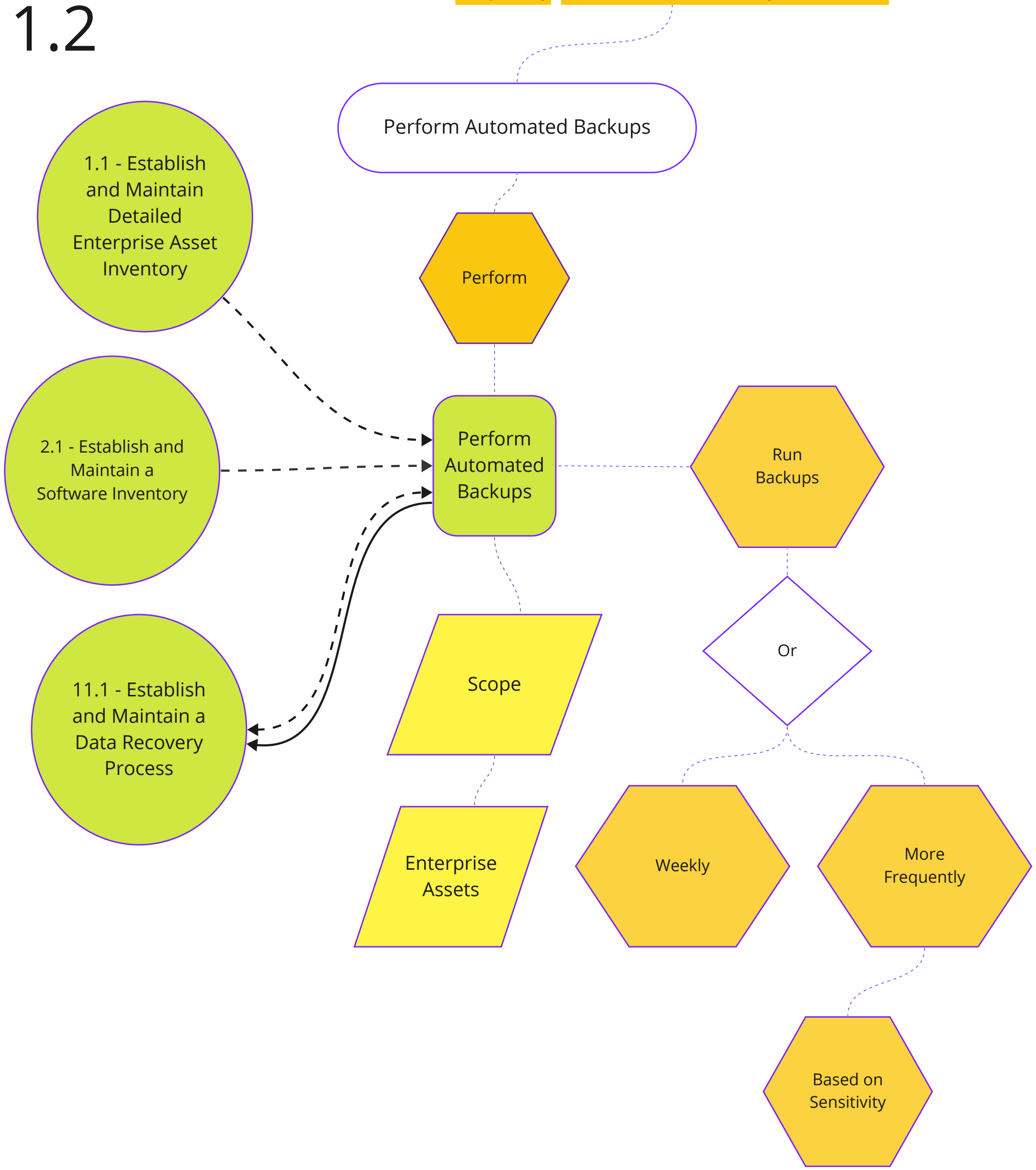
11.3 - Protect Recovery Data

11.5 - Test Data Recovery

Group Validated

11.2

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



Perform Automated Backups

Perform

Perform Automated Backups

Run Backups

Or

Weekly

More Frequently

Based on Sensitivity

Scope

Enterprise Assets

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

2.1 - Establish and Maintain a Software Inventory

11.1 - Establish and Maintain a Data Recovery Process

IG1

Recover

Data

Data Recovery

Data Backup and Recovery Tool

Group Validated

11.3

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

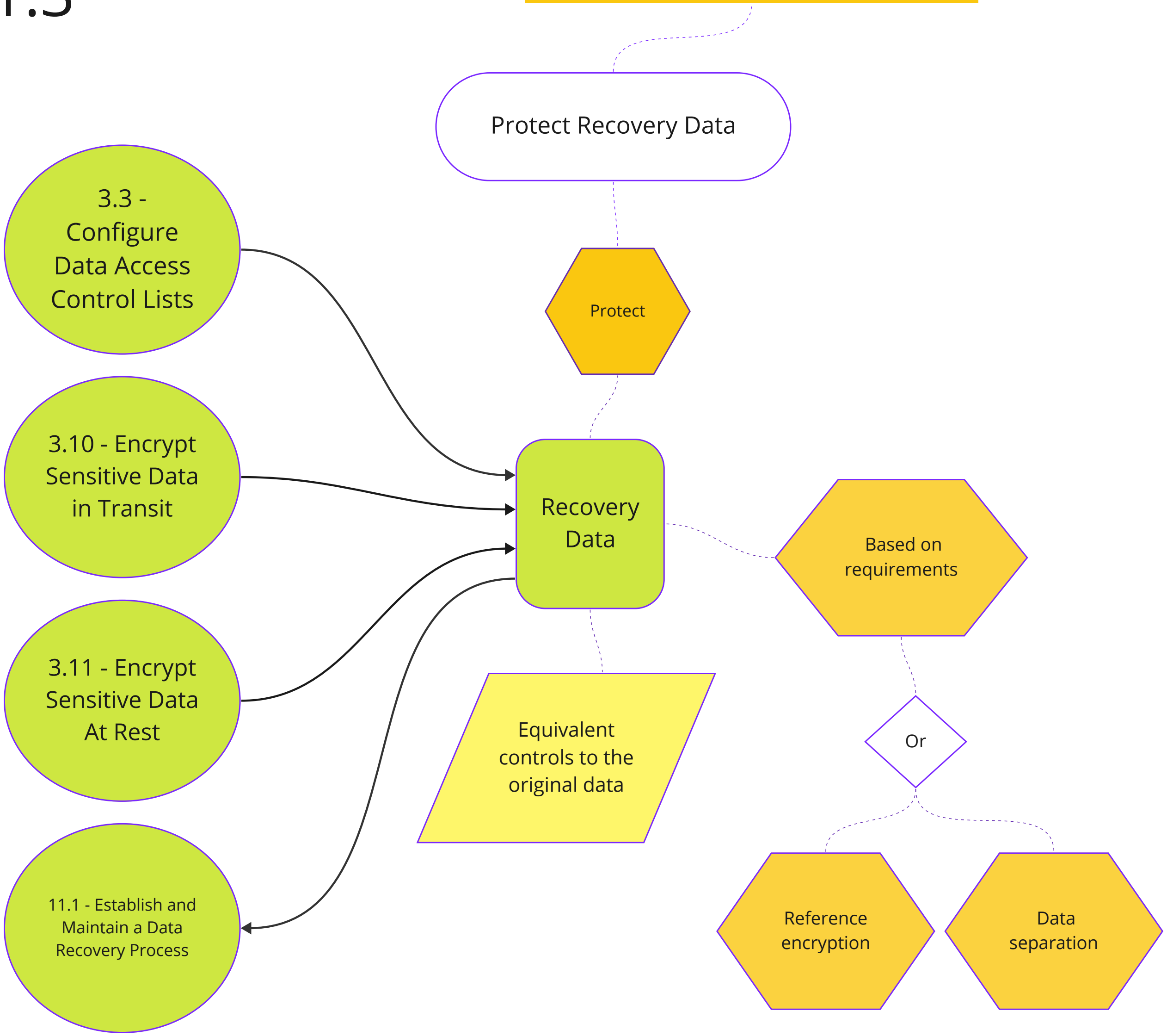
IG1

Protect

Data

Data Recovery

Data Backup and Recovery Tool



Protect Recovery Data

Protect

Recovery Data

3.3 - Configure Data Access Control Lists

3.10 - Encrypt Sensitive Data in Transit

3.11 - Encrypt Sensitive Data At Rest

11.1 - Establish and Maintain a Data Recovery Process

Equivalent controls to the original data

Based on requirements

Or

Reference encryption

Data separation

Group Validated

11.4

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.

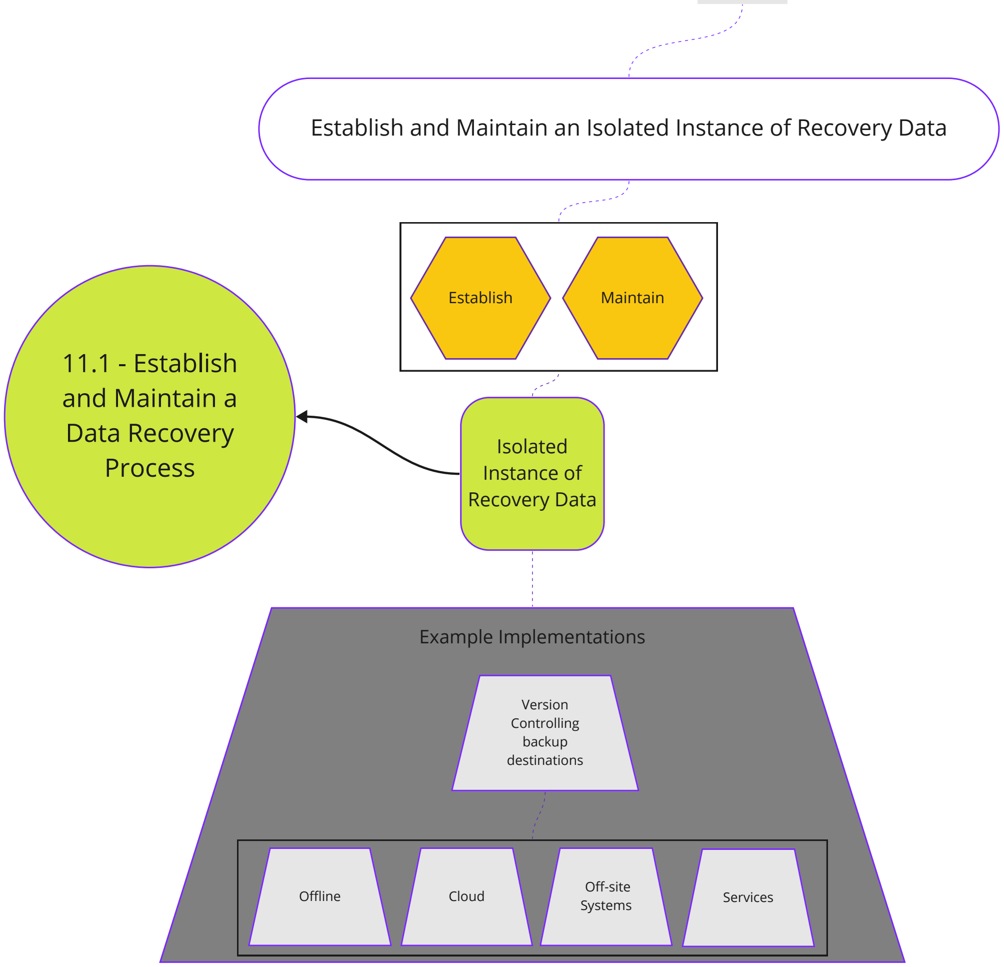
IG1

Data Recovery

Recover

Data

Data Backup and Recovery Tool



Establish and Maintain an Isolated Instance of Recovery Data

Establish

Maintain

Isolated Instance of Recovery Data

11.1 - Establish and Maintain a Data Recovery Process

Example Implementations

Version Controlling backup destinations

Offline

Cloud

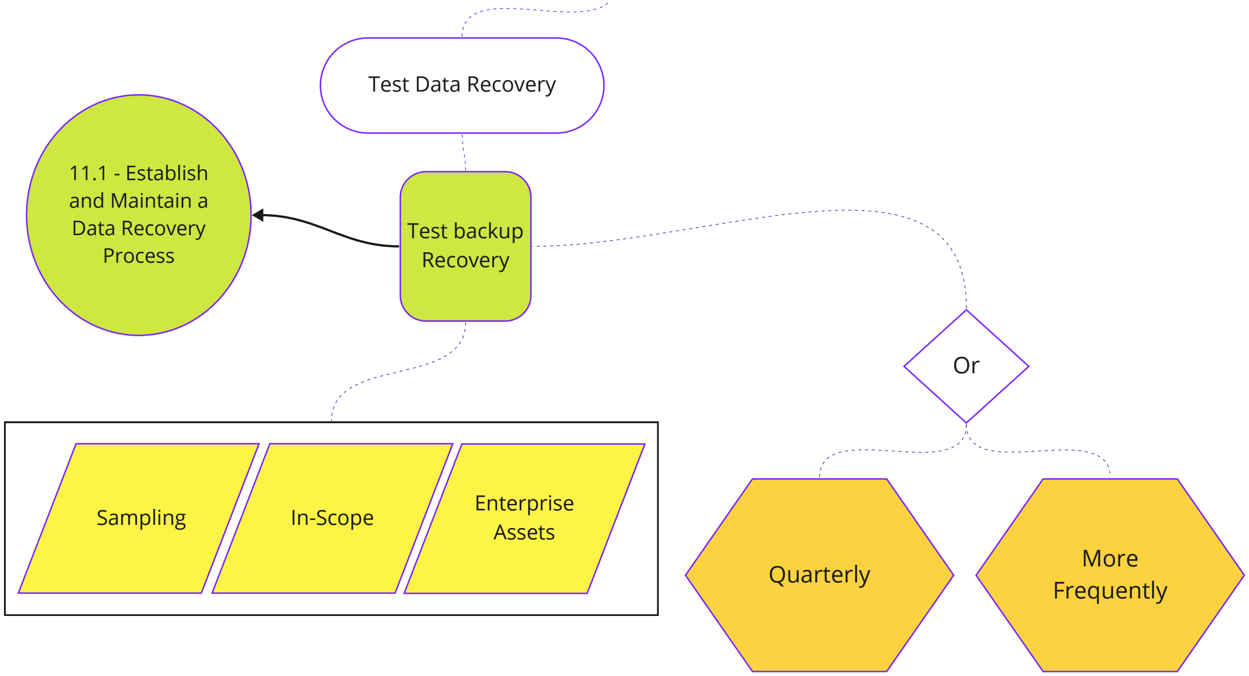
Off-site Systems

Services

Group Validated

11.5

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



Test Data Recovery

Test backup Recovery

11.1 - Establish and Maintain a Data Recovery Process

Sampling

In-Scope

Enterprise Assets

Or

Quarterly

More Frequently

IG2

Recover

Data

Data Recovery

Data Recovery Policy/Process

Data Backup and Recovery Tool

CONTROL 12

Network Infrastructure Management

SAFEGUARDS TOTAL	IG1	IG2	IG3
8	1/8	7/8	8/8

Overview

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

Group Validated

12.1

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.

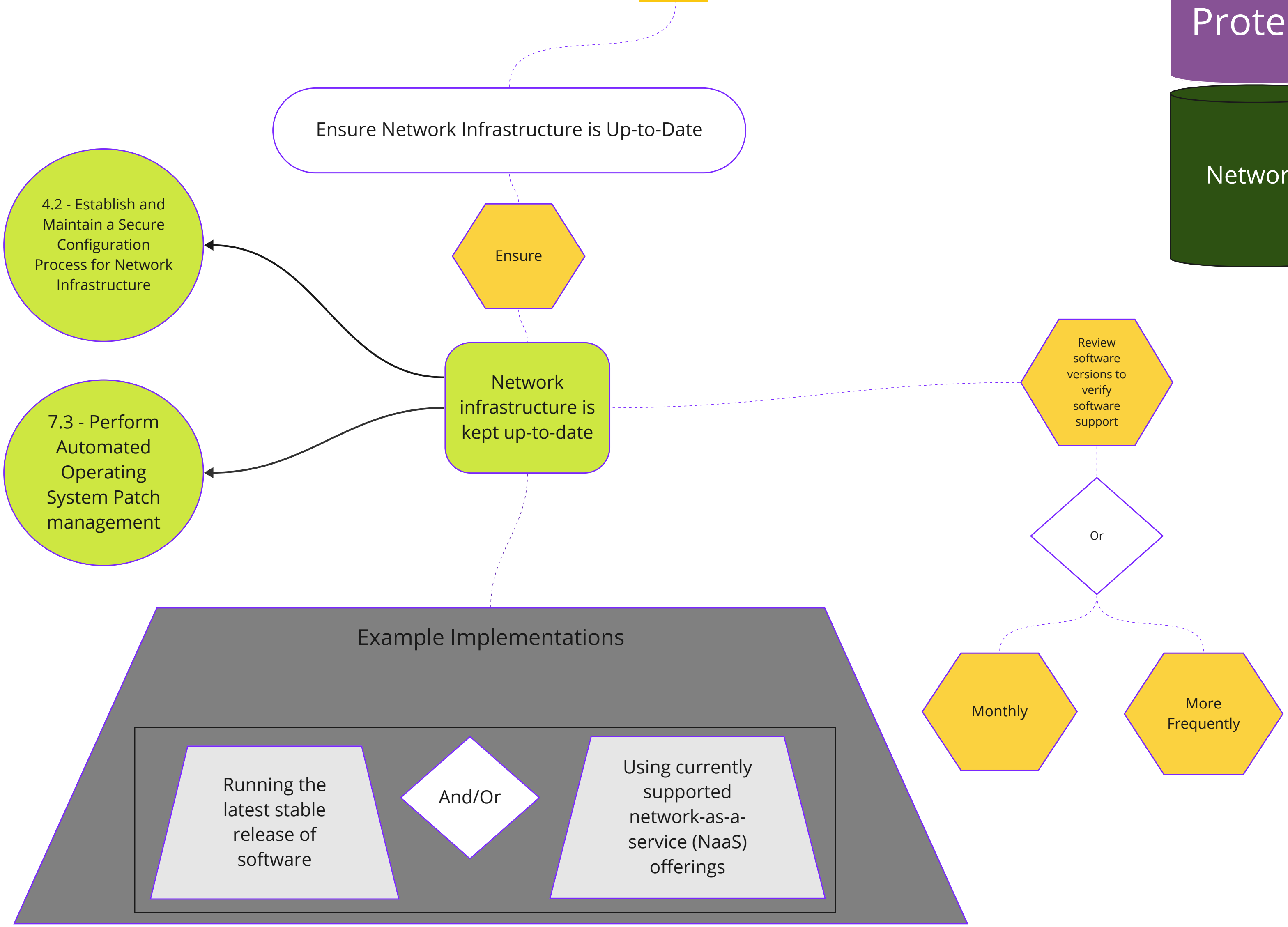
IG1

Protect

Network

Asset Management

Enterprise and Software Asset Management Tool



Ensure Network Infrastructure is Up-to-Date

Ensure

Network infrastructure is kept up-to-date

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

7.3 - Perform Automated Operating System Patch management

Review software versions to verify software support

Or

Monthly

More Frequently

Example Implementations

Running the latest stable release of software

And/Or

Using currently supported network-as-a-service (NaaS) offerings

Group Validated

12.2

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

Process Oriented Safeguard

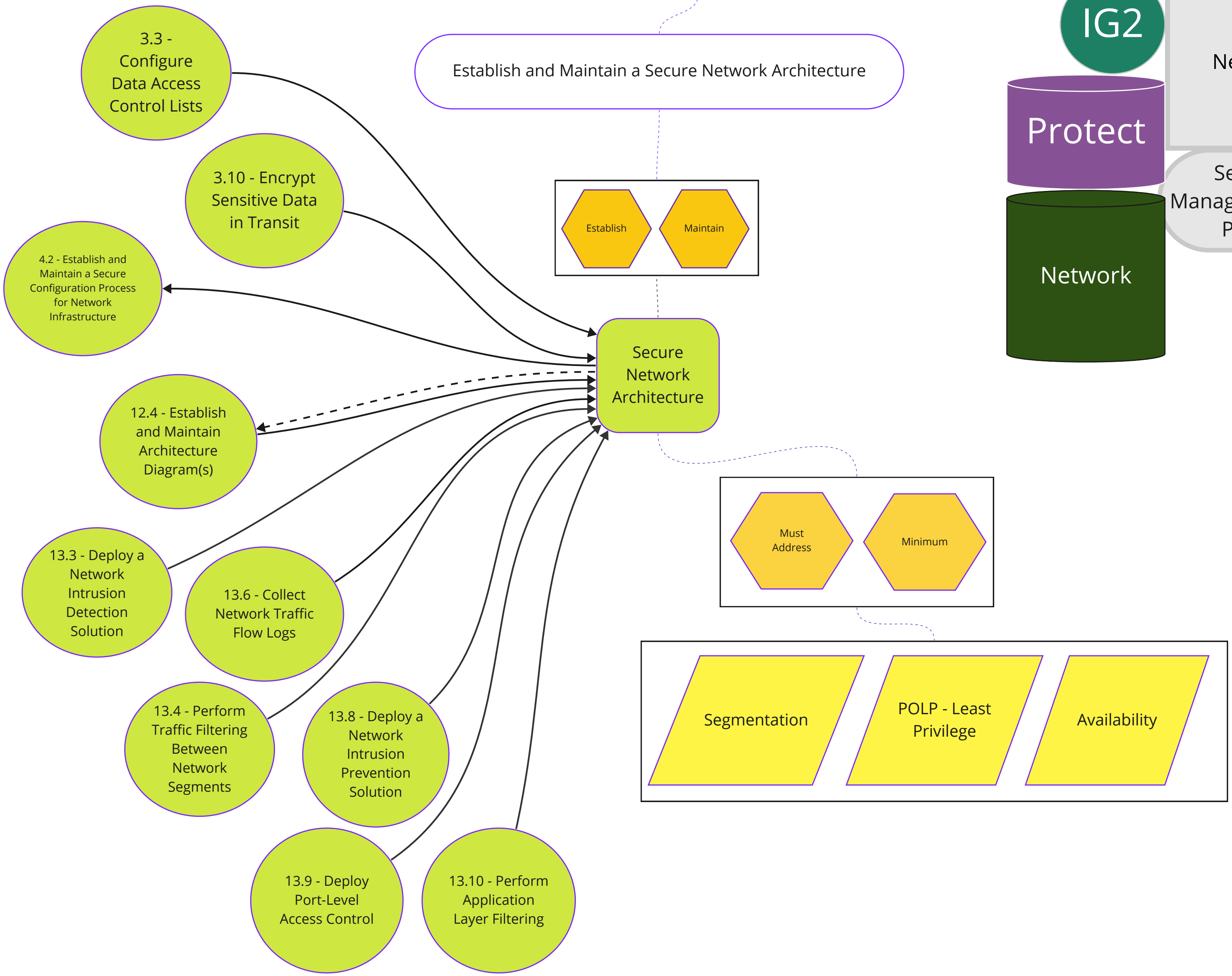
IG2

Network Security

Protect

Secure Network Management and Design Policy/Process

Network



Establish and Maintain a Secure Network Architecture

Establish

Maintain

Secure Network Architecture

Must Address

Minimum

Segmentation

POLP - Least Privilege

Availability

3.3 - Configure Data Access Control Lists

3.10 - Encrypt Sensitive Data in Transit

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

12.4 - Establish and Maintain Architecture Diagram(s)

13.3 - Deploy a Network Intrusion Detection Solution

13.6 - Collect Network Traffic Flow Logs

13.4 - Perform Traffic Filtering Between Network Segments

13.8 - Deploy a Network Intrusion Prevention Solution

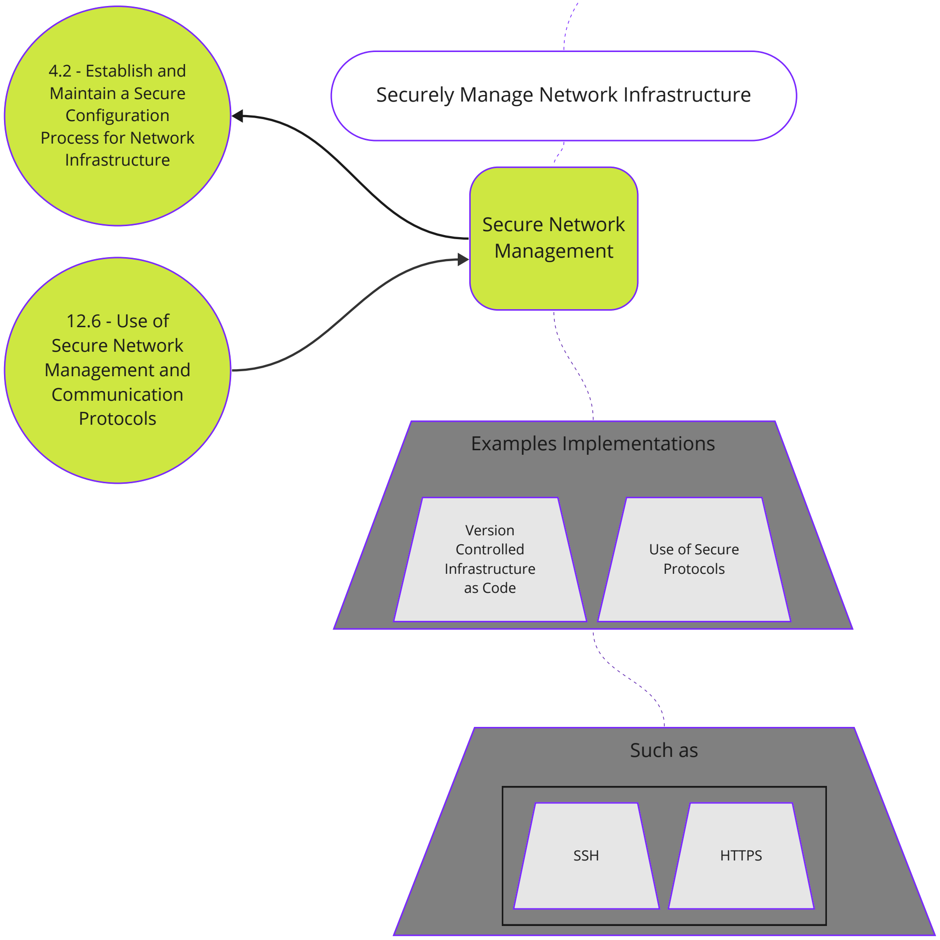
13.9 - Deploy Port-Level Access Control

13.10 - Perform Application Layer Filtering

Group Validated

12.3

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



Securely Manage Network Infrastructure

Secure Network Management

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

12.6 - Use of Secure Network Management and Communication Protocols

Examples Implementations

Version Controlled Infrastructure as Code

Use of Secure Protocols

Such as

SSH

HTTPS

Process Oriented Safeguard

IG2

Network Security

Protect

Network

Secure Network Management and Design Policy/Process

Network Management and Monitoring Tool

Group Validated

12.4

Process Oriented Safeguard

IG2

Network Security

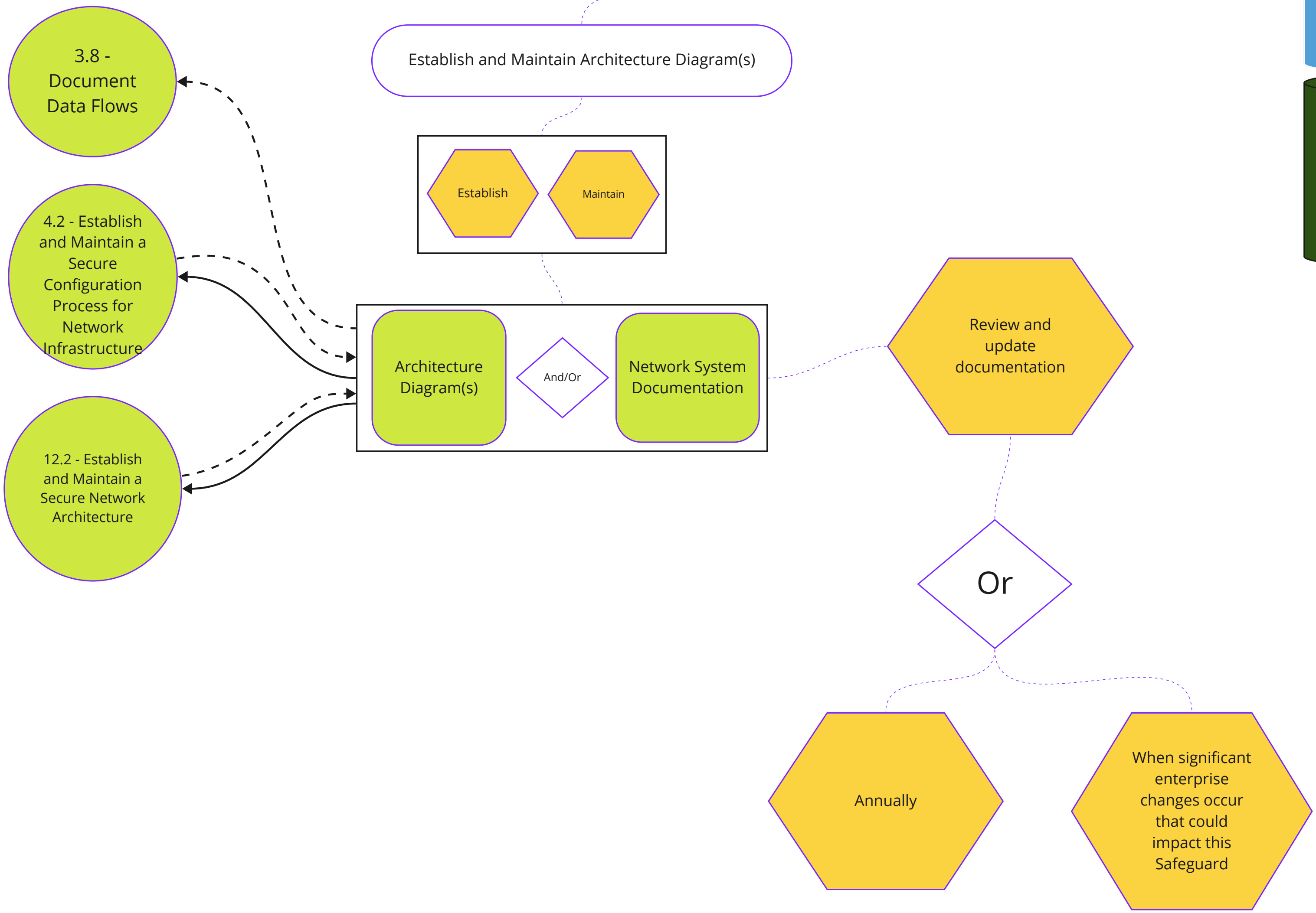
Identify

Network

Secure Network Management and Design Policy/Process

Network Architecture Diagramming Tool

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.



Establish and Maintain Architecture Diagram(s)
Establish
Maintain
3.8 - Document Data Flows
4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure
12.2 - Establish and Maintain a Secure Network Architecture
Architecture Diagram(s)
And/Or
Network System Documentation
Review and update documentation
Or
Annually
When significant enterprise changes occur that could impact this Safeguard

Group Validated

12.5

IG2

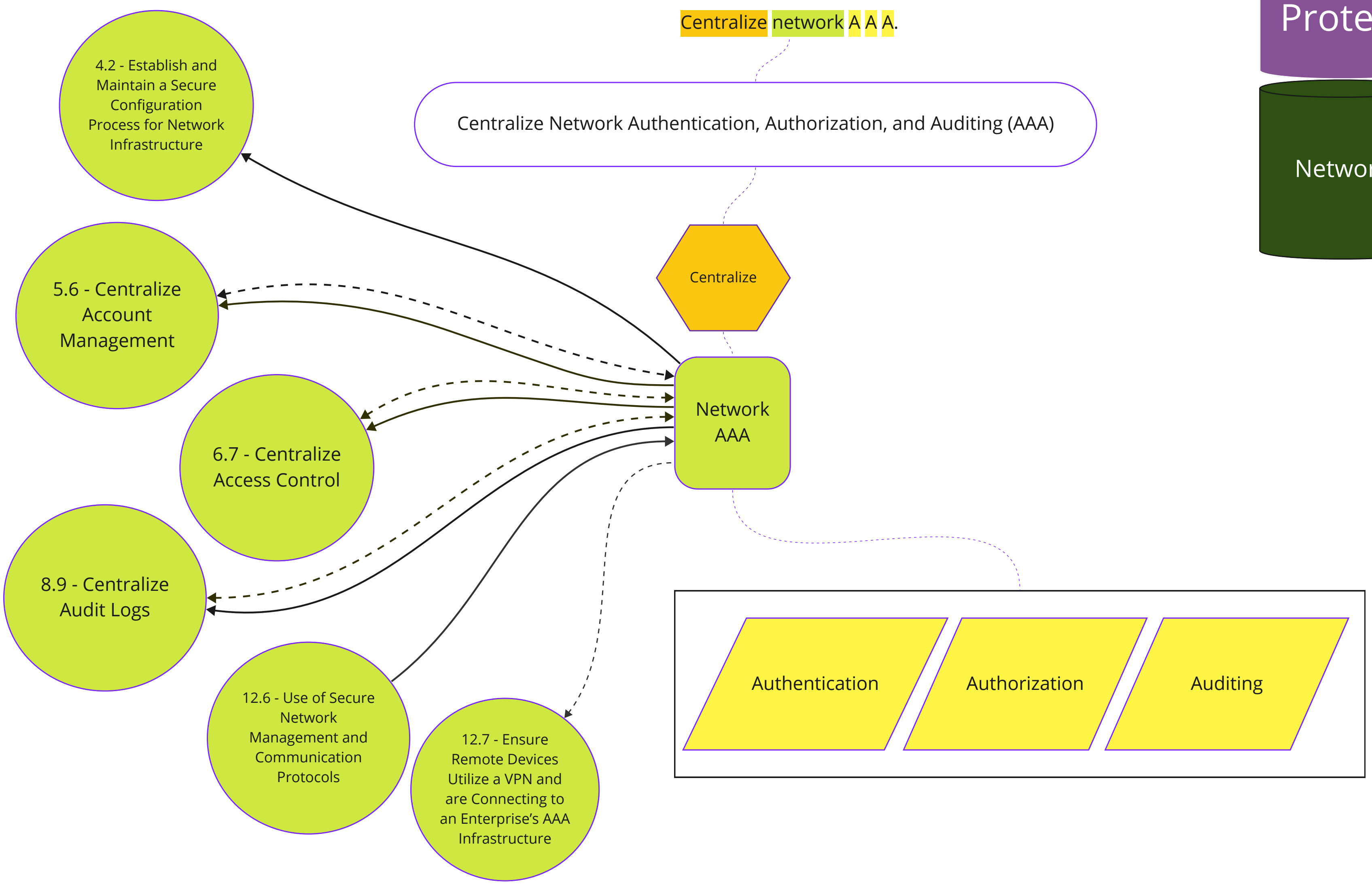
Protect

Network

Account and Access Control Management

Secure Network Management and Design Policy/Process

Identity and Access Management Tool



Centralize network A A A.

Centralize Network Authentication, Authorization, and Auditing (AAA)

Centralize

Network AAA

Authentication

Authorization

Auditing

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

5.6 - Centralize Account Management

6.7 - Centralize Access Control

8.9 - Centralize Audit Logs

12.6 - Use of Secure Network Management and Communication Protocols

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

Group Validated

12.6

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

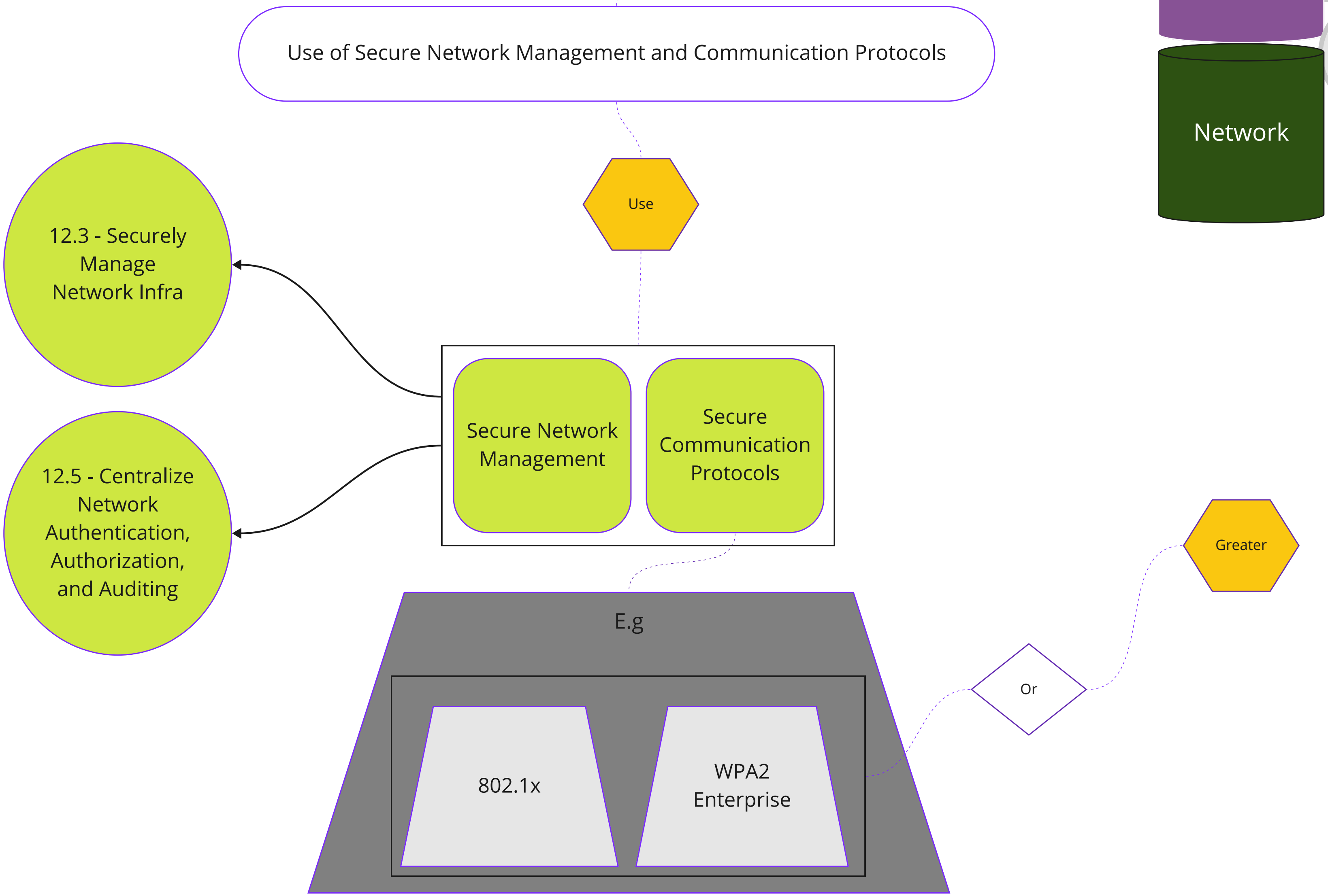
IG2

Network Security

Protect

Secure Network Management and Design Policy/Process

Network



Use of Secure Network Management and Communication Protocols

Use

12.3 - Securely Manage Network Infra

12.5 - Centralize Network Authentication, Authorization, and Auditing

Secure Network Management

Secure Communication Protocols

E.g

802.1x

WPA2 Enterprise

Or

Greater

Group Validated

12.7

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

IG2

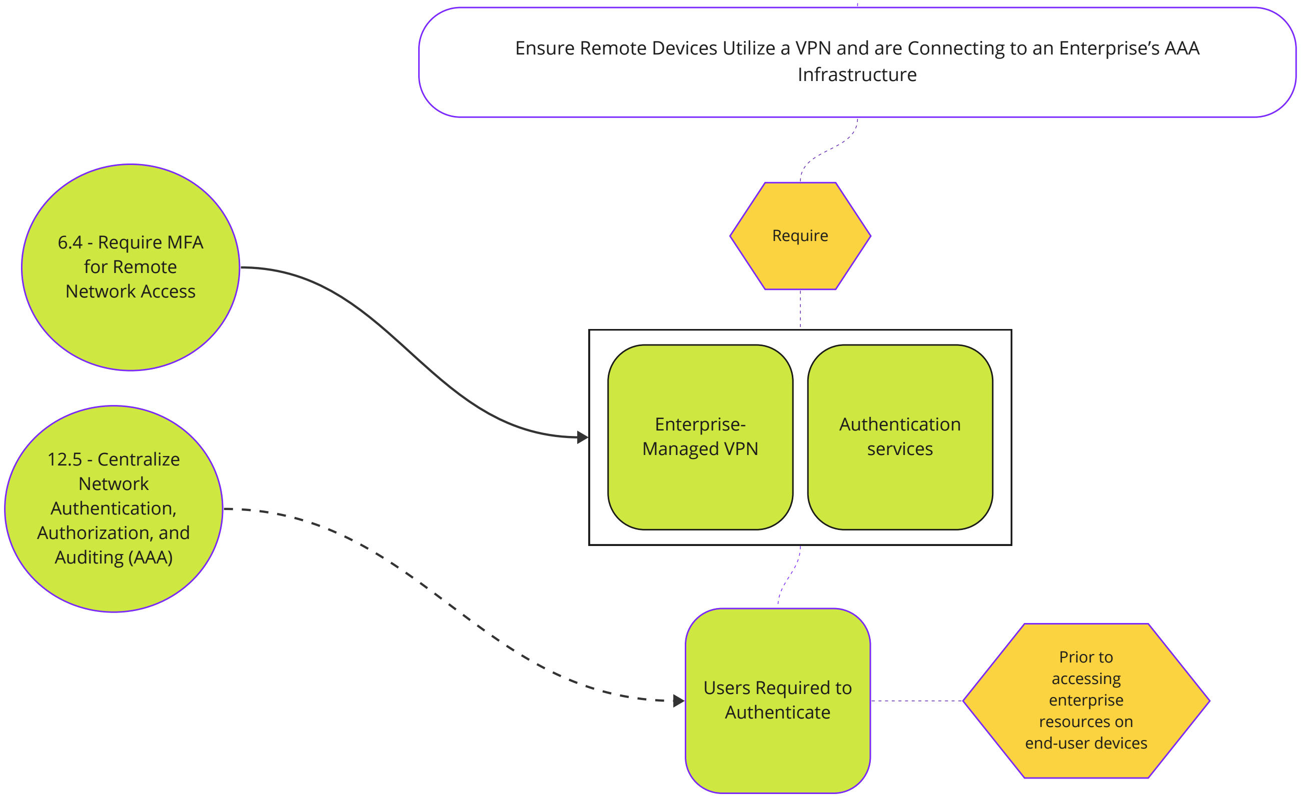
Network Security

Protect

Secure Network Management and Design Policy/Process

Devices

VPN / Encryption Tool



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

Require

6.4 - Require MFA for Remote Network Access

Enterprise-Managed VPN

Authentication services

12.5 - Centralize Network Authentication, Authorization, and Auditing (AAA)

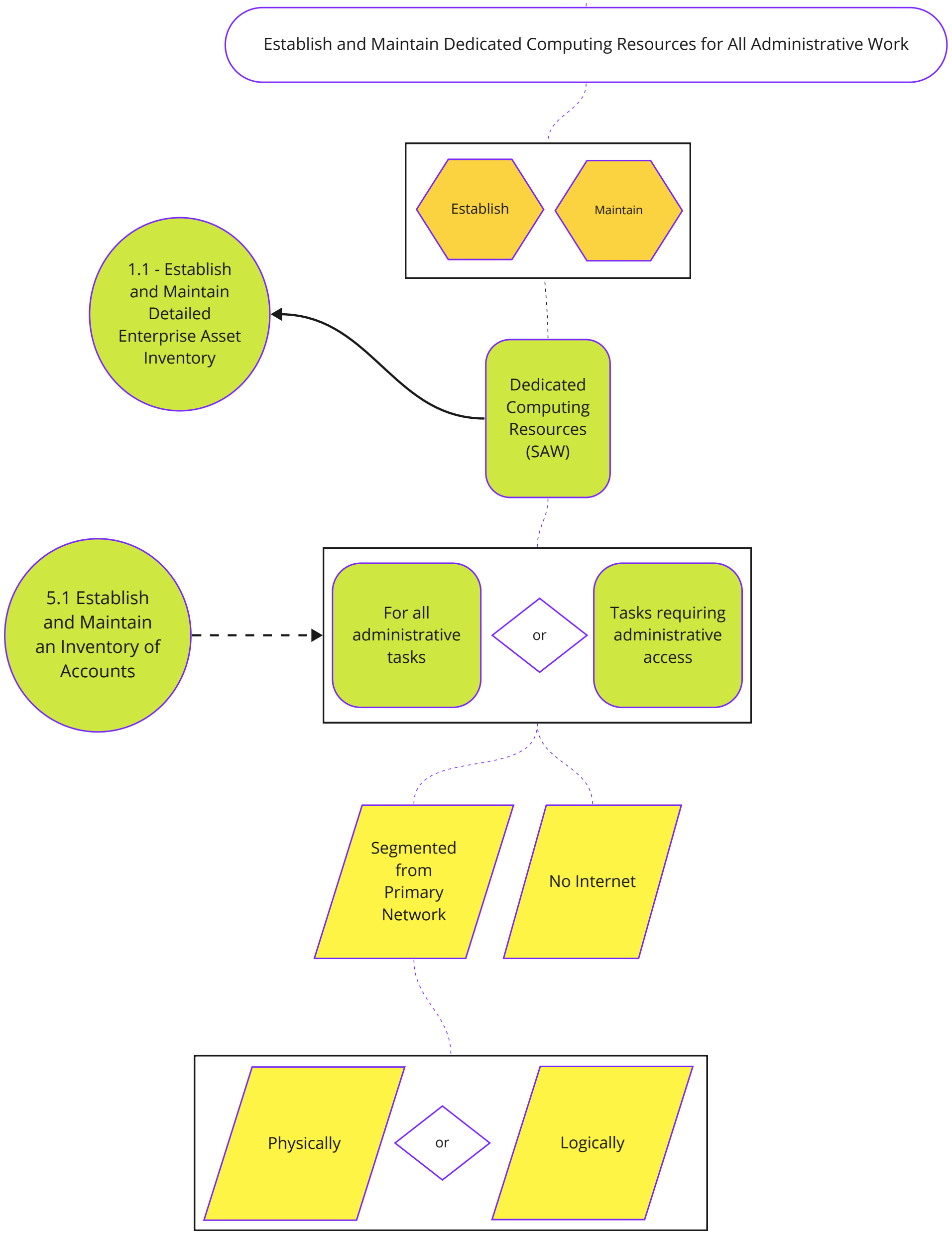
Users Required to Authenticate

Prior to accessing enterprise resources on end-user devices

Group Validated

12.8

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.



Establish and Maintain Dedicated Computing Resources for All Administrative Work

Establish

Maintain

Dedicated Computing Resources (SAW)

1.1 - Establish and Maintain Detailed Enterprise Asset Inventory

5.1 Establish and Maintain an Inventory of Accounts

For all administrative tasks

or

Tasks requiring administrative access

Segmented from Primary Network

No Internet

Physically

or

Logically

Process Oriented Safeguard

IG3

Network Security

Protect

Secure Network Management and Design Policy/Process

Devices

CONTROL 13

Network Monitoring and Defense

Safeguards Total 11 — IG1 0/11 — IG2 6/11 — IG3 11/11

Overview

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.

Group Validated

13.1

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.

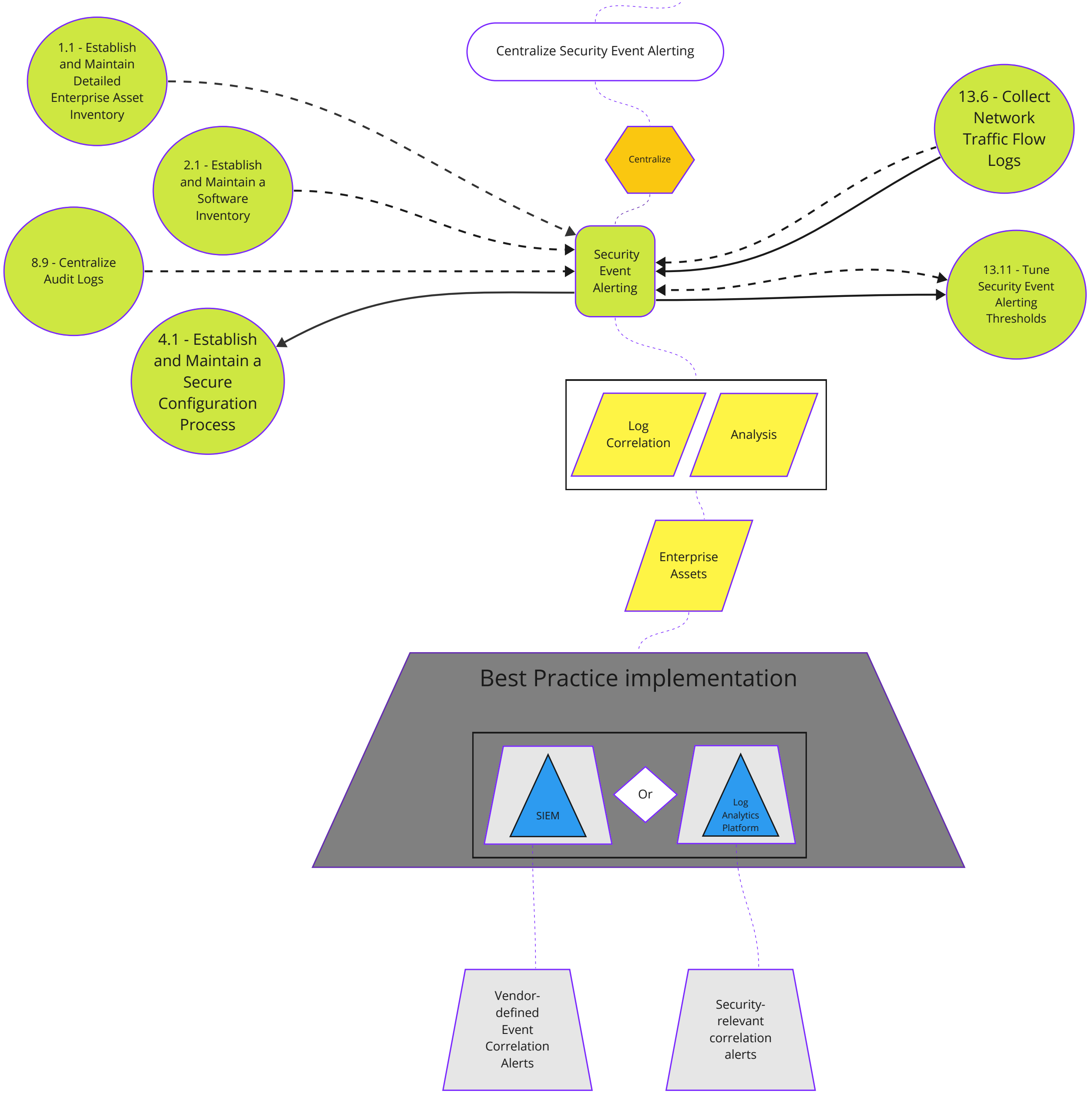
IG2

Malware Defense

Detect

Network

Security Alert Correlation Tool


Centralize Security Event Alerting
Centralize
1.1 - Establish and Maintain Detailed Enterprise Asset Inventory
2.1 - Establish and Maintain a Software Inventory
8.9 - Centralize Audit Logs
4.1 - Establish and Maintain a Secure Configuration Process
Security Event Alerting
13.6 - Collect Network Traffic Flow Logs
13.11 - Tune Security Event Alerting Thresholds
Log Correlation
Analysis
Enterprise Assets
Best Practice implementation
SIEM
Or
Log Analytics Platform
Vendor-defined Event Correlation Alerts
Security-relevant correlation alerts

Group Validated

13.2

IG2

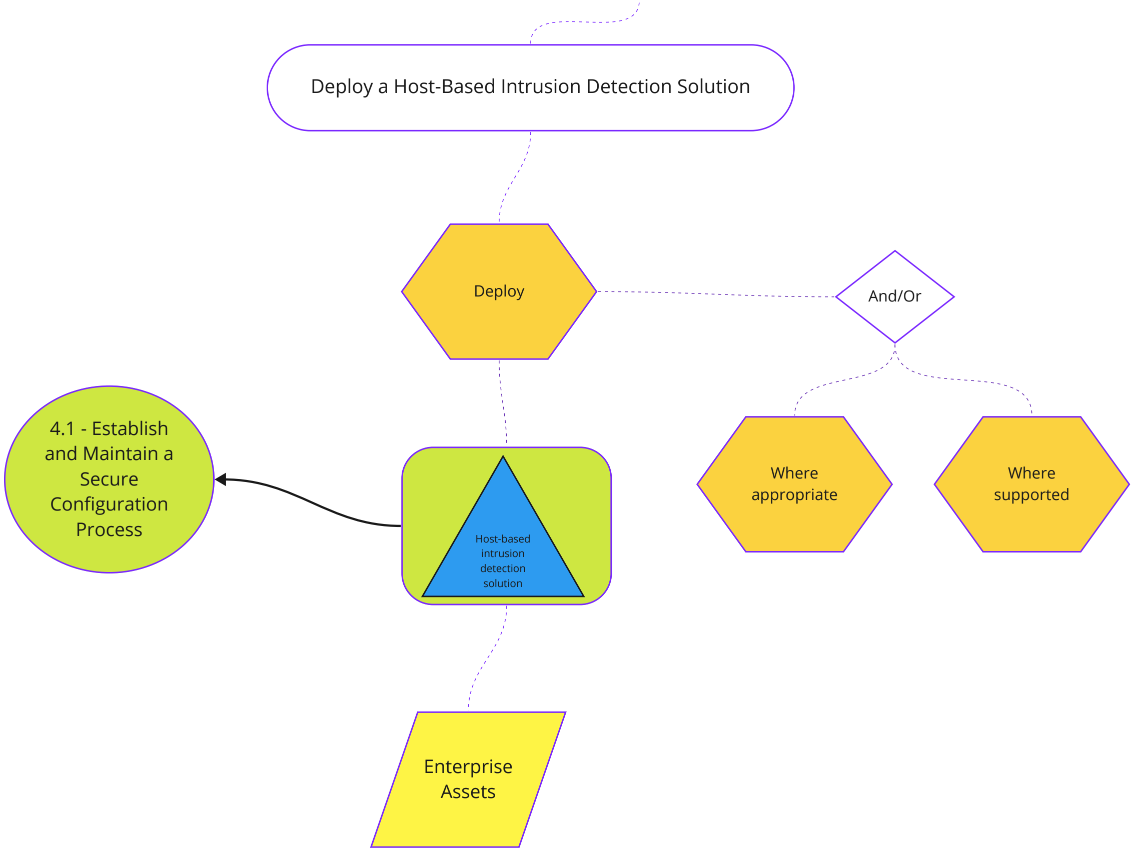
Malware Defense

Detect

Anti-Malware Software

Devices

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



Deploy a Host-Based Intrusion Detection Solution

Deploy

And/Or

Where appropriate

Where supported

4.1 - Establish and Maintain a Secure Configuration Process

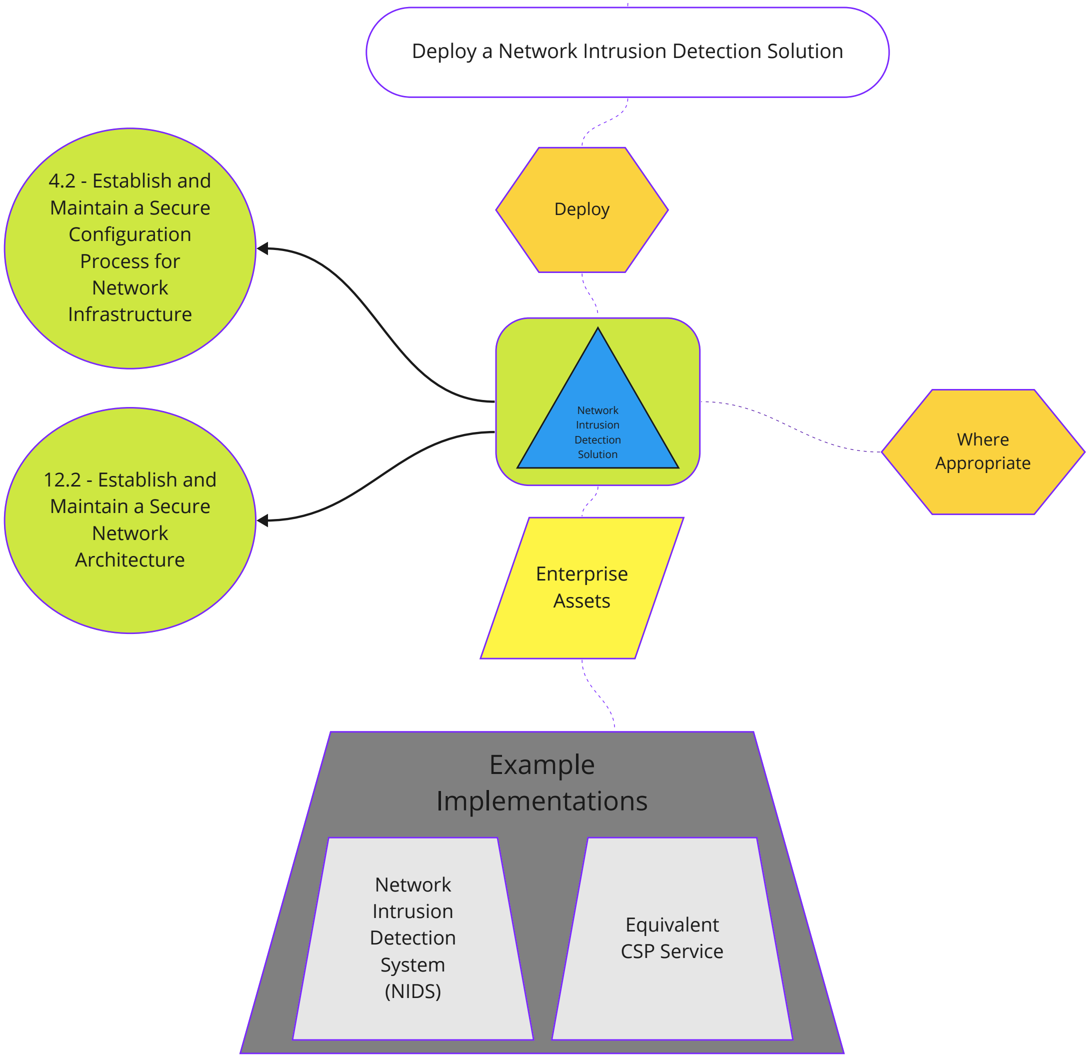
Host-based intrusion detection solution

Enterprise Assets

Group Validated

13.3

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



Deploy a Network Intrusion Detection Solution

Deploy

Network Intrusion Detection Solution

Where Appropriate

Enterprise Assets

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

12.2 - Establish and Maintain a Secure Network Architecture

Example Implementations

Network Intrusion Detection System (NIDS)

Equivalent CSP Service

IG2

Network Defense

Detect

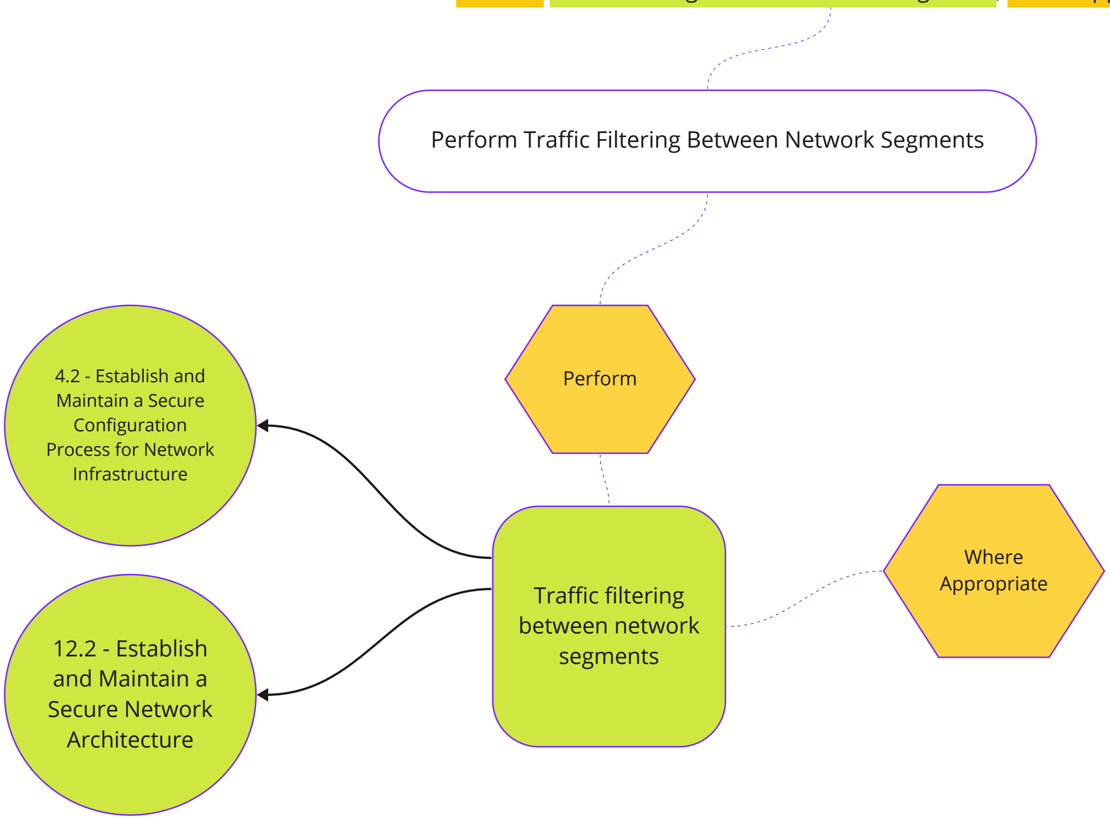
Network

Intrusion Detection System

Group Validated

13.4

Perform traffic filtering between network segments, where appropriate



Perform Traffic Filtering Between Network Segments

Perform

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

Traffic filtering between network segments

Where Appropriate

12.2 - Establish and Maintain a Secure Network Architecture

IG2

Secure Configurations

Protect

Firewall

Network

Group Validated

13.5

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

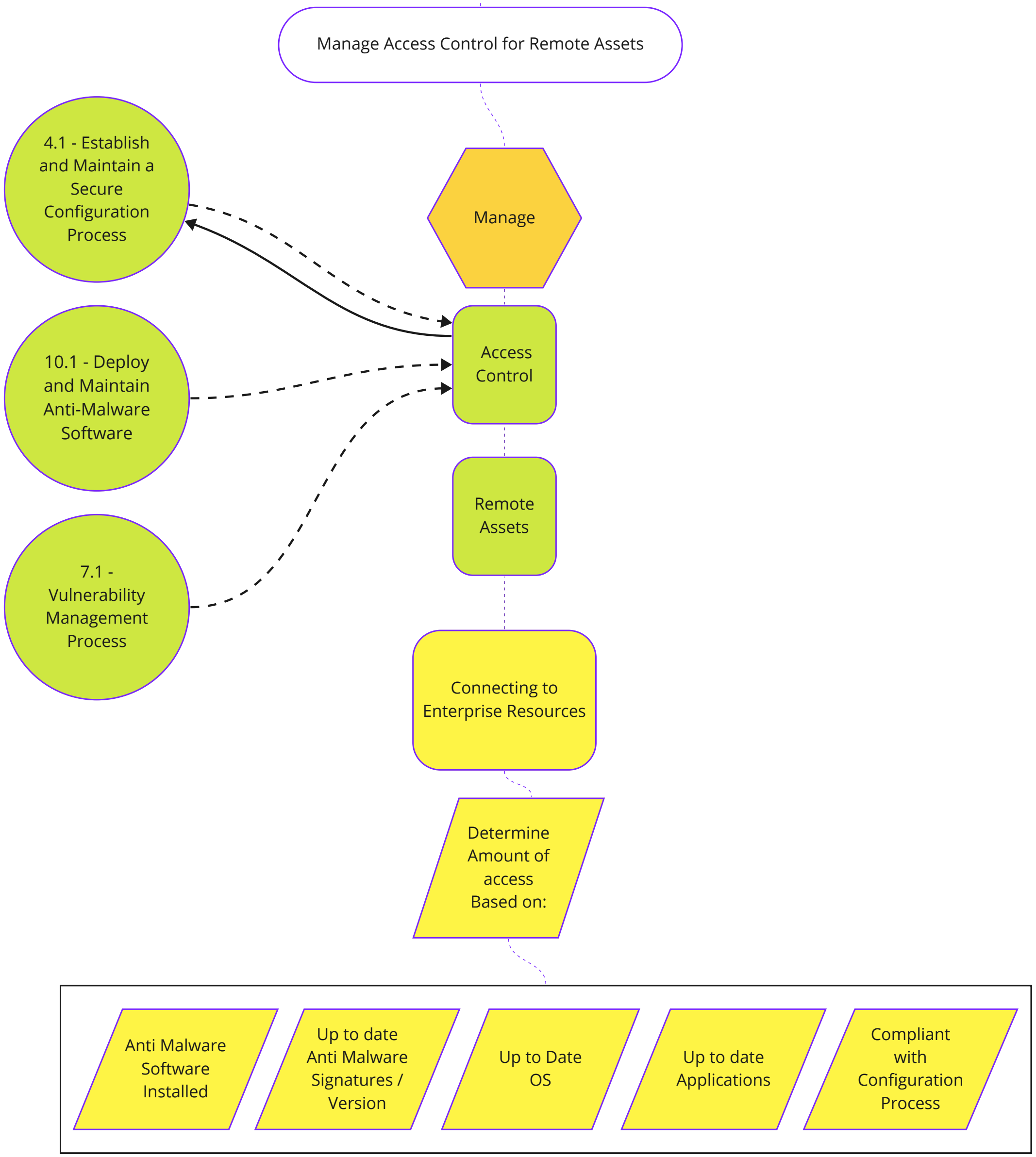
IG2

Network Defense

Protect

Device Posture Tool

Devices



Manage Access Control for Remote Assets

Manage

Access Control

Remote Assets

Connecting to Enterprise Resources

Determine Amount of access Based on:

4.1 - Establish and Maintain a Secure Configuration Process

10.1 - Deploy and Maintain Anti-Malware Software

7.1 - Vulnerability Management Process

Anti Malware Software Installed

Up to date Anti Malware Signatures / Version

Up to Date OS

Up to date Applications

Compliant with Configuration Process

Group Validated

13.6

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

IG2

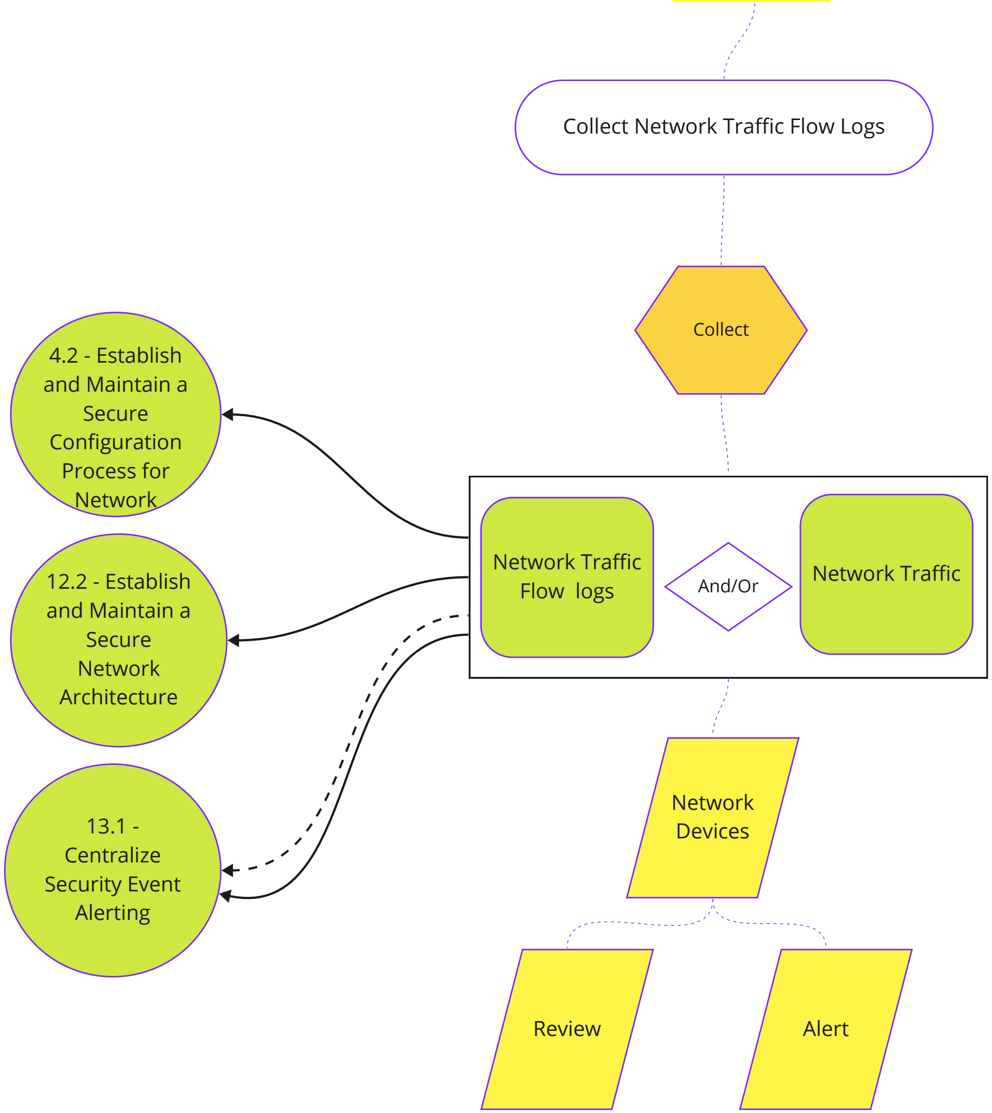
Detect

Network

Network Defense

Network Flow Collection Tool

Security Alert Correlation Tool


Collect Network Traffic Flow Logs
Collect
4.2 - Establish and Maintain a Secure Configuration Process for Network
12.2 - Establish and Maintain a Secure Network Architecture
13.1 - Centralize Security Event Alerting
Network Traffic Flow logs
And/Or
Network Traffic
Network Devices
Review
Alert

Group Validated

13.7

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.

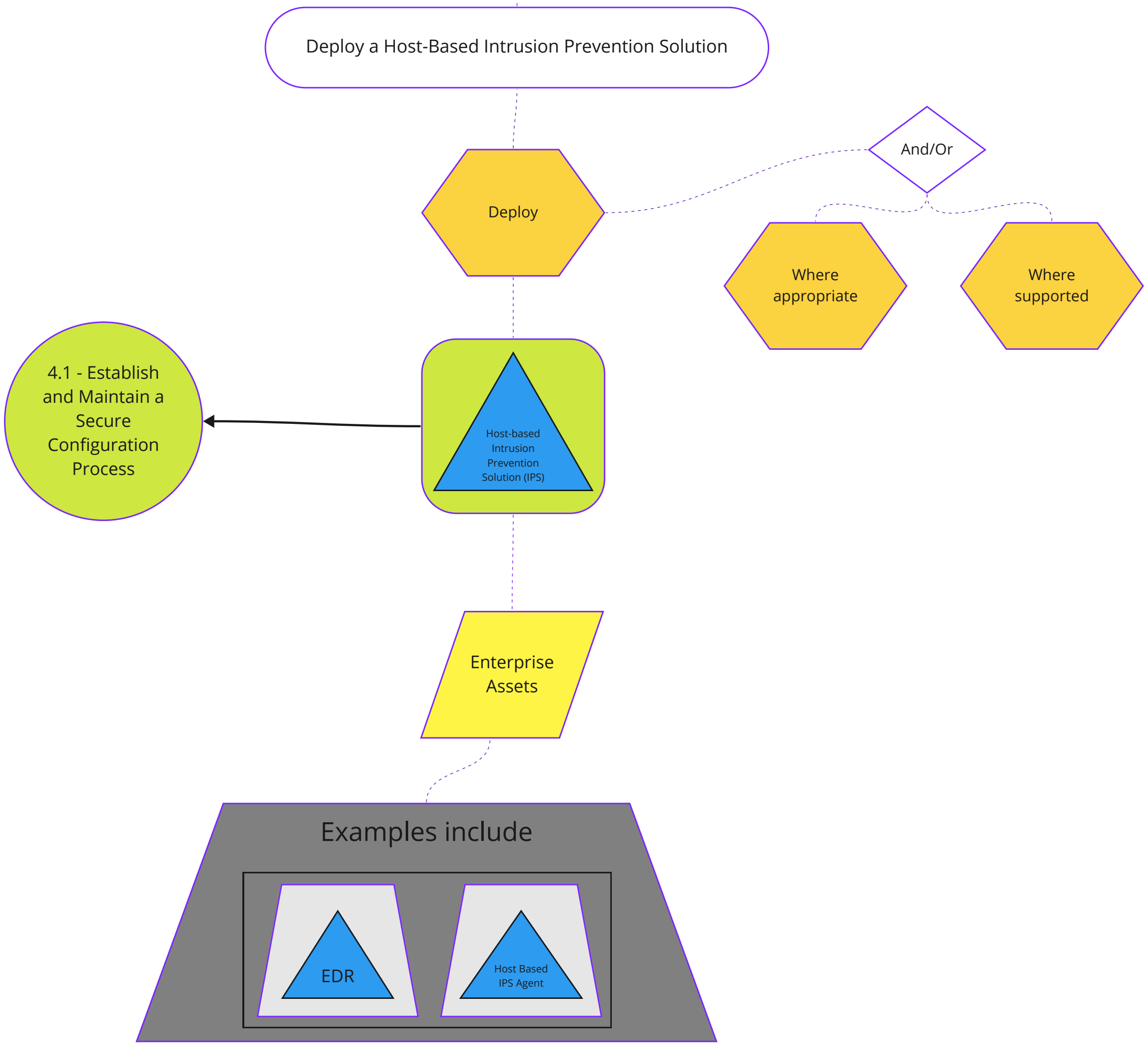
IG3

Network Defense

Protect

Devices

Intrusion Prevention Solution



Deploy a Host-Based Intrusion Prevention Solution

Deploy

And/Or

Where appropriate

Where supported

4.1 - Establish and Maintain a Secure Configuration Process

Host-based Intrusion Prevention Solution (IPS)

Enterprise Assets

Examples include

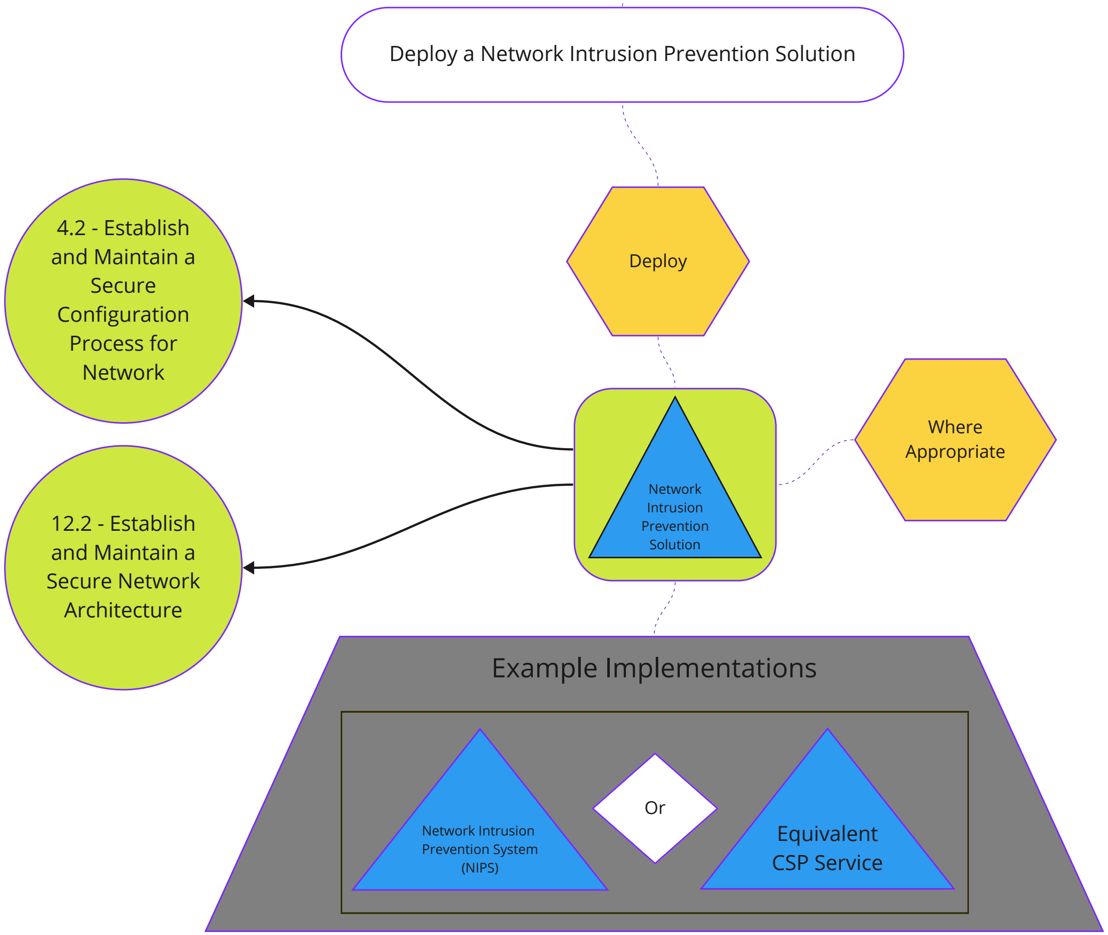
EDR

Host Based IPS Agent

Group Validated

13.8

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



Deploy a Network Intrusion Prevention Solution

Deploy

Network Intrusion Prevention Solution

Where Appropriate

4.2 - Establish and Maintain a Secure Configuration Process for Network

12.2 - Establish and Maintain a Secure Network Architecture

Example Implementations

Network Intrusion Prevention System (NIPS)

Or

Equivalent CSP Service

IG3

Network Defense

Protect

Intrusion Prevention System

Network

Firewall

Group Validated

13.9

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

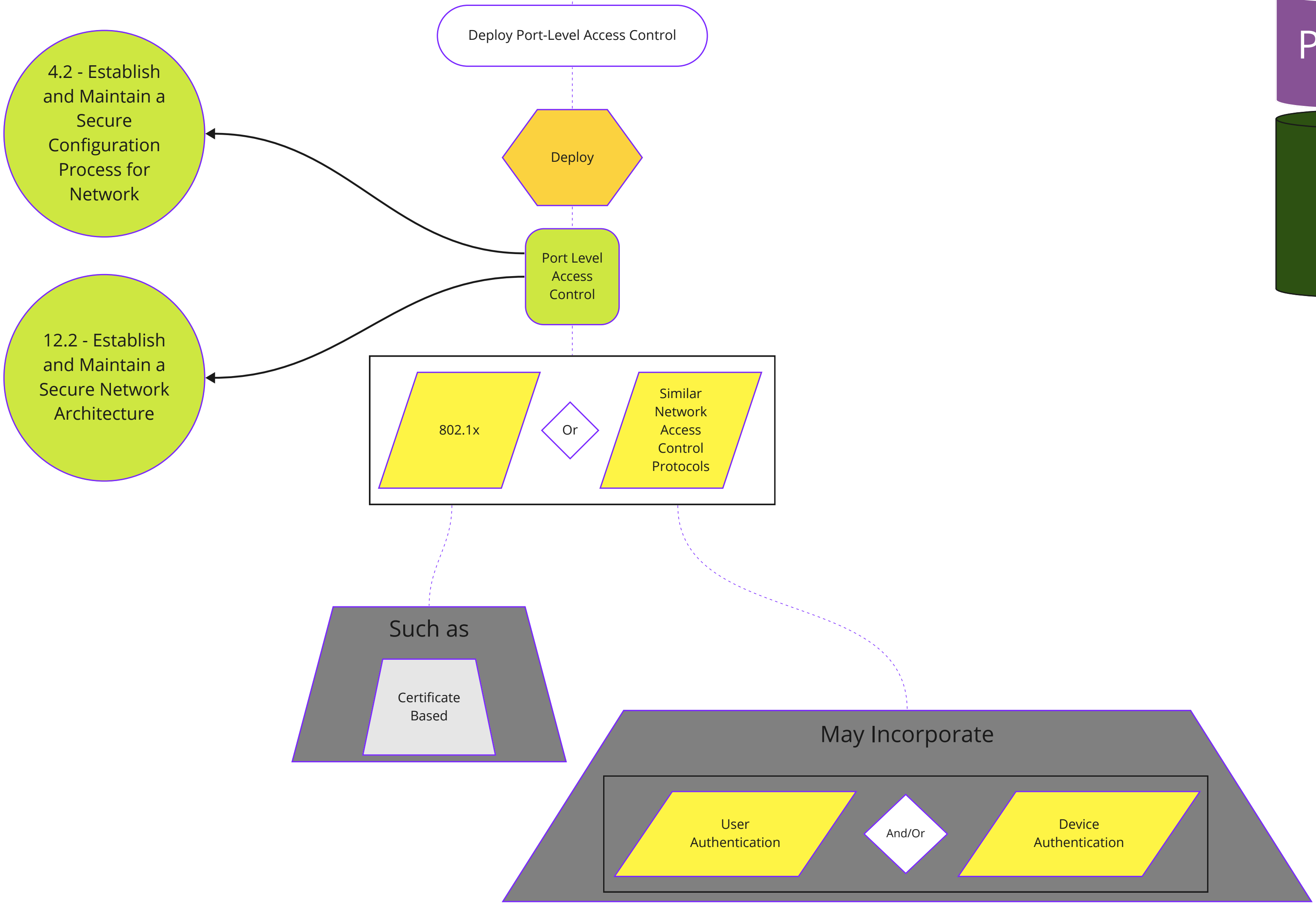
IG3

Network Defense

Protect

Network Access Control Tool

Devices



Deploy Port-Level Access Control

Deploy

Port Level Access Control

4.2 - Establish and Maintain a Secure Configuration Process for Network

12.2 - Establish and Maintain a Secure Network Architecture

802.1x

Or

Similar Network Access Control Protocols

Such as

Certificate Based

May Incorporate

User Authentication

And/Or

Device Authentication

Group Validated

13.10

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

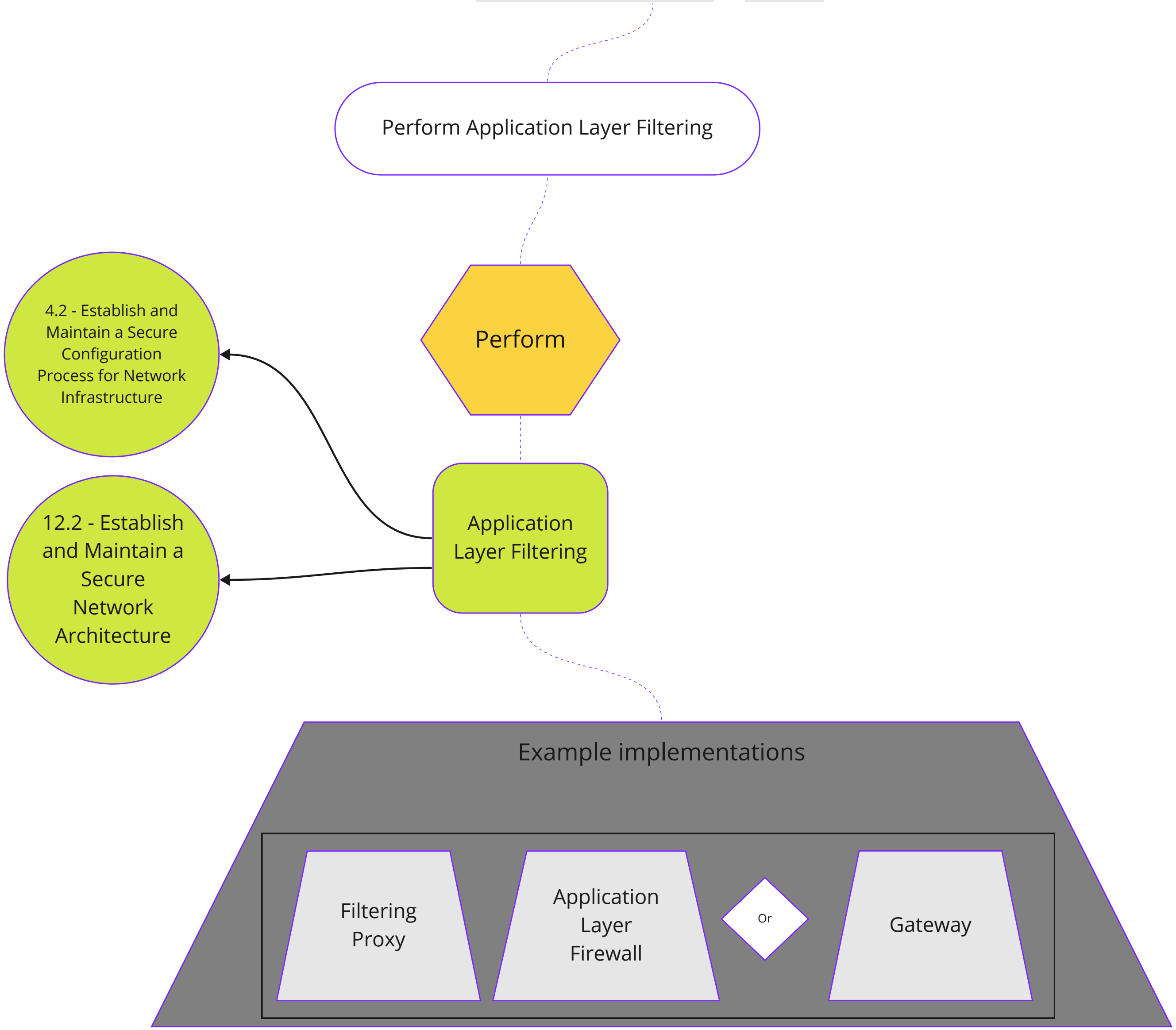
IG3

Network Defense

Protect

Firewall

Network



Perform Application Layer Filtering

Perform

Application Layer Filtering

4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure

12.2 - Establish and Maintain a Secure Network Architecture

Example implementations

Filtering Proxy

Application Layer Firewall

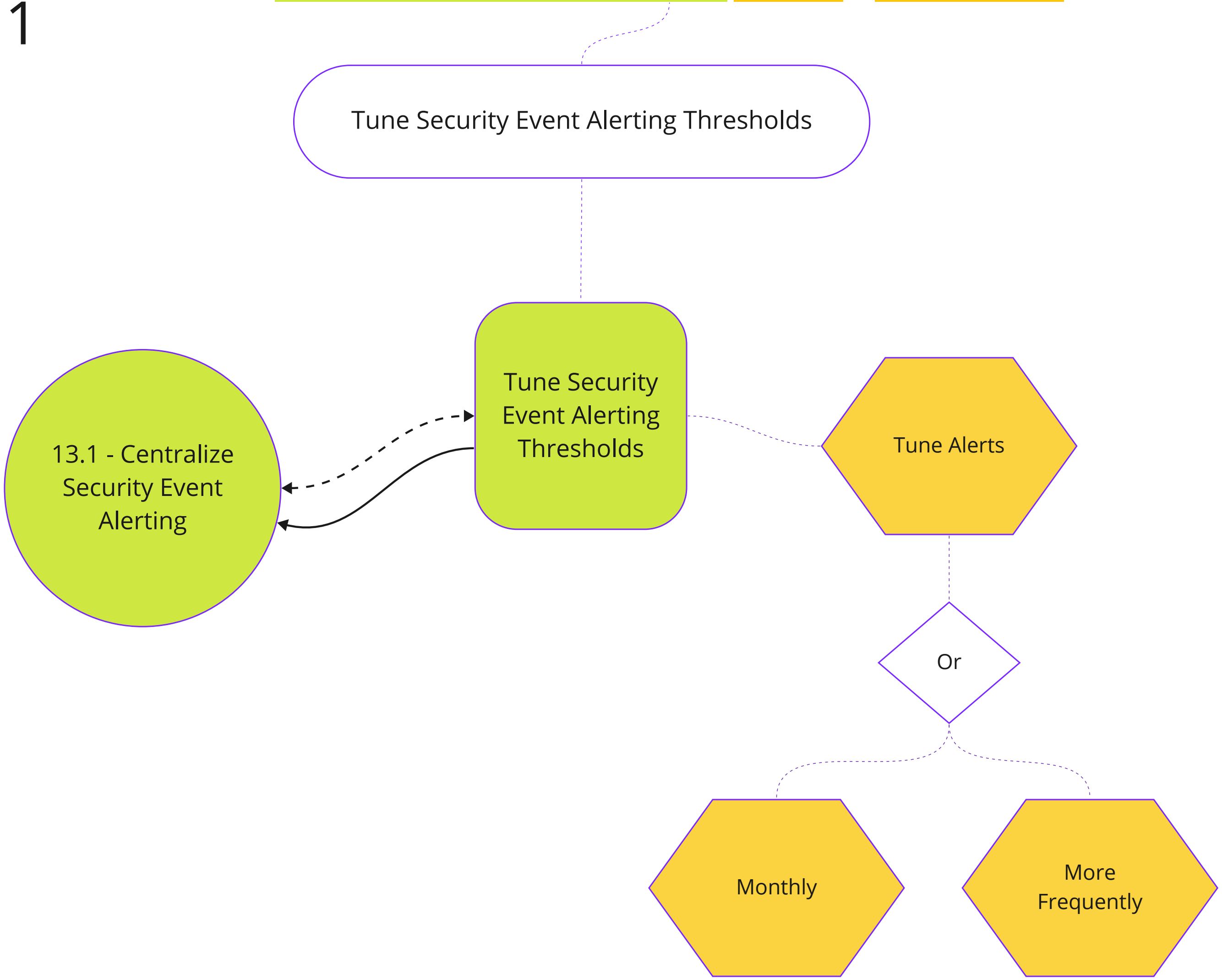
Or

Gateway

Group Validated

13.11

Tune security event alerting thresholds monthly, or more frequently



Tune Security Event Alerting Thresholds

13.1 - Centralize Security Event Alerting

Tune Security Event Alerting Thresholds

Tune Alerts

Or

Monthly

More Frequently

IG3

Network Defense

Detect

SOC Operations

Network

CONTROL 14

Security Awareness and Skills Training

Safeguards Total	IG1	IG2	IG3
9	8/9	9/9	8/8

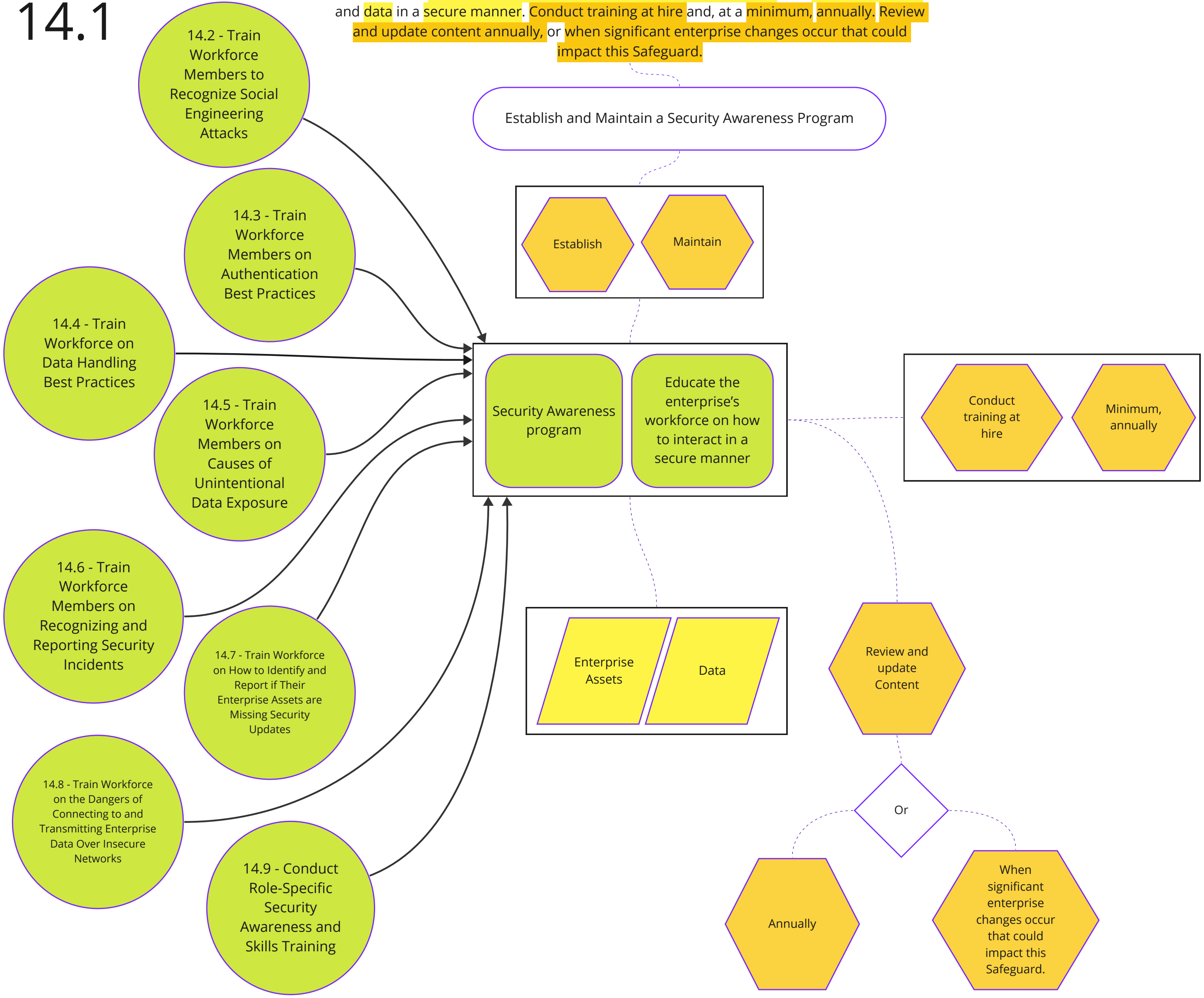
Overview

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.

Group Validated

14.1

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.



Establish and Maintain a Security Awareness Program

Establish

Maintain

Security Awareness program

Educate the enterprise's workforce on how to interact in a secure manner

Conduct training at hire

Minimum, annually

Enterprise Assets

Data

Review and update Content

Or

Annually

When significant enterprise changes occur that could impact this Safeguard.

14.2 - Train Workforce Members to Recognize Social Engineering Attacks

14.3 - Train Workforce Members on Authentication Best Practices

14.4 - Train Workforce on Data Handling Best Practices

14.5 - Train Workforce Members on Causes of Unintentional Data Exposure

14.6 - Train Workforce Members on Recognizing and Reporting Security Incidents

14.7 - Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

14.8 - Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

14.9 - Conduct Role-Specific Security Awareness and Skills Training

Process Oriented Safeguard

IG1

Security Training

Protect

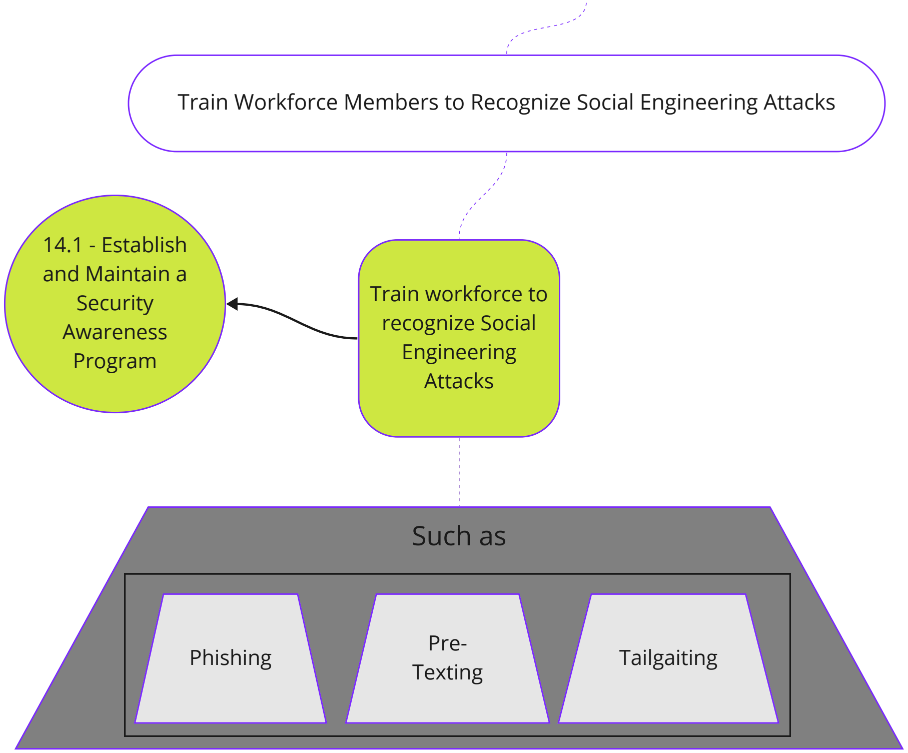
Security Training and Awareness Policy/Process

N/A

Group Validated

14.2

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



Train Workforce Members to Recognize Social Engineering Attacks

Train workforce to recognize Social Engineering Attacks

14.1 - Establish and Maintain a Security Awareness Program

Such as

- Phishing
- Pre-Texting
- Tailgating

IG1

Security Training

Protect

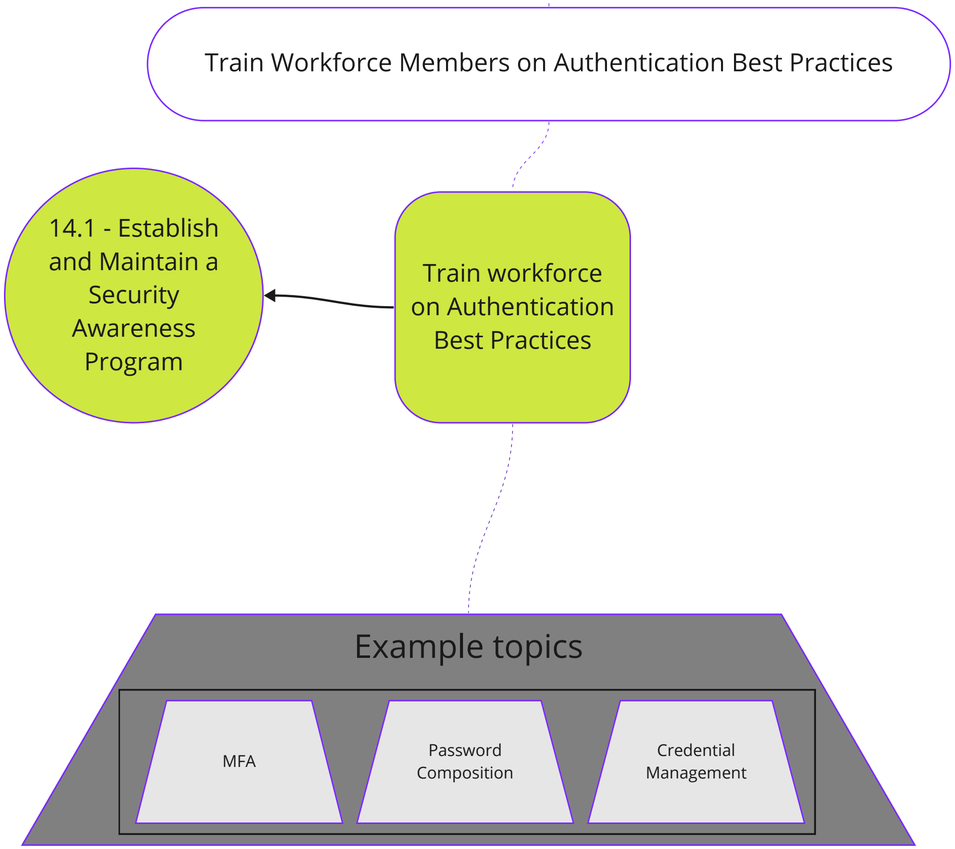
Security Training and Awareness Tool(s)

N/A

Group Validated

14.3

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



Train Workforce Members on Authentication Best Practices

Train workforce on Authentication Best Practices

14.1 - Establish and Maintain a Security Awareness Program

Example topics

MFA

Password Composition

Credential Management

IG1

Security Training

Protect

Security Training and Awareness Tool(s)

N/A

Group Validated

14.4

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.

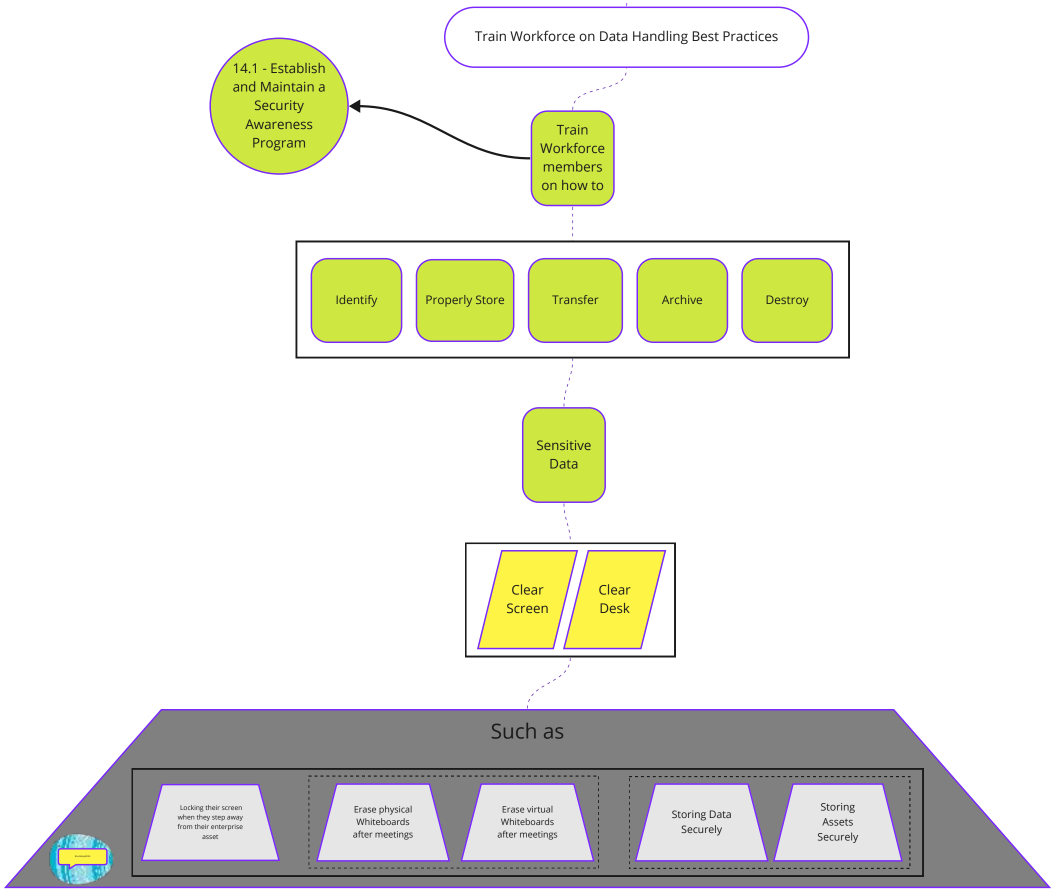
IG1

Security Training

Protect

Security Training and Awareness Tool(s)

N/A



Train Workforce on Data Handling Best Practices

Train Workforce members on how to

14.1 - Establish and Maintain a Security Awareness Program

Identify

Properly Store

Transfer

Archive

Destroy

Sensitive Data

Clear Screen

Clear Desk

Such as

Locking their screen when they step away from their enterprise asset

Erase physical Whiteboards after meetings

Erase virtual Whiteboards after meetings

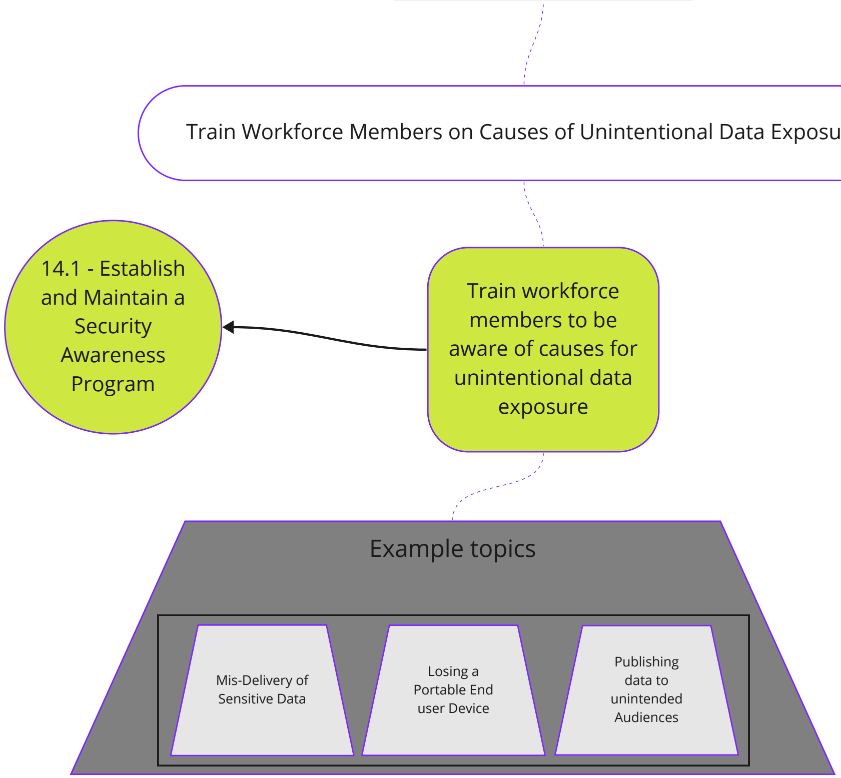
Storing Data Securely

Storing Assets Securely

Group Validated

14.5

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.



Train Workforce Members on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposure

14.1 - Establish and Maintain a Security Awareness Program

Example topics

Mis-Delivery of Sensitive Data

Losing a Portable End user Device

Publishing data to unintended Audiences

IG1

Security Training

Protect

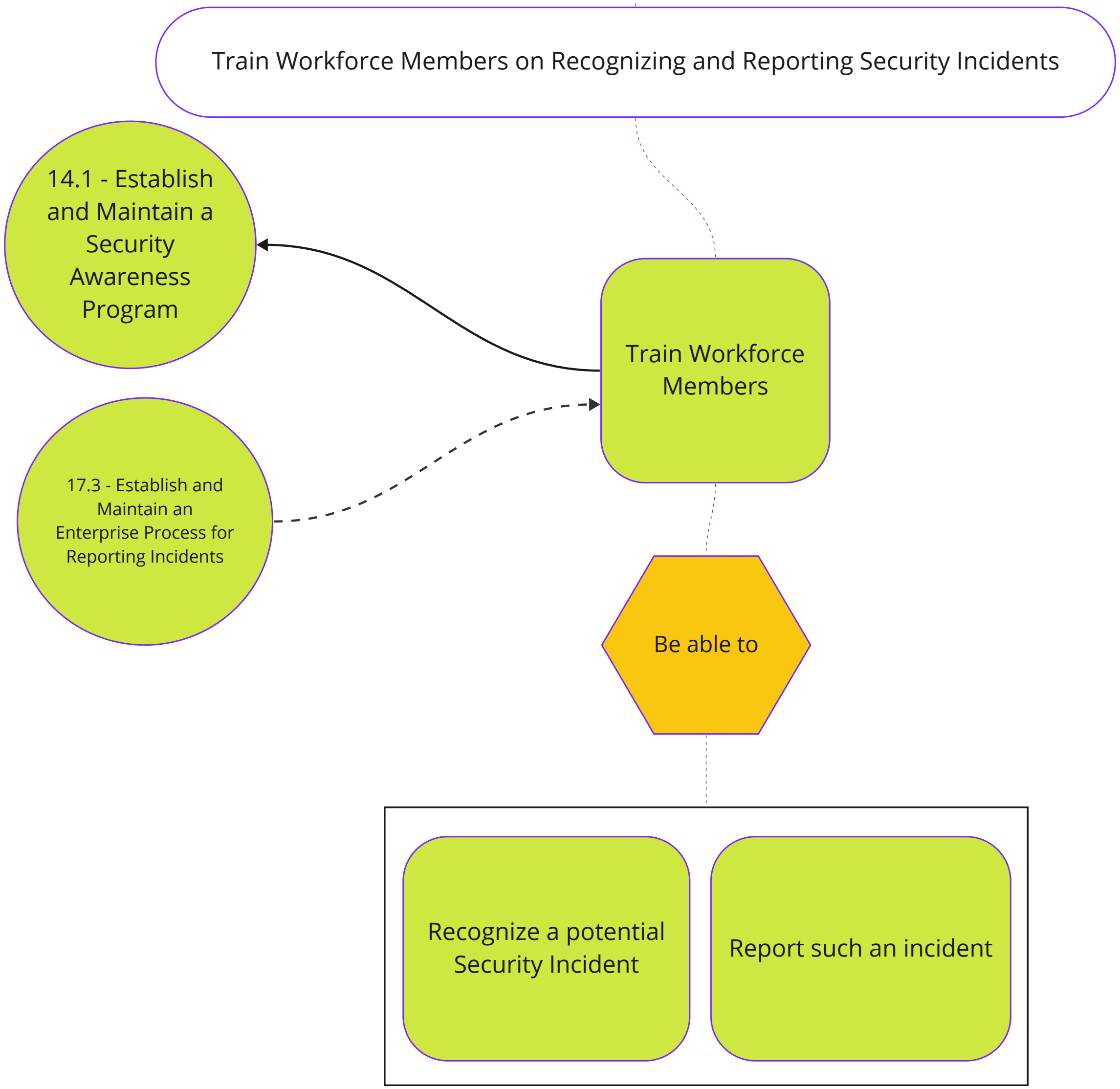
Security Training and Awareness Tool(s)

N/A

Group Validated

14.6

Train workforce members to be able to recognize a potential incident and be able to report such an incident.



Train Workforce Members on Recognizing and Reporting Security Incidents

14.1 - Establish and Maintain a Security Awareness Program

Train Workforce Members

17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents

Be able to

Recognize a potential Security Incident

Report such an incident

IG1

Security Training

Protect

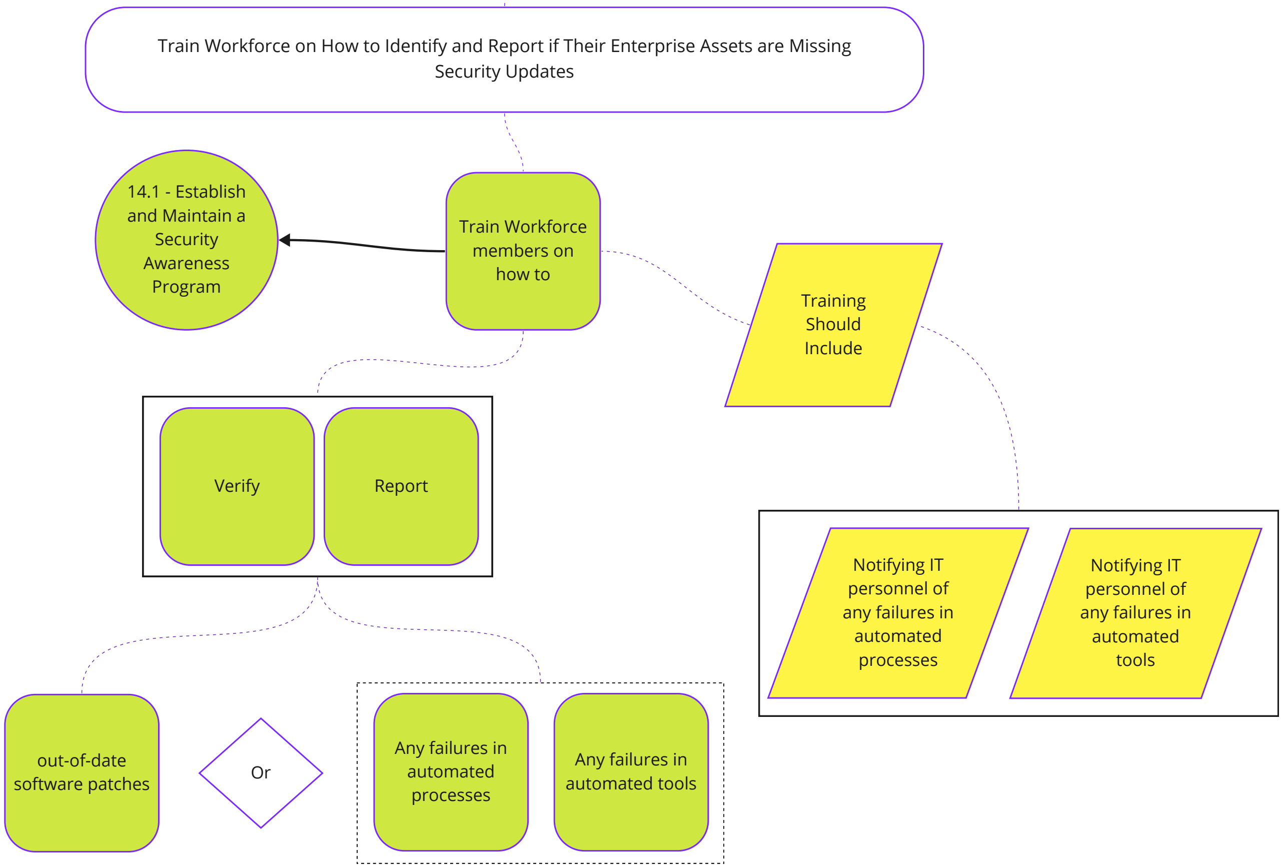
Security Training and Awareness Tool(s)

N/A

Group Validated

14.7

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.



Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

14.1 - Establish and Maintain a Security Awareness Program

Train Workforce members on how to

Training Should Include

Verify

Report

Notifying IT personnel of any failures in automated processes

Notifying IT personnel of any failures in automated tools

out-of-date software patches

Or

Any failures in automated processes

Any failures in automated tools

IG1

Security Training

Protect

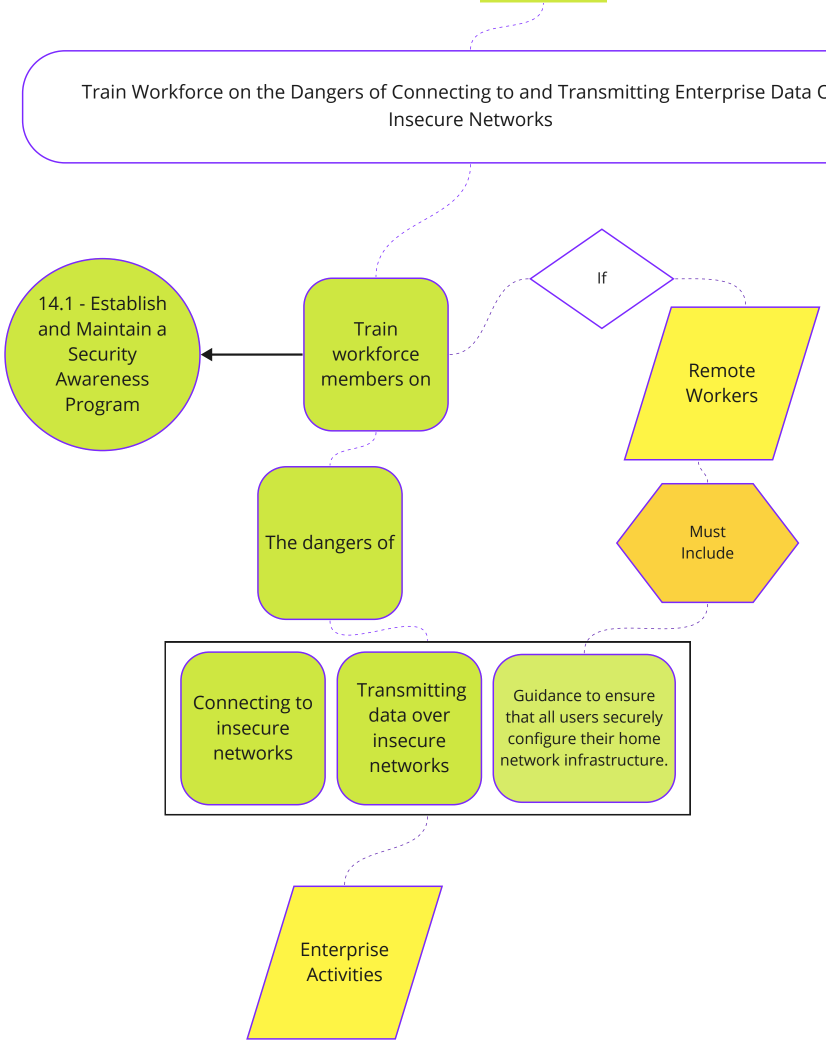
Security Training and Awareness Tool(s)

N/A

Group Validated

14.8

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.



Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

14.1 - Establish and Maintain a Security Awareness Program

Train workforce members on

If

Remote Workers

Must Include

The dangers of

Connecting to insecure networks

Transmitting data over insecure networks

Guidance to ensure that all users securely configure their home network infrastructure.

Enterprise Activities

IG1

Protect

N/A

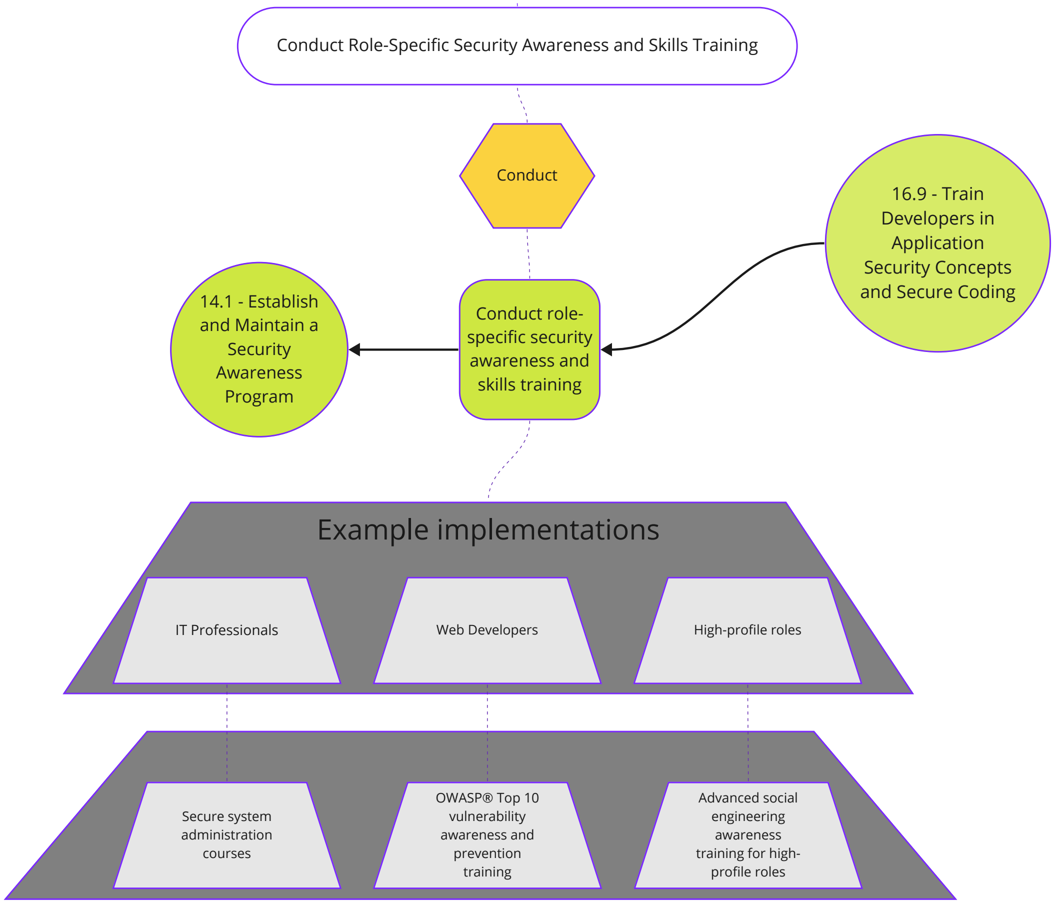
Security Training

Security Training and Awareness Tool(s)

Group Validated

14.9

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.



Conduct Role-Specific Security Awareness and Skills Training

Conduct

Conduct role-specific security awareness and skills training

14.1 - Establish and Maintain a Security Awareness Program

16.9 - Train Developers in Application Security Concepts and Secure Coding

Example implementations

IT Professionals

Web Developers

High-profile roles

Secure system administration courses

OWASP® Top 10 vulnerability awareness and prevention training

Advanced social engineering awareness training for high-profile roles

IG2

Protect

N/A

Security Training

Security Training and Awareness Tool(s)

CONTROL 15

Service Provider Management

Safeguards Total	IG1	IG2	IG3
7	1/7	4/7	7/7

Overview

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.

Group Validated

15.1

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.

Process Oriented Safeguard

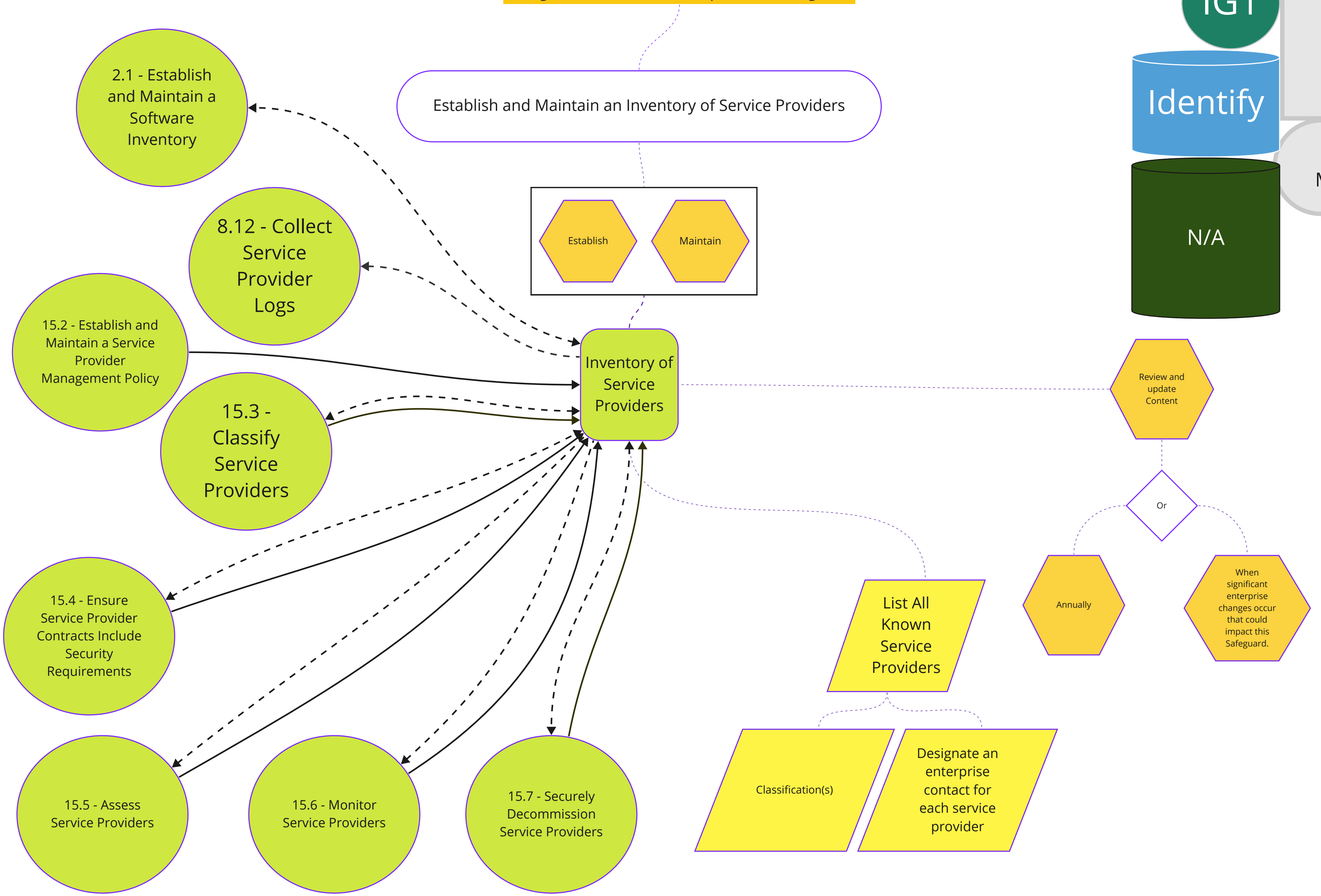
IG1

Service Provider Management

Identify

Third-Party Risk Management Tool

N/A



Establish and Maintain an Inventory of Service Providers

Establish

Maintain

Inventory of Service Providers

2.1 - Establish and Maintain a Software Inventory

8.12 - Collect Service Provider Logs

15.2 - Establish and Maintain a Service Provider Management Policy

15.3 - Classify Service Providers

15.4 - Ensure Service Provider Contracts Include Security Requirements

15.5 - Assess Service Providers

15.6 - Monitor Service Providers

15.7 - Securely Decommission Service Providers

List All Known Service Providers

Classification(s)

Designate an enterprise contact for each service provider

Review and update Content

Or

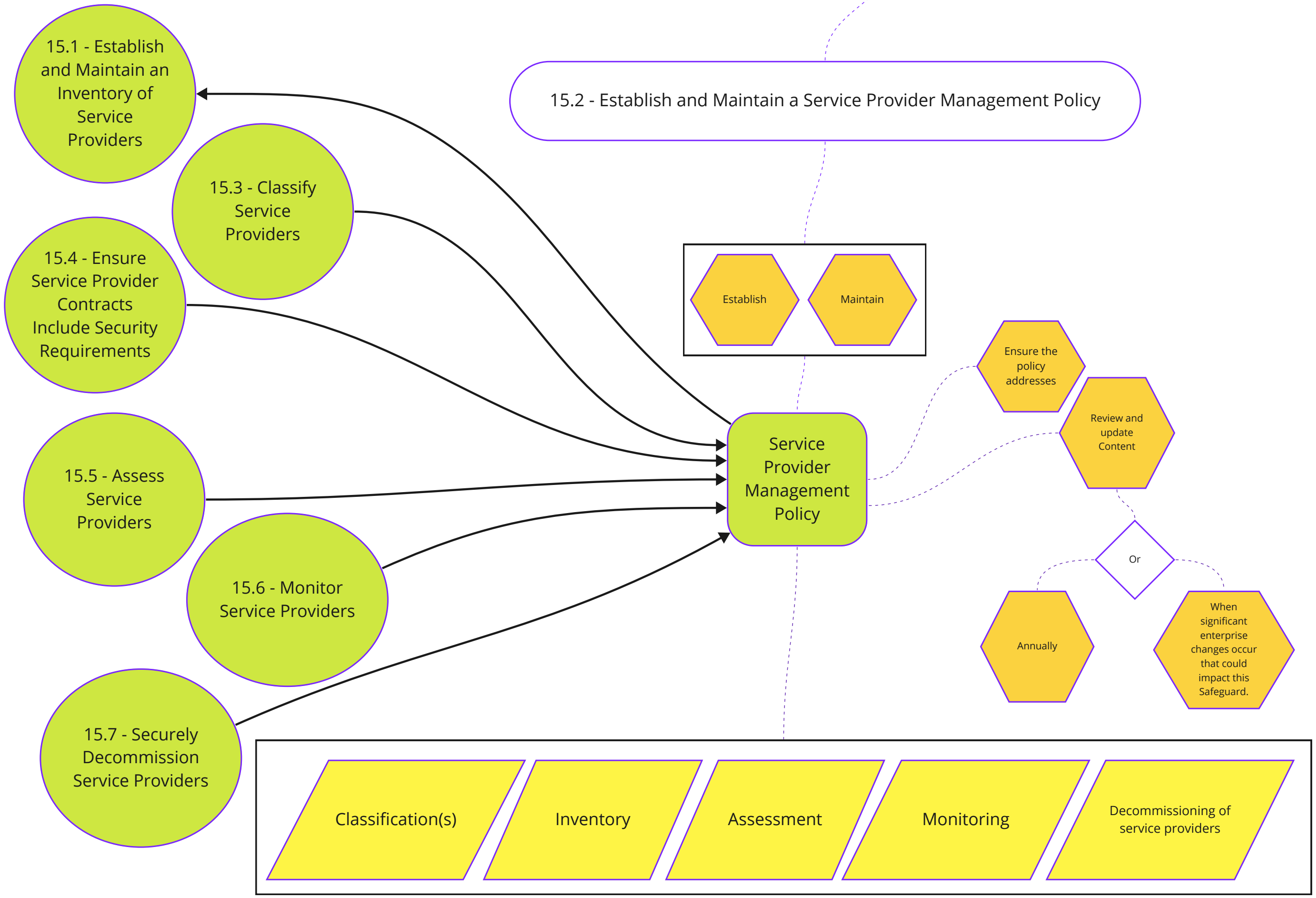
Annually

When significant enterprise changes occur that could impact this Safeguard.

Group Validated

15.2

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.



15.2 - Establish and Maintain a Service Provider Management Policy

Establish

Maintain

Service Provider Management Policy

15.1 - Establish and Maintain an Inventory of Service Providers

15.3 - Classify Service Providers

15.4 - Ensure Service Provider Contracts Include Security Requirements

15.5 - Assess Service Providers

15.6 - Monitor Service Providers

15.7 - Securely Decommission Service Providers

Ensure the policy addresses

Review and update Content

Or

Annually

When significant enterprise changes occur that could impact this Safeguard.

Classification(s)

Inventory

Assessment

Monitoring

Decommissioning of service providers

Process Oriented Safeguard

IG2

Service Provider Management

Identify

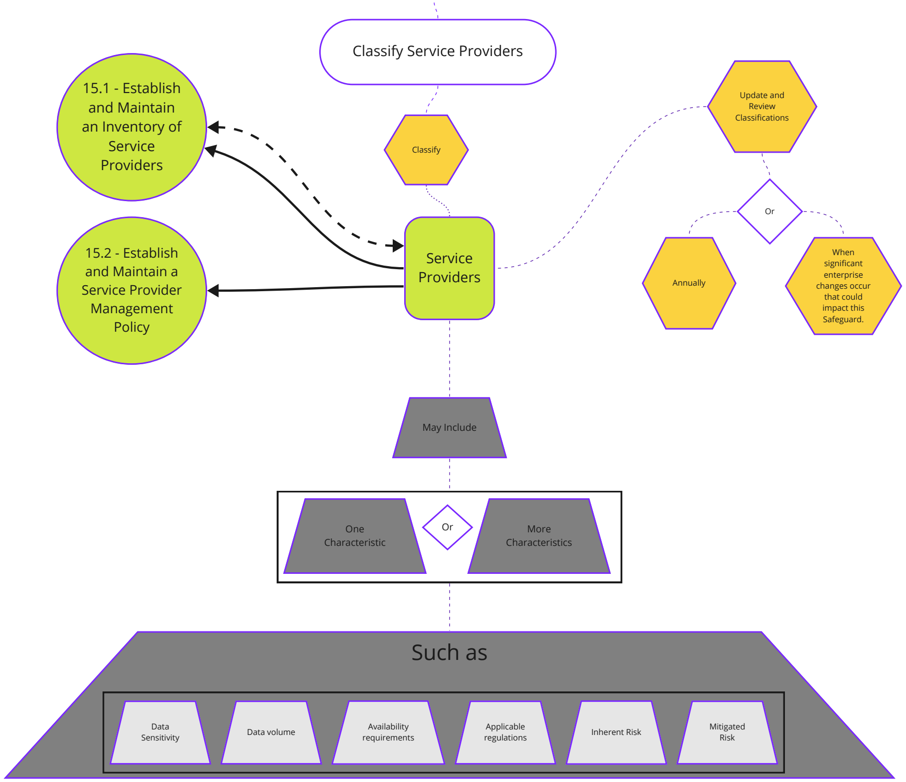
N/A

Service Provider Management Policy

Group Validated

15.3

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.


Classify Service Providers
Classify
15.1 - Establish and Maintain an Inventory of Service Providers
15.2 - Establish and Maintain a Service Provider Management Policy
Service Providers
Update and Review Classifications
Or
Annually
When significant enterprise changes occur that could impact this Safeguard.
May Include
One Characteristic
Or
More Characteristics
Such as
Data Sensitivity
Data volume
Availability requirements
Applicable regulations
Inherent Risk
Mitigated Risk

Process Oriented Safeguard

IG2

Identify

N/A

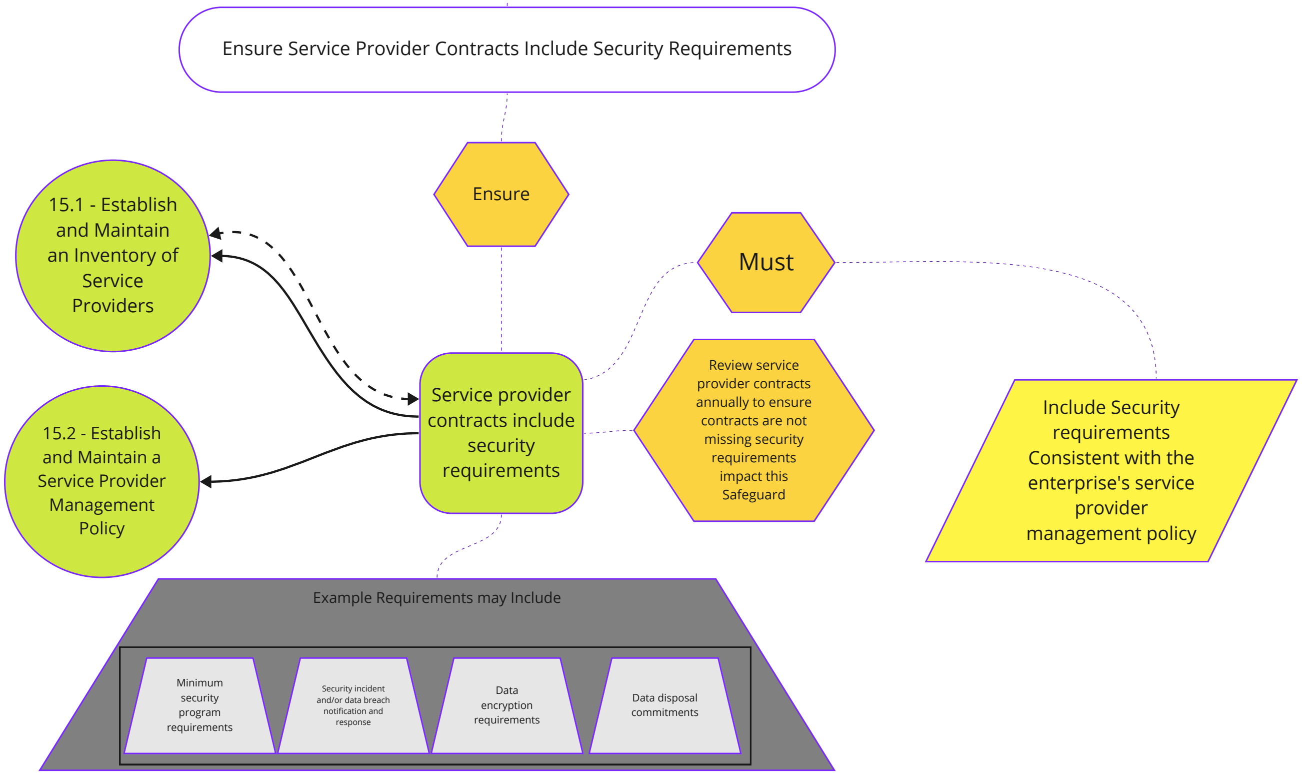
Service Provider Management

Service Provider Management Policy

Group Validated

15.4

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.



Ensure Service Provider Contracts Include Security Requirements

Ensure

Must

15.1 - Establish and Maintain an Inventory of Service Providers

Service provider contracts include security requirements

Review service provider contracts annually to ensure contracts are not missing security requirements impact this Safeguard

Include Security requirements Consistent with the enterprise's service provider management policy

15.2 - Establish and Maintain a Service Provider Management Policy

Example Requirements may Include

Minimum security program requirements

Security incident and/or data breach notification and response

Data encryption requirements

Data disposal commitments

Process Oriented Safeguard

IG2

Service Provider Management

Protect

Service Provider Management Policy

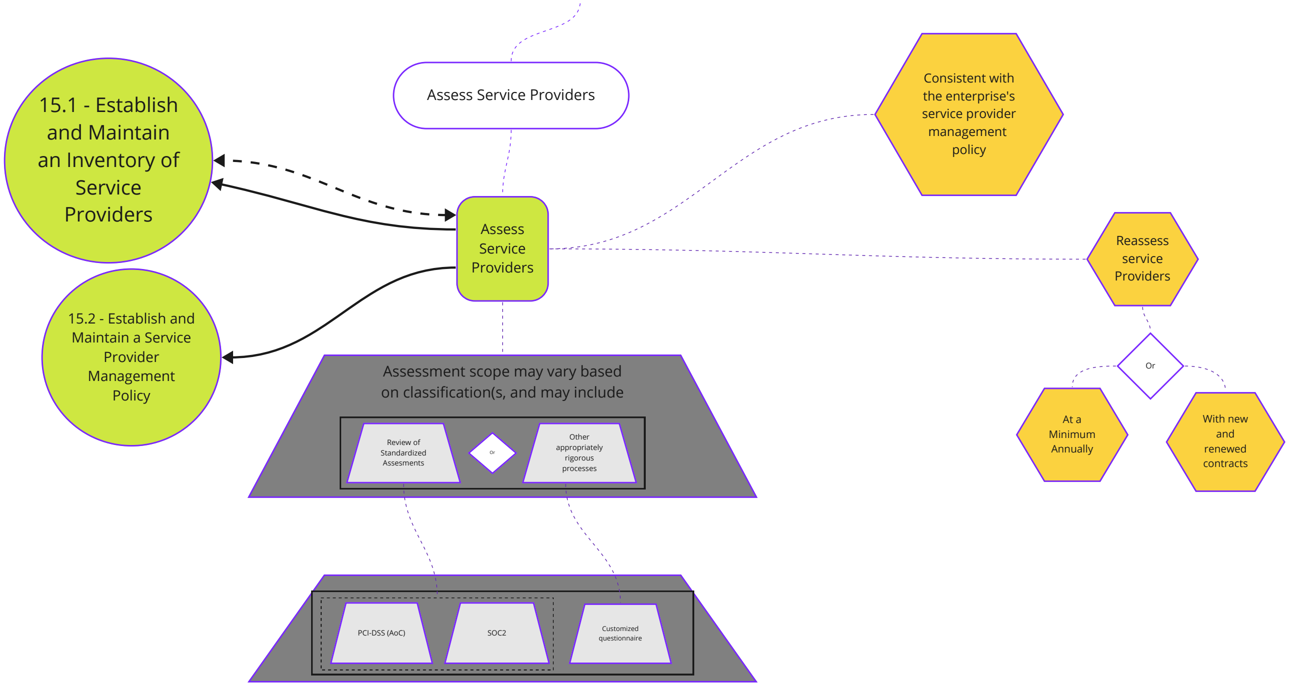
N/A

Contract Management

Group Validated

15.5

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.



Assess Service Providers
15.1 - Establish and Maintain an Inventory of Service Providers
15.2 - Establish and Maintain a Service Provider Management Policy
Assess Service Providers
Consistent with the enterprise's service provider management policy
Reassess service Providers
Or
At a Minimum Annually
With new and renewed contracts
Assessment scope may vary based on classification(s, and may include
Review of Standardized Assesments
Or
Other appropriately rigorous processes
PCI-DSS (AoC)
SOC2
Customized questionnaire

Process Oriented Safeguard

IG3

Identify

N/A

Service Provider Management

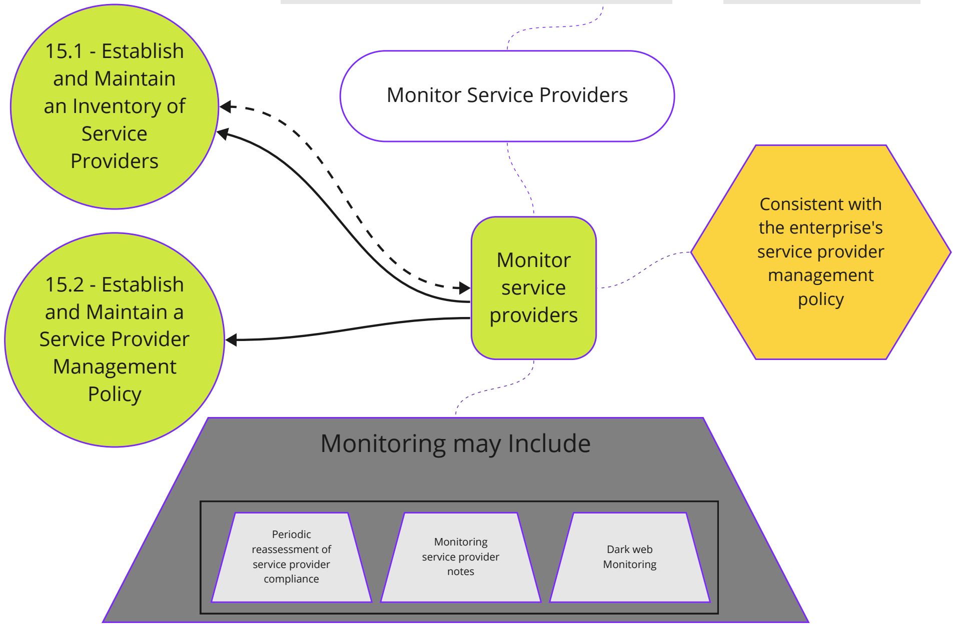
Service Provider Management Policy

Third-Party Risk Management Tool

Group Validated

15.6

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.



Monitor Service Providers

15.1 - Establish and Maintain an Inventory of Service Providers

15.2 - Establish and Maintain a Service Provider Management Policy

Monitor service providers

Consistent with the enterprise's service provider management policy

Monitoring may Include

Periodic reassessment of service provider compliance

Monitoring service provider notes

Dark web Monitoring

Process Oriented Safeguard

IG3

Service Provider Management

Detect

Data

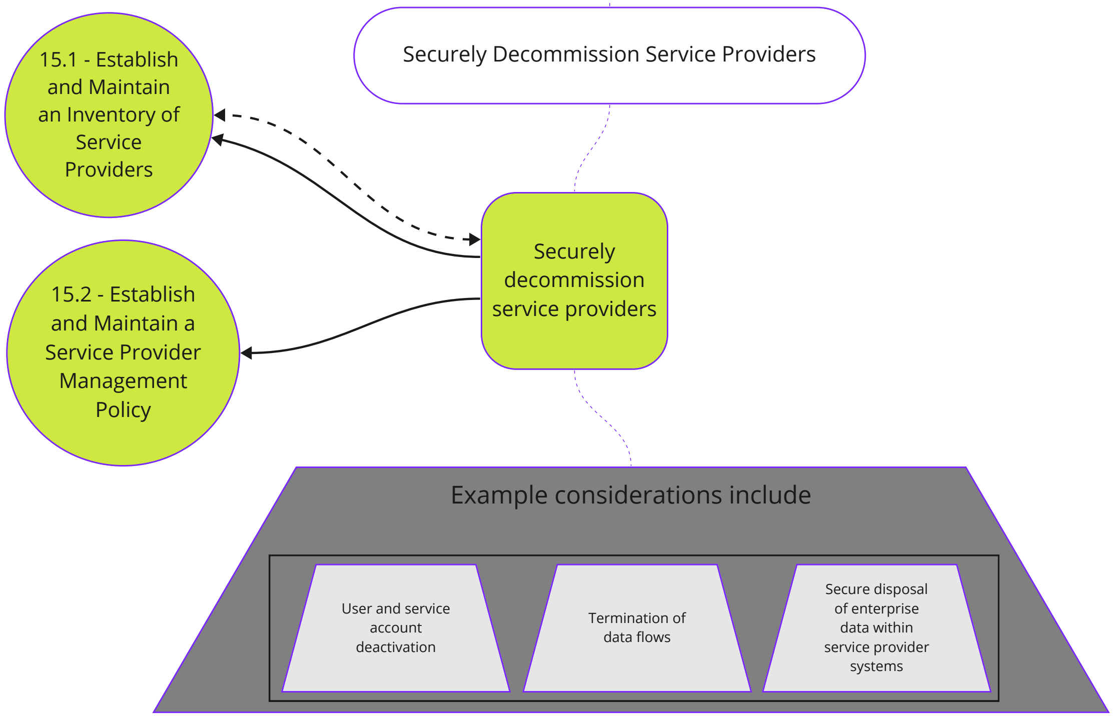
Service Provider Management Policy

Third-Party Risk Management Tool

Group Validated

15.7

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.



Securely Decommission Service Providers

15.1 - Establish and Maintain an Inventory of Service Providers

15.2 - Establish and Maintain a Service Provider Management Policy

Securely decommission service providers

Example considerations include

User and service account deactivation

Termination of data flows

Secure disposal of enterprise data within service provider systems

Process Oriented Safeguard

IG3

Service Provider Management

Protect

Data

Service Provider Management Policy

Third-Party Risk Management Tool

CONTROL 16

Application Software Security

SAFEGUARDS TOTAL	IG1	IG2	IG3
14	0/14	11/14	14/14

Overview

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.

Group Validated

16.1

Process Oriented Safeguard

IG2

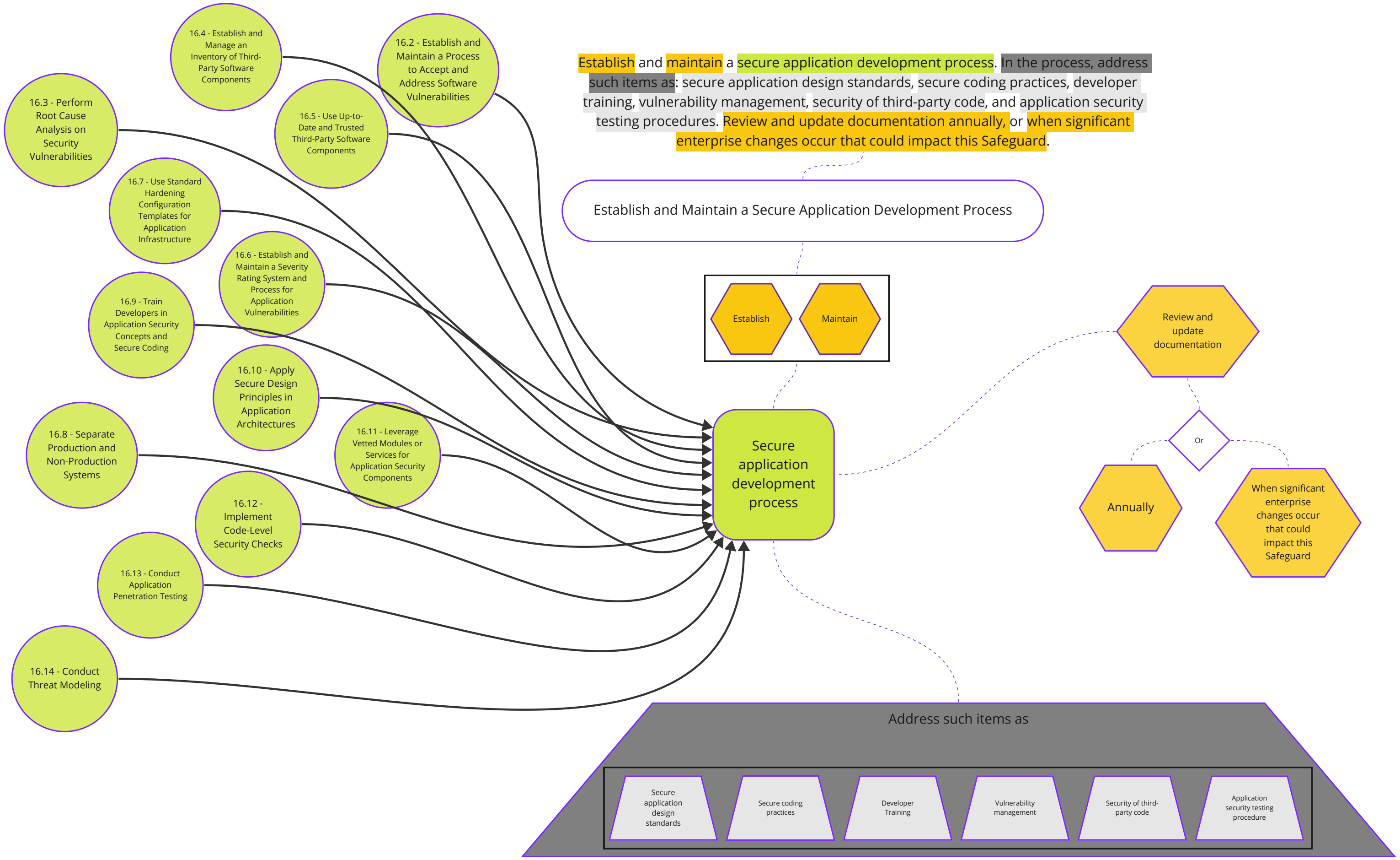
Secure Application Deveploment

Protect

Applications

Secure Application Development Policy / 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.



16.4 - Establish and Manage an Inventory of Third-Party Software Components

16.2 - Establish and Maintain a Process to Accept and Address Software Vulnerabilities

16.3 - Perform Root Cause Analysis on Security Vulnerabilities

16.5 - Use Up-to-Date and Trusted Third-Party Software Components

16.7 - Use Standard Hardening Configuration Templates for Application Infrastructure

16.6 - Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

16.9 - Train Developers in Application Security Concepts and Secure Coding

16.10 - Apply Secure Design Principles in Application Architectures

16.8 - Separate Production and Non-Production Systems

16.11 - Leverage Vetted Modules or Services for Application Security Components

16.12 - Implement Code-Level Security Checks

16.13 - Conduct Application Penetration Testing

16.14 - Conduct Threat Modeling

Establish and Maintain a Secure Application Development Process

Establish

Maintain

Secure application development process

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Address such items as

Secure application design standards

Secure coding practices

Developer Training

Vulnerability management

Security of third-party code

Application security testing procedure

Group Validated

16.2

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.

Process Oriented Safeguard

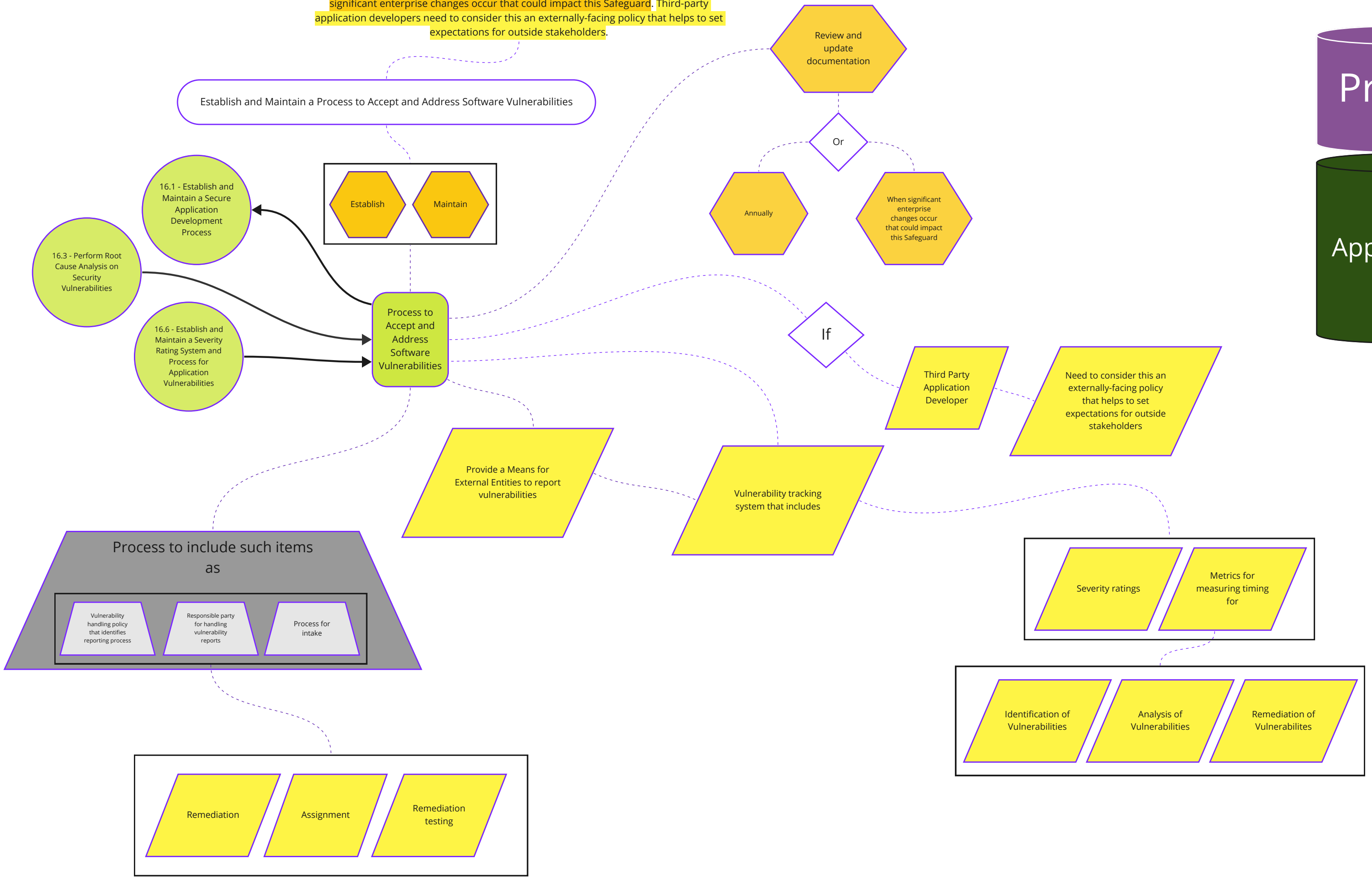
IG2

Secure Application Development

Protect

Software Development Vulnerability Policy / Process

Applications



Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Establish

Maintain

Process to Accept and Address Software Vulnerabilities

16.1 - Establish and Maintain a Secure Application Development Process

16.3 - Perform Root Cause Analysis on Security Vulnerabilities

16.6 - Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Review and update documentation

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

If

Third Party Application Developer

Need to consider this an externally-facing policy that helps to set expectations for outside stakeholders

Provide a Means for External Entities to report vulnerabilities

Vulnerability tracking system that includes

Severity ratings

Metrics for measuring timing for

Identification of Vulnerabilities

Analysis of Vulnerabilities

Remediation of Vulnerabilites

Process to include such items as

Vulnerability handling policy that identifies reporting process

Responsible party for handling vulnerability reports

Process for intake

Remediation

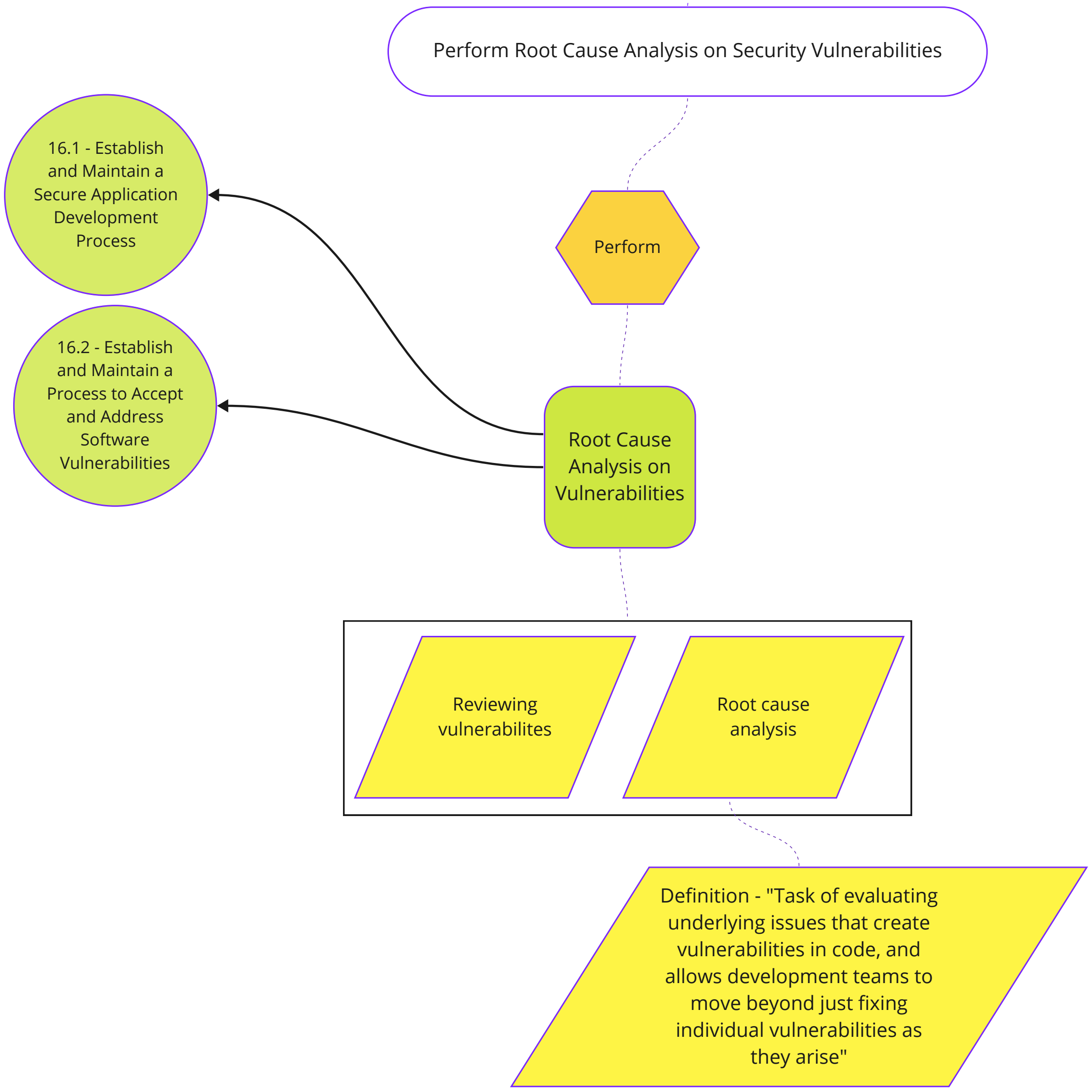
Assignment

Remediation testing

Group Validated

16.3

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.



Perform Root Cause Analysis on Security Vulnerabilities

Perform

Root Cause Analysis on Vulnerabilities

16.1 - Establish and Maintain a Secure Application Development Process

16.2 - Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Reviewing vulnerabilites

Root cause analysis

Definition - "Task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise"

Process Oriented Safeguard

IG2

Secure Application Development

Protect

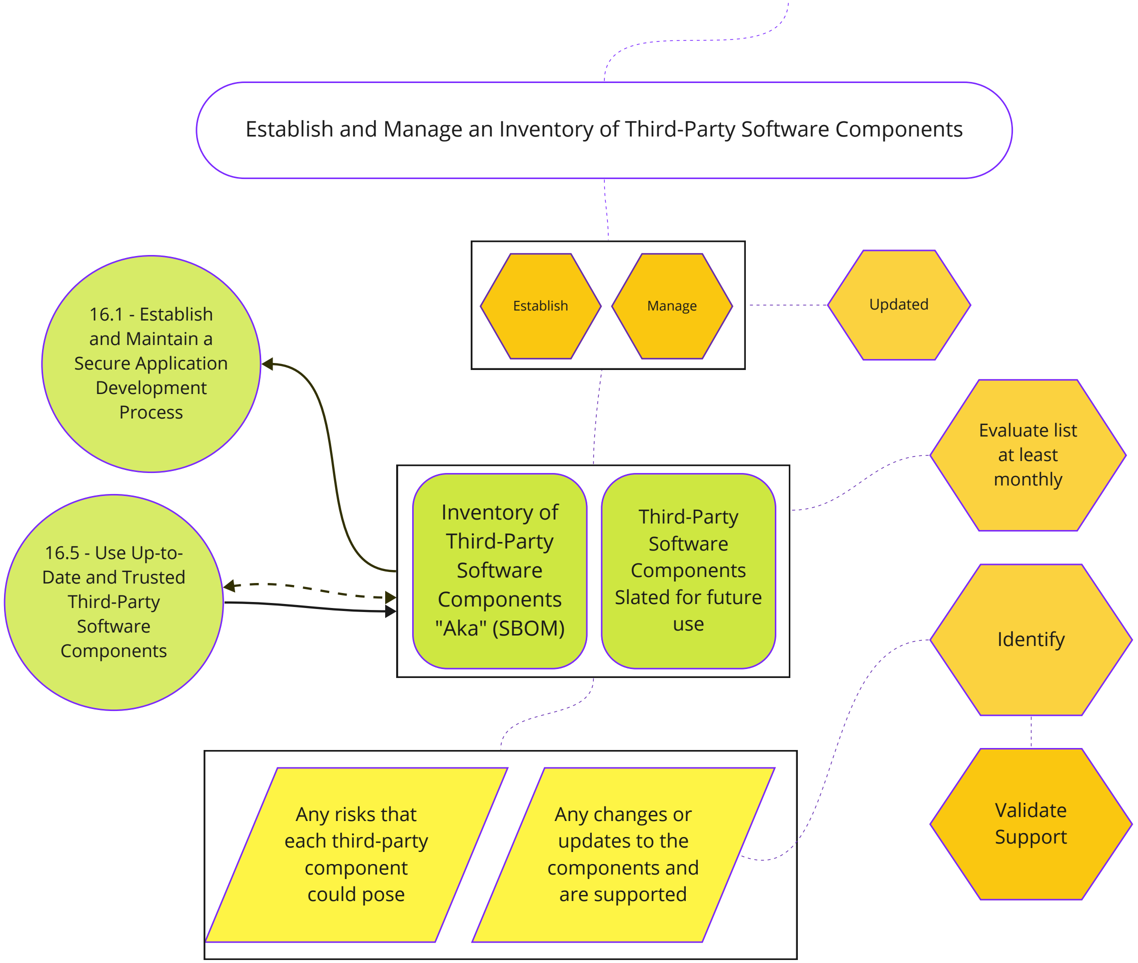
Software Development Vulnerability Policy / Process

Applications

Group Validated

16.4

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.



Establish and Manage an Inventory of Third-Party Software Components

Establish

Manage

Updated

16.1 - Establish and Maintain a Secure Application Development Process

16.5 - Use Up-to-Date and Trusted Third-Party Software Components

Inventory of Third-Party Software Components "Aka" (SBOM)

Third-Party Software Components Slated for future use

Evaluate list at least monthly

Identify

Validate Support

Any risks that each third-party component could pose

Any changes or updates to the components and are supported

Process Oriented Safeguard

IG2

Secure Application Development

Protect

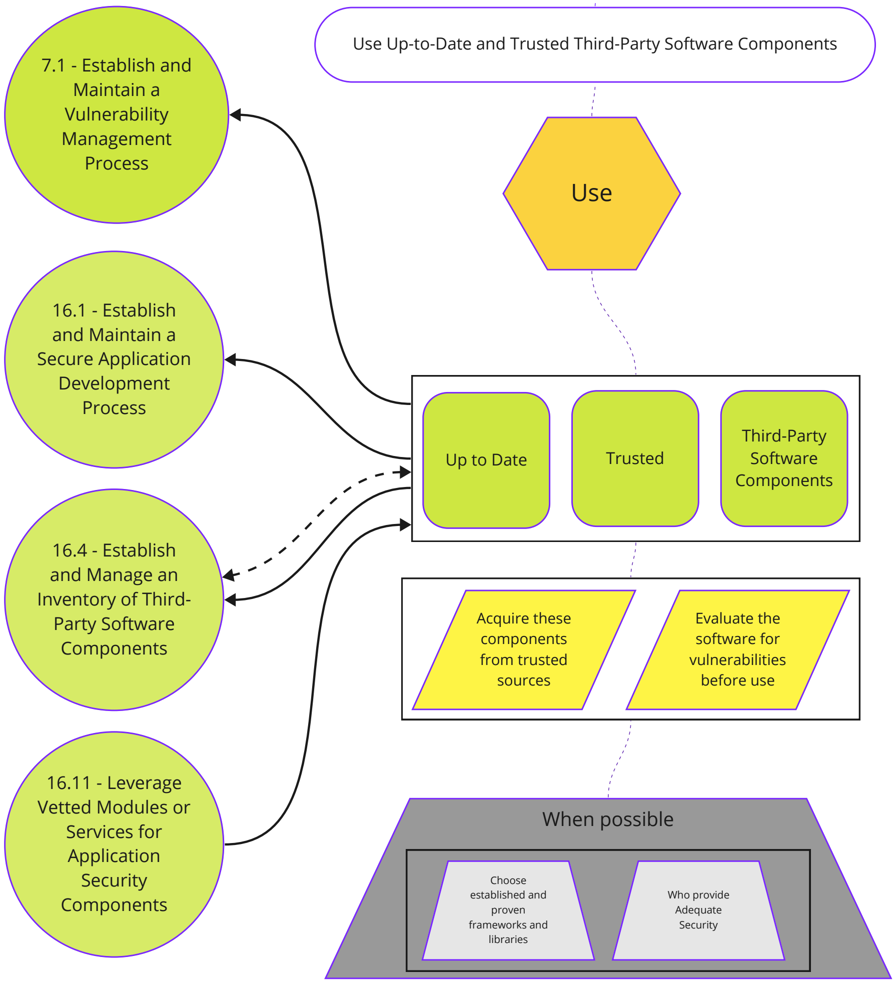
Software Composition Analysis (SCA) Tool

Applications

Group Validated

16.5

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.



Use Up-to-Date and Trusted Third-Party Software Components

Use

Up to Date

Trusted

Third-Party Software Components

Acquire these components from trusted sources

Evaluate the software for vulnerabilities before use

When possible

Choose established and proven frameworks and libraries

Who provide Adequate Security

7.1 - Establish and Maintain a Vulnerability Management Process

16.1 - Establish and Maintain a Secure Application Development Process

16.4 - Establish and Manage an Inventory of Third-Party Software Components

16.11 - Leverage Vetted Modules or Services for Application Security Components

Process Oriented Safeguard

IG2

Secure Application Development

Protect

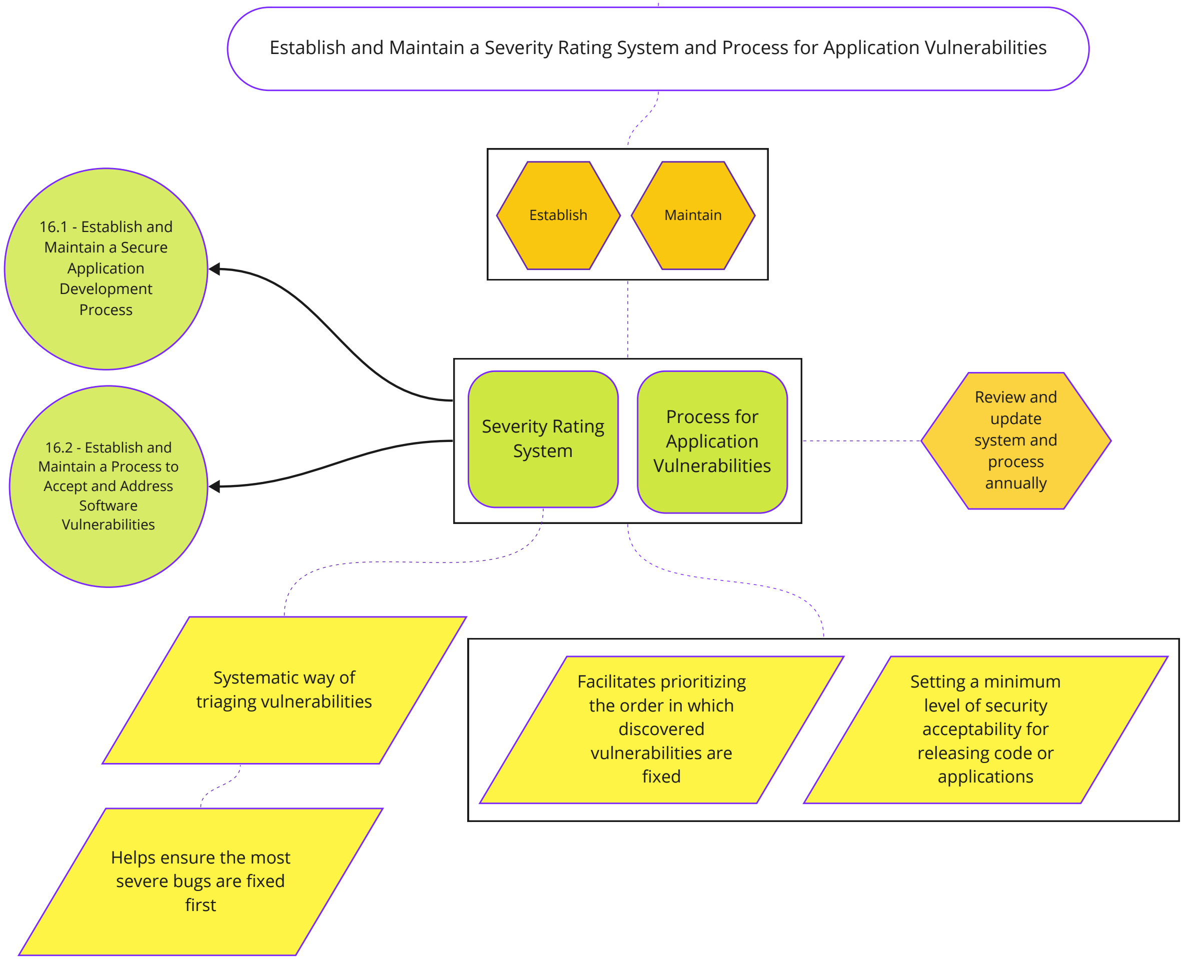
Software Composition Analysis (SCA) Tool

Applications

Group Validated

16.6

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.



Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Establish

Maintain

16.1 - Establish and Maintain a Secure Application Development Process

16.2 - Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Severity Rating System

Process for Application Vulnerabilities

Review and update system and process annually

Systematic way of triaging vulnerabilities

Helps ensure the most severe bugs are fixed first

Facilitates prioritizing the order in which discovered vulnerabilities are fixed

Setting a minimum level of security acceptability for releasing code or applications

Process Oriented Safeguard

IG2

Secure Application Development

Protect

Software Development Vulnerability Policy / Process

Applications

Group Validated

16.7

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.

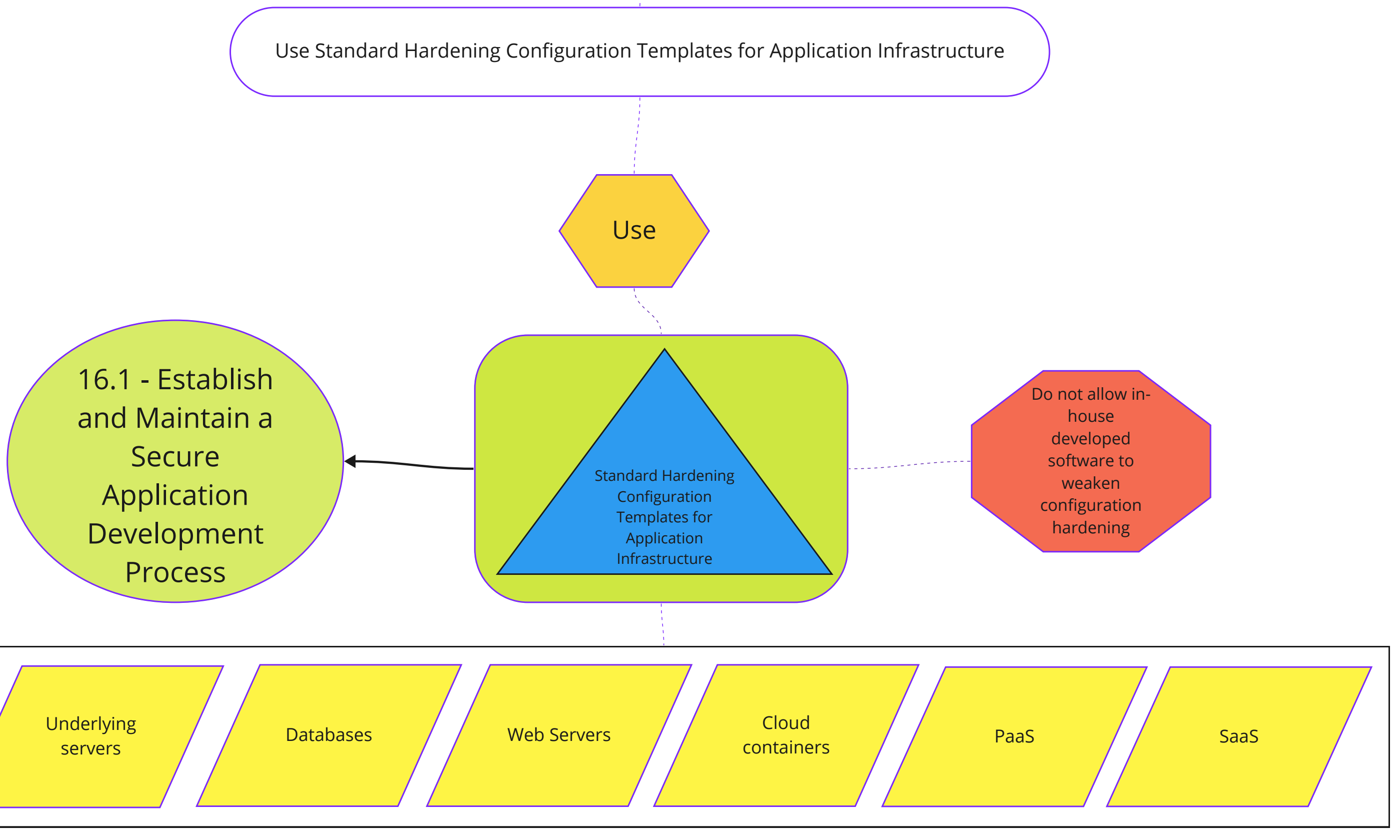
IG2

Secure Application Development

Protect

Applications

Configuration Baseline Tool



Use Standard Hardening Configuration Templates for Application Infrastructure

Use

Standard Hardening Configuration Templates for Application Infrastructure

16.1 - Establish and Maintain a Secure Application Development Process

Do not allow in-house developed software to weaken configuration hardening

Underlying servers

Databases

Web Servers

Cloud containers

PaaS

SaaS

Group Validated

16.8

Maintain separate environments for production and non-production systems.

Process Oriented Safeguard

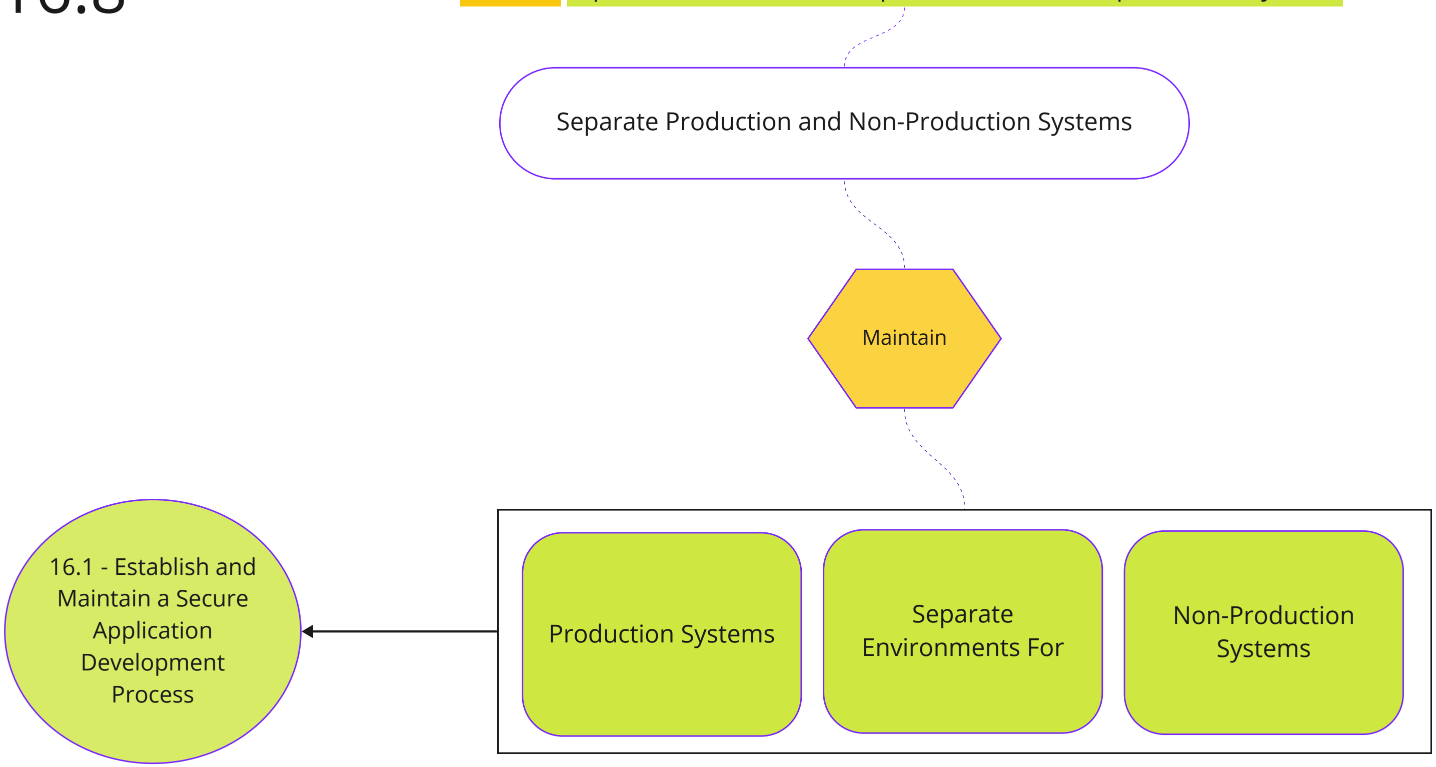
IG2

Secure Application Deveplopment

Protect

Applications

Secure Application Development Policy / Process



Separate Production and Non-Production Systems

Maintain

Production Systems

Separate Environments For

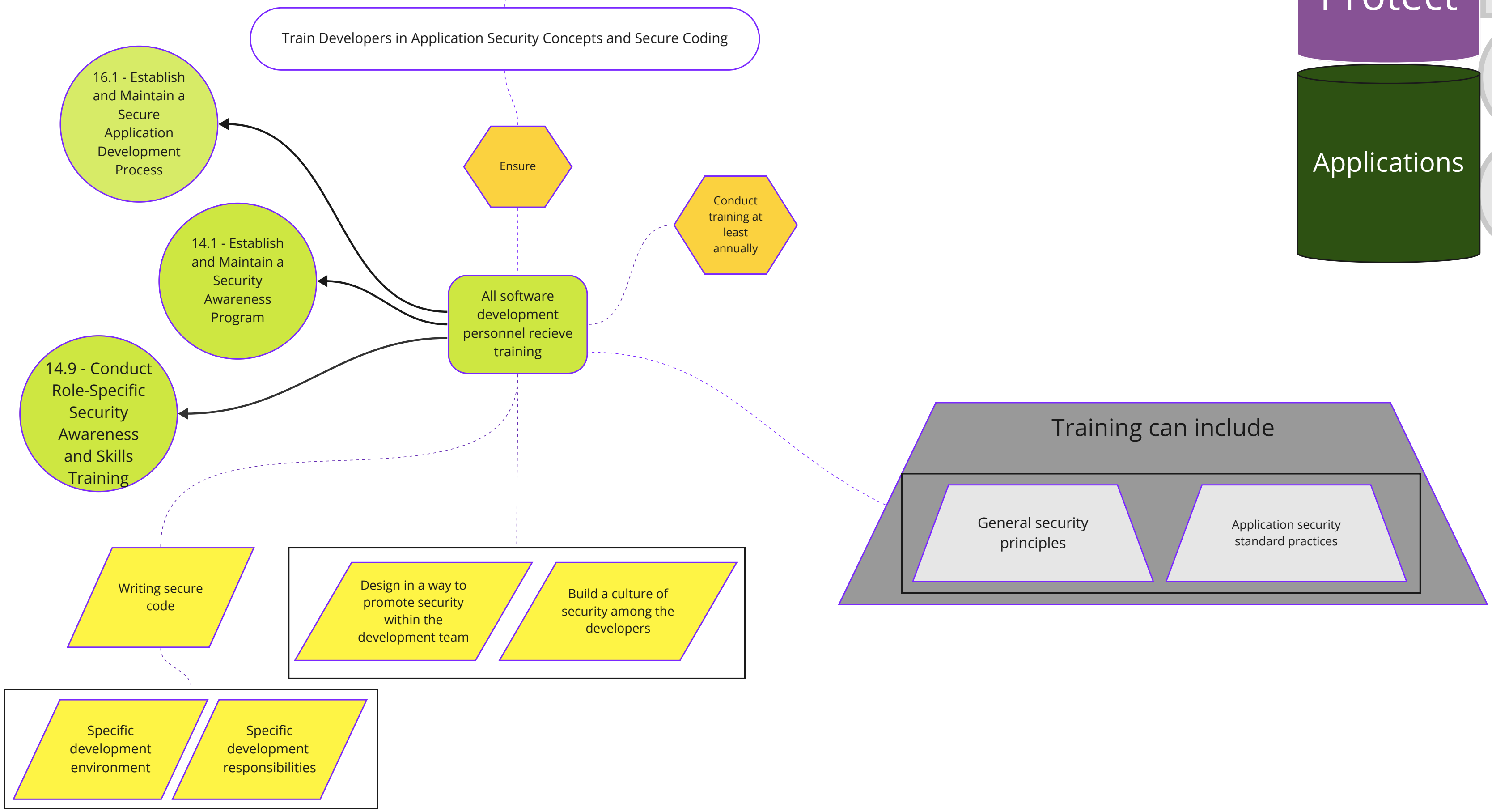
Non-Production Systems

16.1 - Establish and Maintain a Secure Application Development Process

Group Validated

16.9

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.



Train Developers in Application Security Concepts and Secure Coding

Ensure

All software development personnel recieve training

Conduct training at least annually

16.1 - Establish and Maintain a Secure Application Development Process

14.1 - Establish and Maintain a Security Awareness Program

14.9 - Conduct Role-Specific Security Awareness and Skills Training

Writing secure code

Specific development environment

Specific development responsibilities

Design in a way to promote security within the development team

Build a culture of security among the developers

Training can include

General security principles

Application security standard practices

IG2

Protect

Applications

Secure Application Deveplopment

Secure Application Development Policy / Process

Security Training and Awareness Tool(s)

Group Validated

16.10

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.

Process Oriented Safeguard

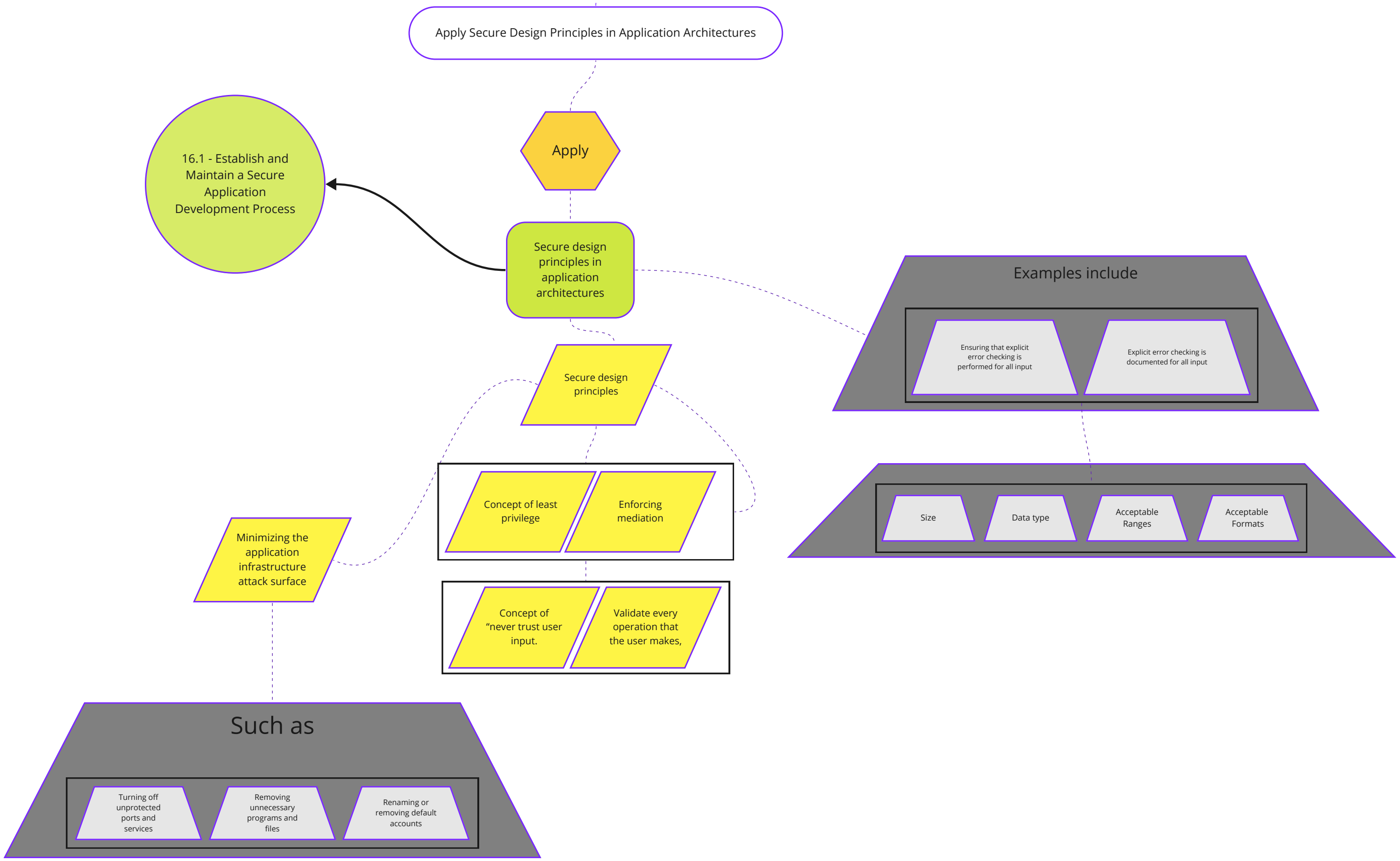
IG2

Secure Application Development

Protect

Secure Application Development Policy / Process

Applications



Apply Secure Design Principles in Application Architectures

Apply

16.1 - Establish and Maintain a Secure Application Development Process

Secure design principles in application architectures

Secure design principles

Concept of least privilege

Enforcing mediation

Concept of “never trust user input.

Validate every operation that the user makes,

Minimizing the application infrastructure attack surface

Such as

Turning off unprotected ports and services

Removing unnecessary programs and files

Renaming or removing default accounts

Examples include

Ensuring that explicit error checking is performed for all input

Explicit error checking is documented for all input

Size

Data type

Acceptable Ranges

Acceptable Formats

Group Validated

16.11

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.

Process Oriented Safeguard

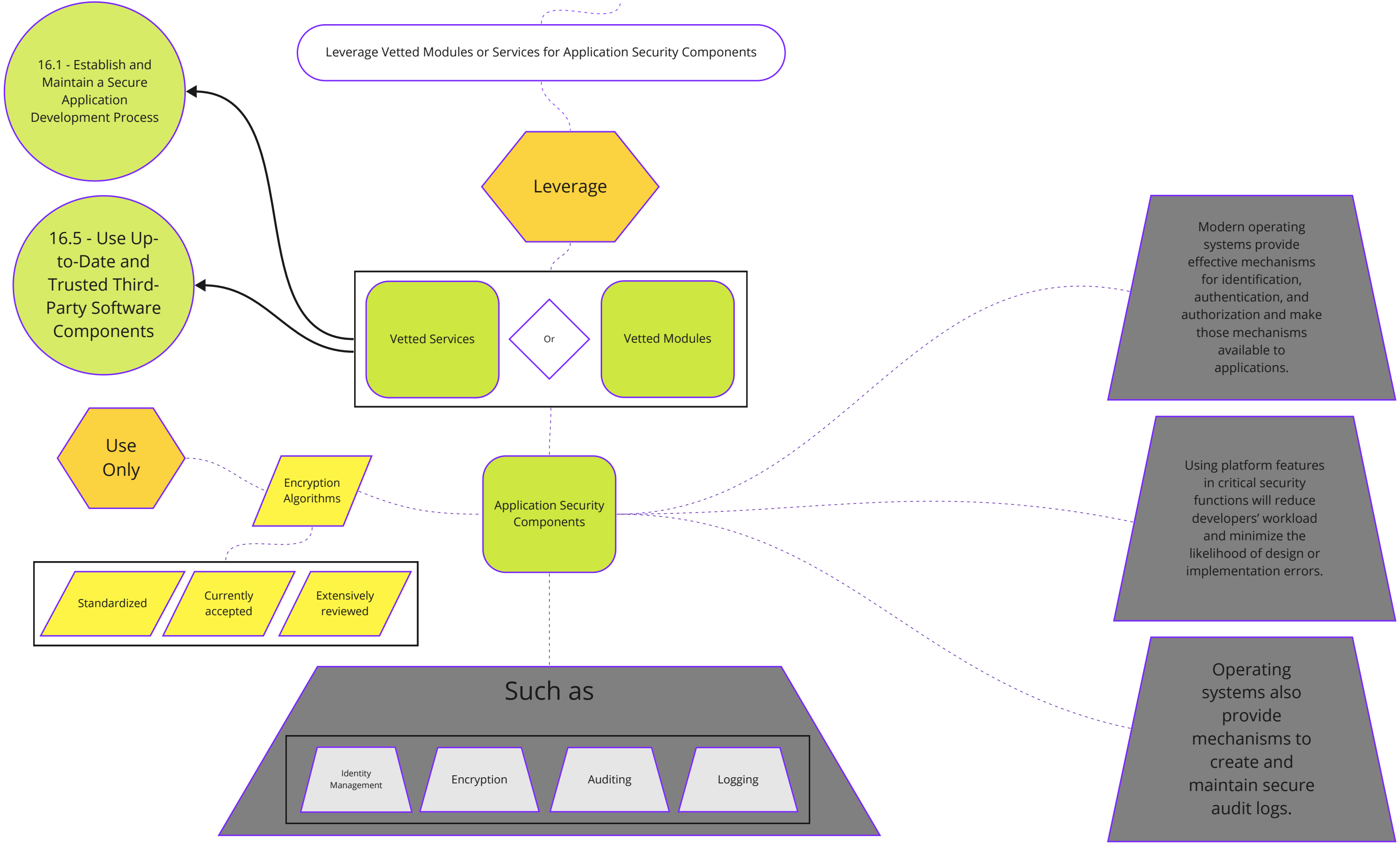
IG2

Secure Application Development

Protect

Applications

Secure Application Development Policy / Process



Leverage Vetted Modules or Services for Application Security Components

Leverage

Vetted Services

Or

Vetted Modules

16.1 - Establish and Maintain a Secure Application Development Process

16.5 - Use Up-to-Date and Trusted Third-Party Software Components

Application Security Components

Use Only

Encryption Algorithms

Standardized

Currently accepted

Extensively reviewed

Such as

Identity Management

Encryption

Auditing

Logging

Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications.

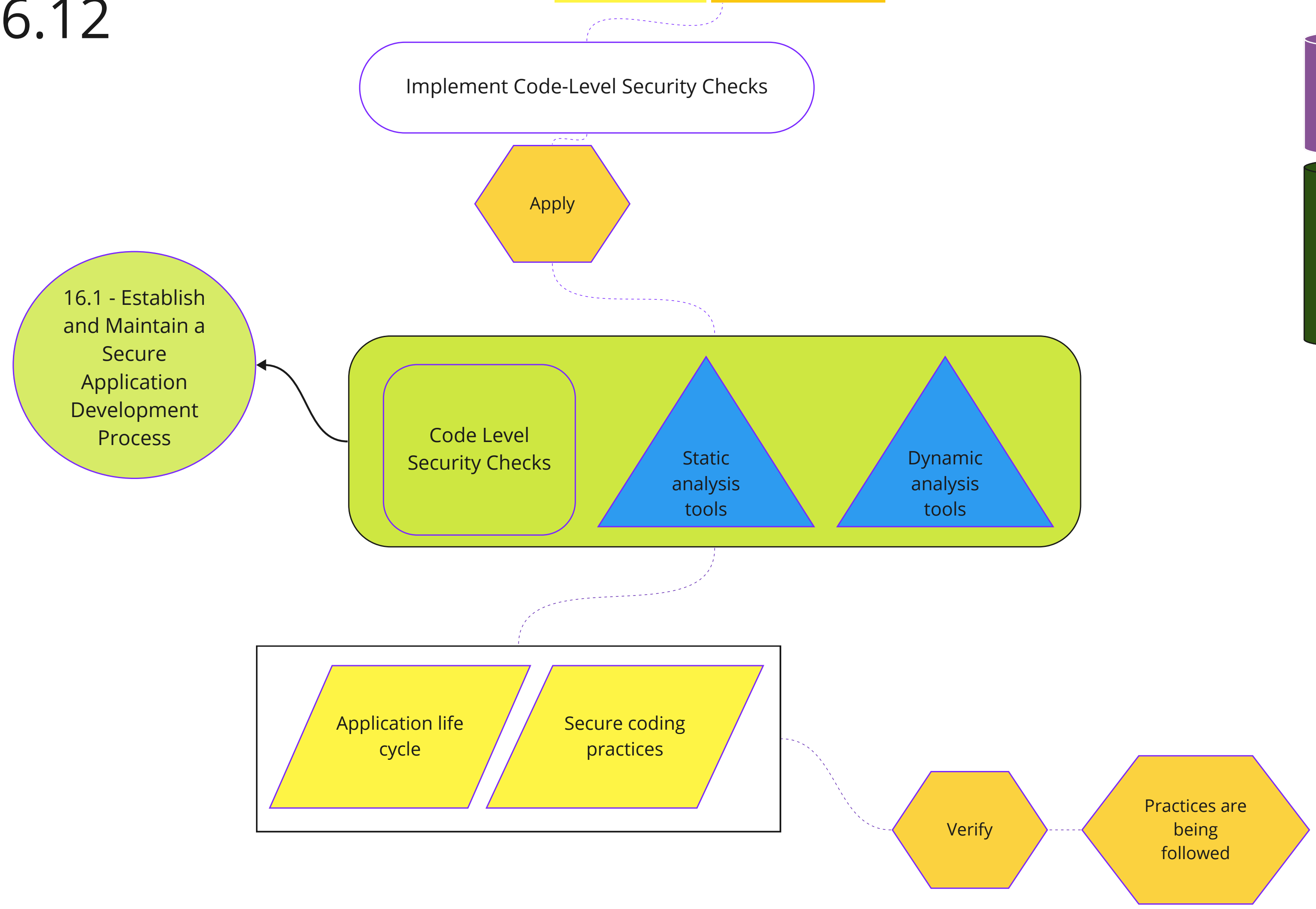
Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors.

Operating systems also provide mechanisms to create and maintain secure audit logs.

Group Validated

16.12

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.



Implement Code-Level Security Checks

Apply

16.1 - Establish and Maintain a Secure Application Development Process

Code Level Security Checks

Static analysis tools

Dynamic analysis tools

Application life cycle

Secure coding practices

Verify

Practices are being followed

IG3

Protect

Applications

Secure Application Development

Code Analysis Tool

Group Validated

16.13

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.

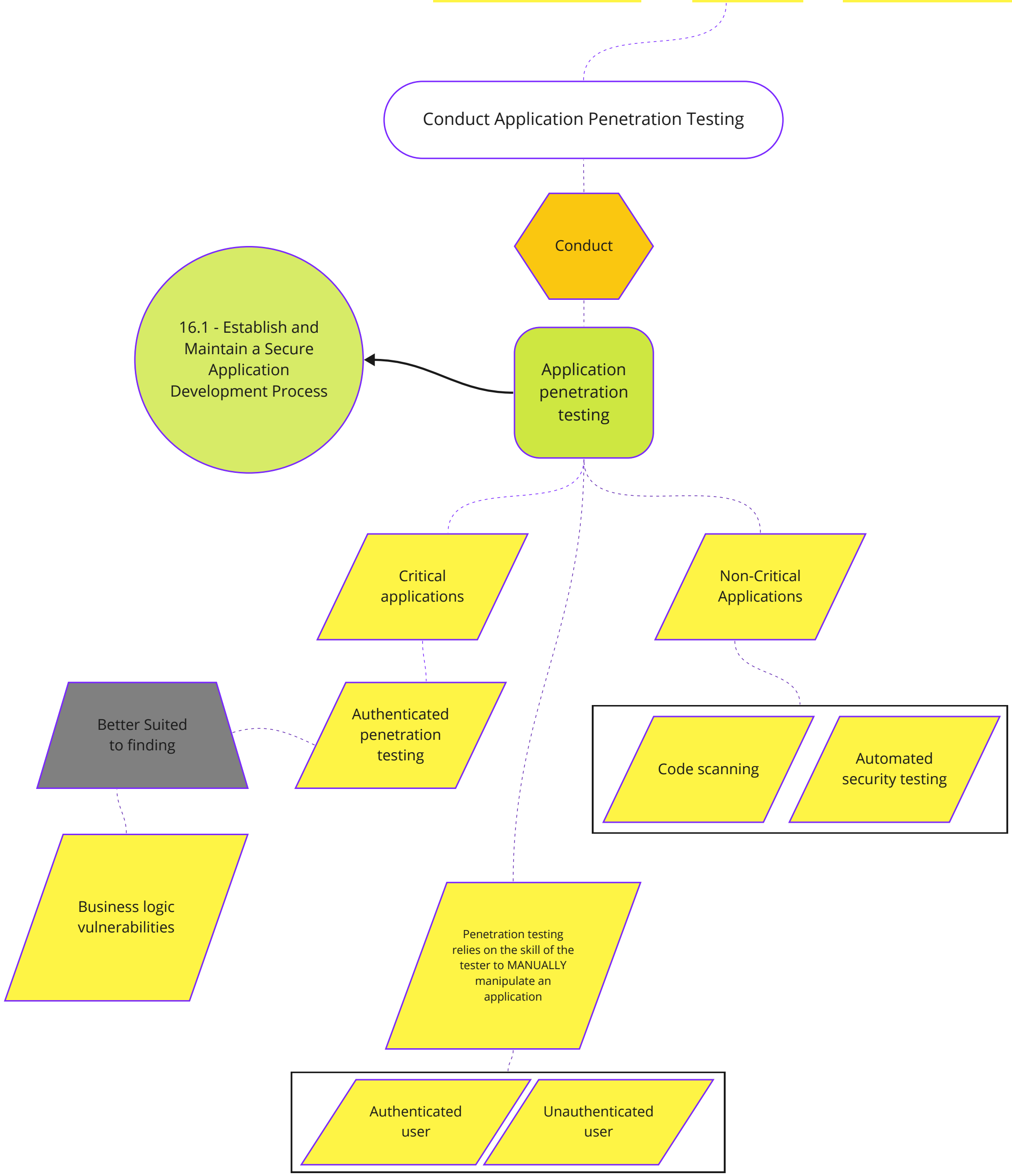
IG3

Protect

Applications

Secure Application Development

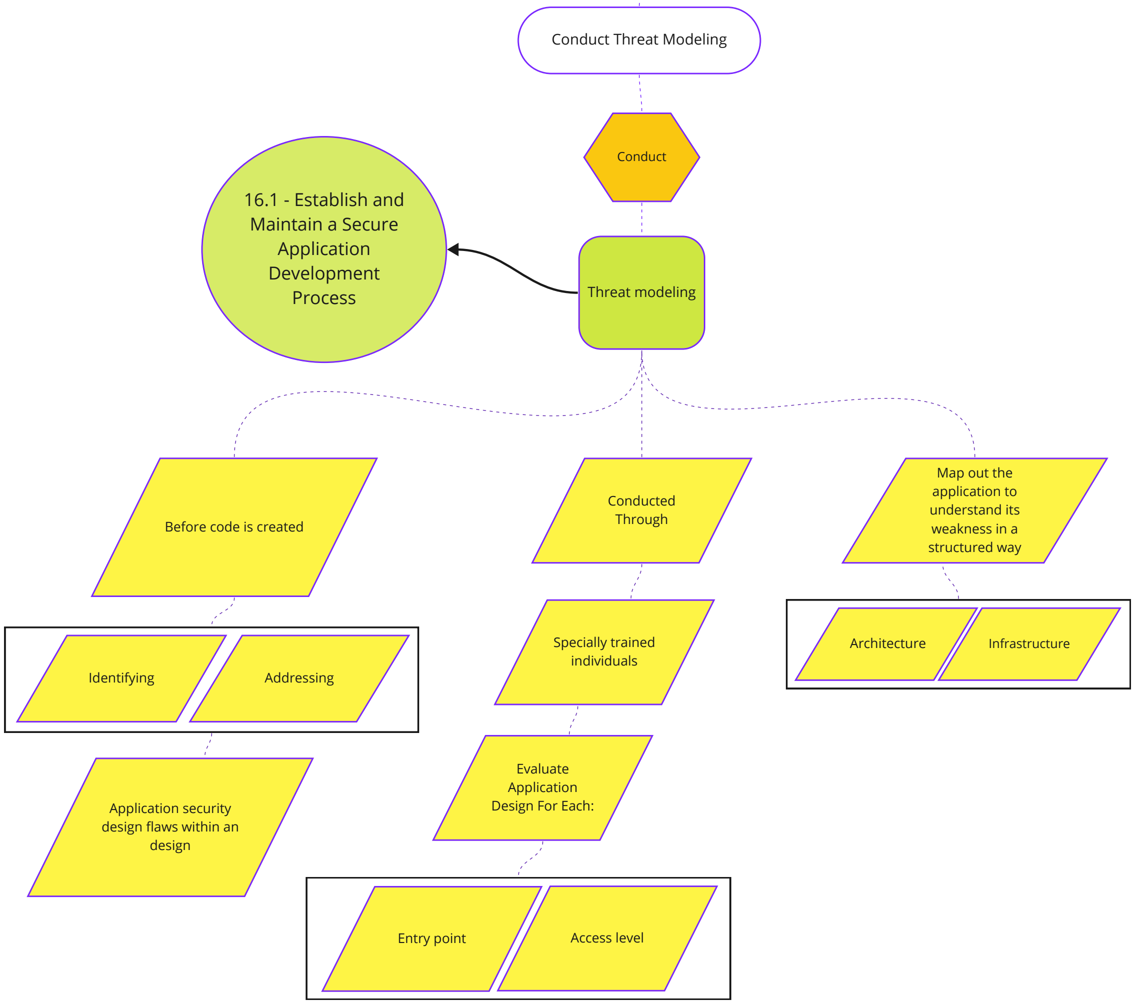
Application Security Testing


Conduct Application Penetration Testing
Conduct
Application penetration testing
16.1 - Establish and Maintain a Secure Application Development Process
Critical applications
Non-Critical Applications
Better Suited to finding
Authenticated penetration testing
Code scanning
Automated security testing
Business logic vulnerabilities
Penetration testing relies on the skill of the tester to MANUALLY manipulate an application
Authenticated user
Unauthenticated user

Group Validated

16.14

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.



Conduct Threat Modeling

Conduct

Threat modeling

16.1 - Establish and Maintain a Secure Application Development Process

Before code is created

Identifying

Addressing

Application security design flaws within an design

Conducted Through

Specially trained individuals

Evaluate Application Design For Each:

Entry point

Access level

Map out the application to understand its weakness in a structured way

Architecture

Infrastructure

Process Oriented Safeguard

IG3

Secure Application Development

Protect

Secure Application Development Policy / Process

Applications

CONTROL 17

Incident Response Management

Safeguards Total	IG1	IG2	IG3
9	3/9	8/9	9/9

Overview

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.

Group Validated

17.1

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.

Process Oriented Safeguard

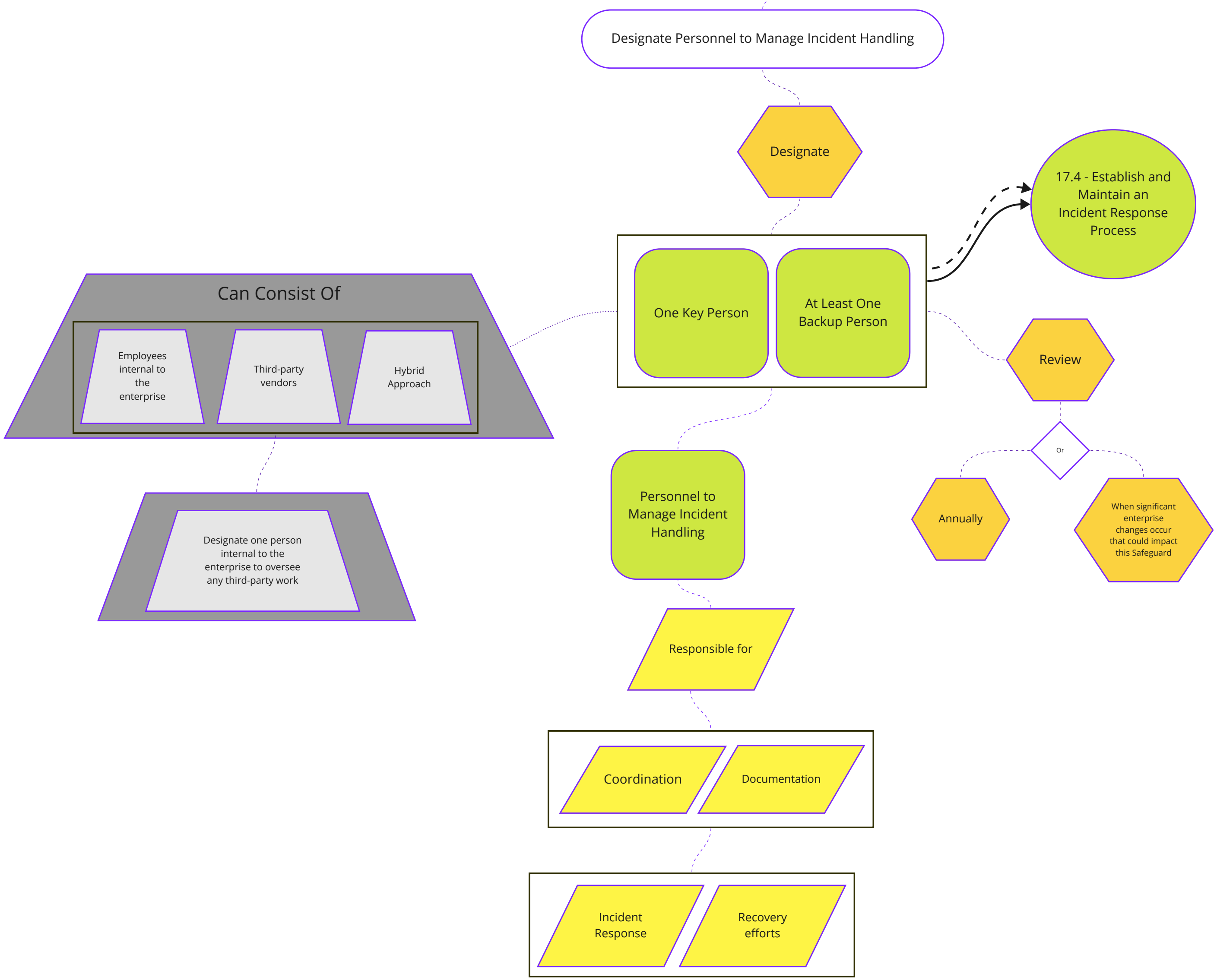
IG1

Incident Response

Respond

Incident Response Planning

N/A



Designate Personnel to Manage Incident Handling

Designate

One Key Person

At Least One Backup Person

17.4 - Establish and Maintain an Incident Response Process

Can Consist Of

Employees internal to the enterprise

Third-party vendors

Hybrid Approach

Designate one person internal to the enterprise to oversee any third-party work

Review

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Personnel to Manage Incident Handling

Responsible for

Coordination

Documentation

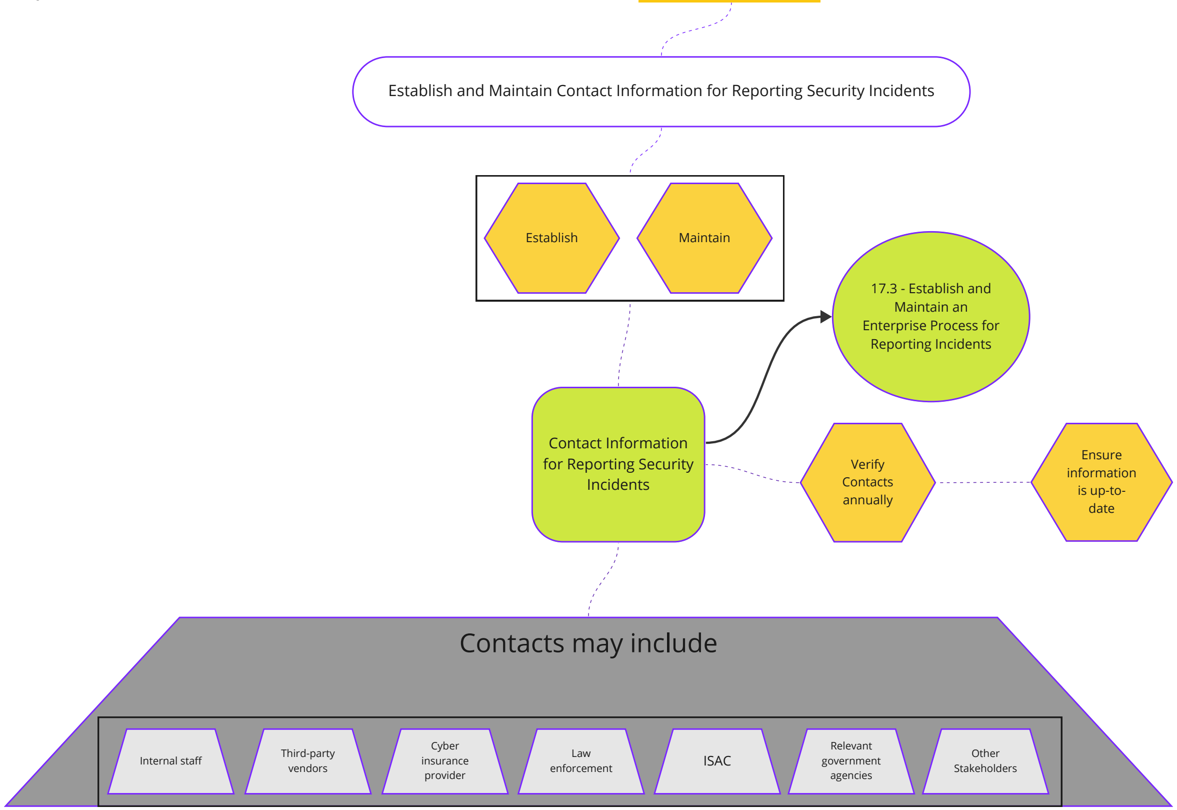
Incident Response

Recovery efforts

Group Validated

17.2

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.



Establish and Maintain Contact Information for Reporting Security Incidents
Establish
Maintain
17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents
Contact Information for Reporting Security Incidents
Verify Contacts annually
Ensure information is up-to-date
Contacts may include
Internal staff
Third-party vendors
Cyber insurance provider
Law enforcement
ISAC
Relevant government agencies
Other Stakeholders

Process Oriented Safeguard

IG1

Incident Response

Respond

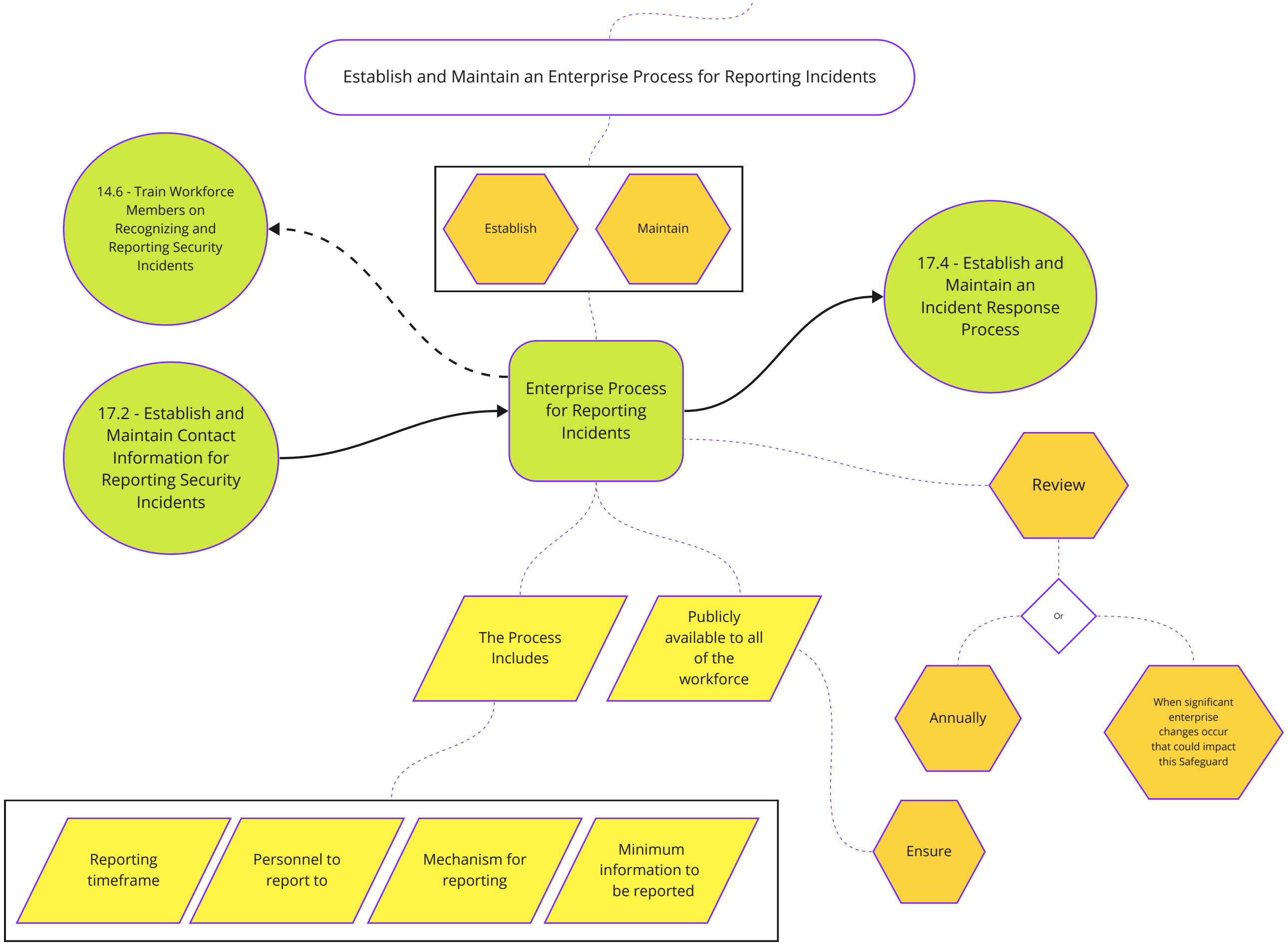
N/A

Incident Response Planning

Group Validated

17.3

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.



Establish and Maintain an Enterprise Process for Reporting Incidents

Establish

Maintain

14.6 - Train Workforce Members on Recognizing and Reporting Security Incidents

17.2 - Establish and Maintain Contact Information for Reporting Security Incidents

Enterprise Process for Reporting Incidents

17.4 - Establish and Maintain an Incident Response Process

Review

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

The Process Includes

Publicly available to all of the workforce

Ensure

Reporting timeframe

Personnel to report to

Mechanism for reporting

Minimum information to be reported

Process Oriented Safeguard

IG1

Incident Response

Respond

N/A

Incident Response Planning

Group Validated

17.4

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.

Process Oriented Safeguard

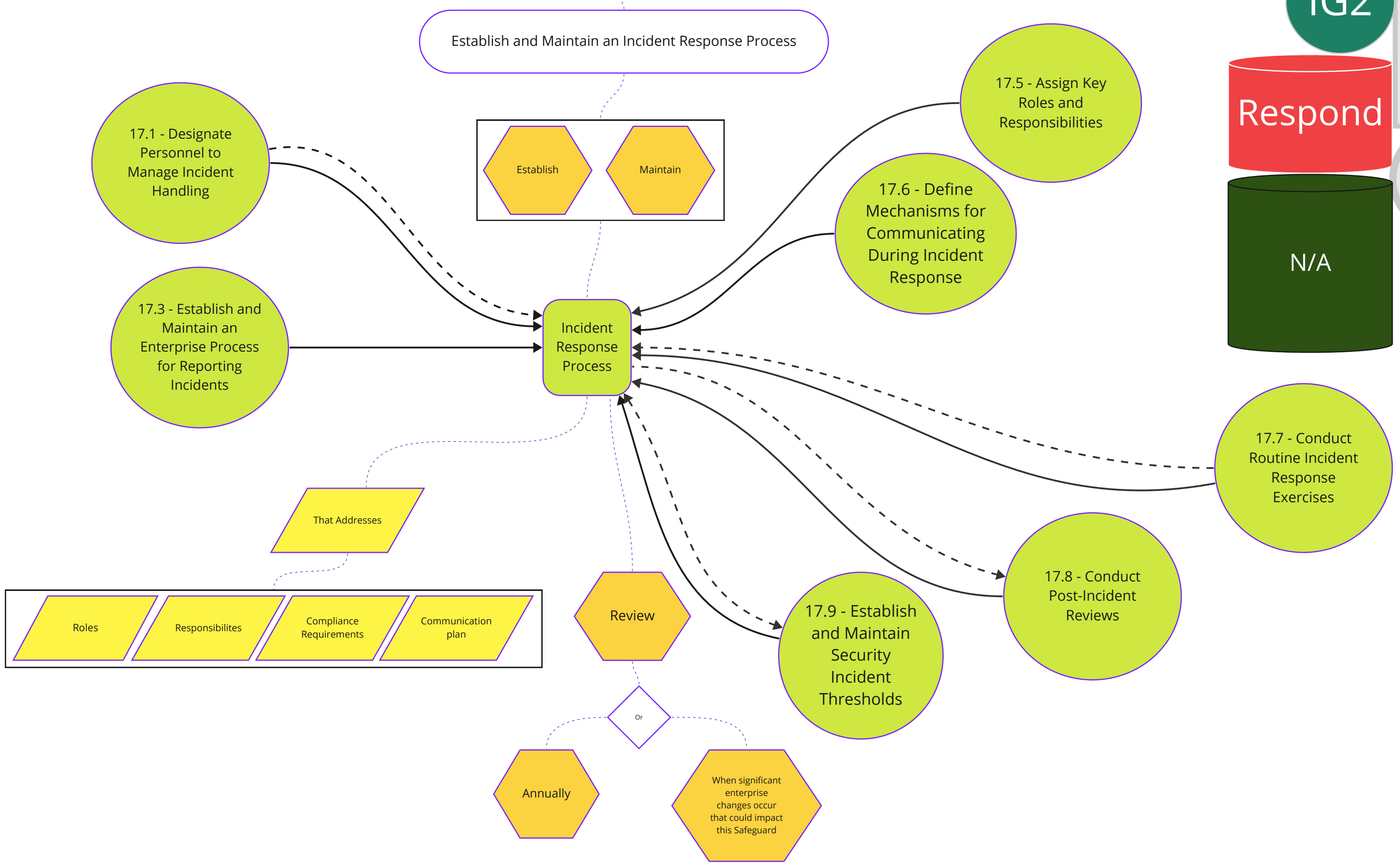
IG2

Incident Response

Respond

Incident Response Planning

N/A

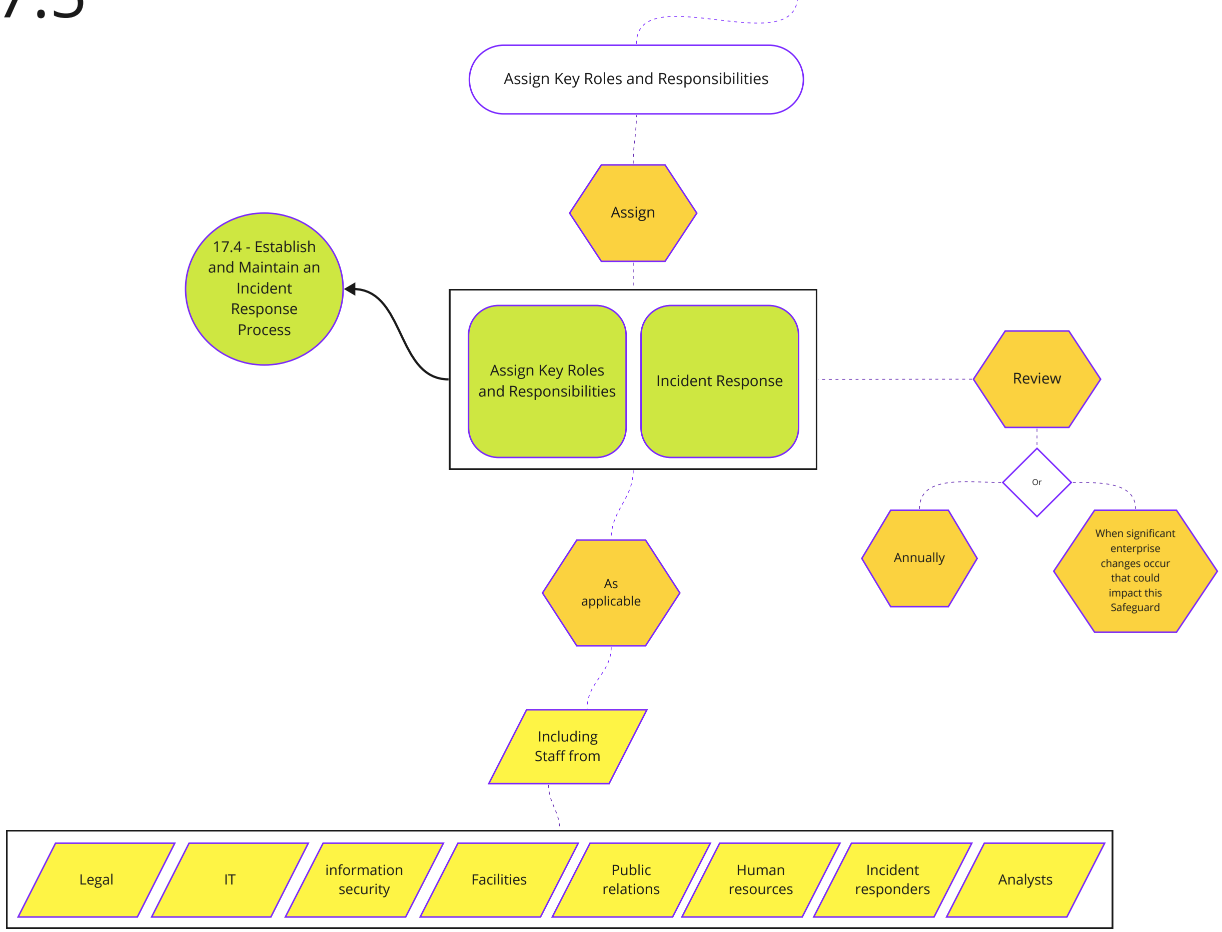


Establish and Maintain an Incident Response Process
Establish
Maintain
17.1 - Designate Personnel to Manage Incident Handling
17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents
Incident Response Process
17.5 - Assign Key Roles and Responsibilities
17.6 - Define Mechanisms for Communicating During Incident Response
17.7 - Conduct Routine Incident Response Exercises
17.8 - Conduct Post-Incident Reviews
17.9 - Establish and Maintain Security Incident Thresholds
That Addresses
Roles
Responsibilites
Compliance Requirements
Communication plan
Review
Or
Annually
When significant enterprise changes occur that could impact this Safeguard

Group Validated

17.5

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.



Assign Key Roles and Responsibilities

Assign

17.4 - Establish and Maintain an Incident Response Process

Assign Key Roles and Responsibilities

Incident Response

Review

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

As applicable

Including Staff from

Legal

IT

information security

Facilities

Public relations

Human resources

Incident responders

Analysts

Process Oriented Safeguard

IG2

Incident Response

Respond

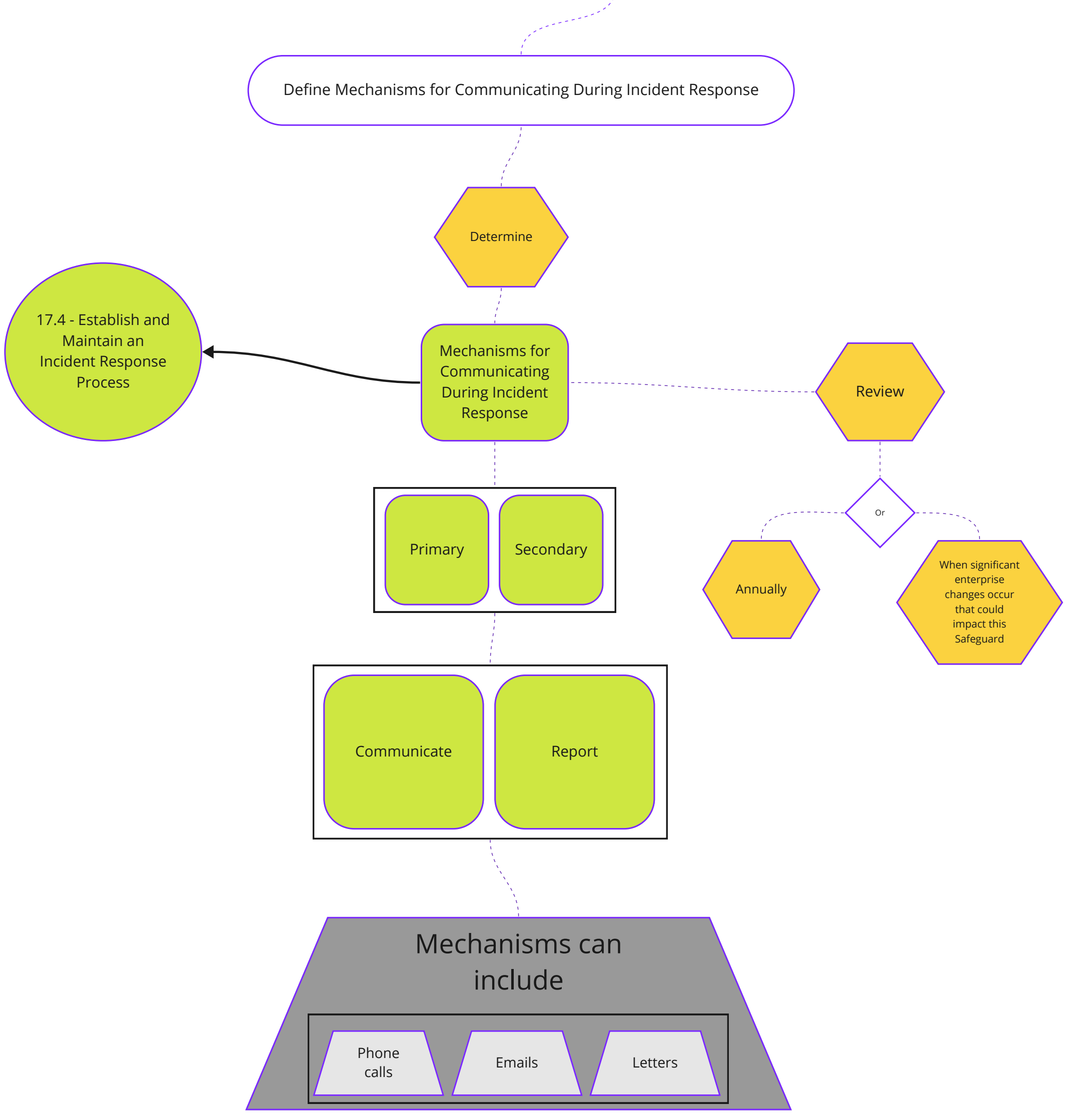
Incident Response Planning

N/A

Group Validated

17.6

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.



Define Mechanisms for Communicating During Incident Response

Determine

Mechanisms for Communicating During Incident Response

17.4 - Establish and Maintain an Incident Response Process

Primary

Secondary

Communicate

Report

Mechanisms can include

Phone calls

Emails

Letters

Review

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

Process Oriented Safeguard

IG2

Incident Response

Respond

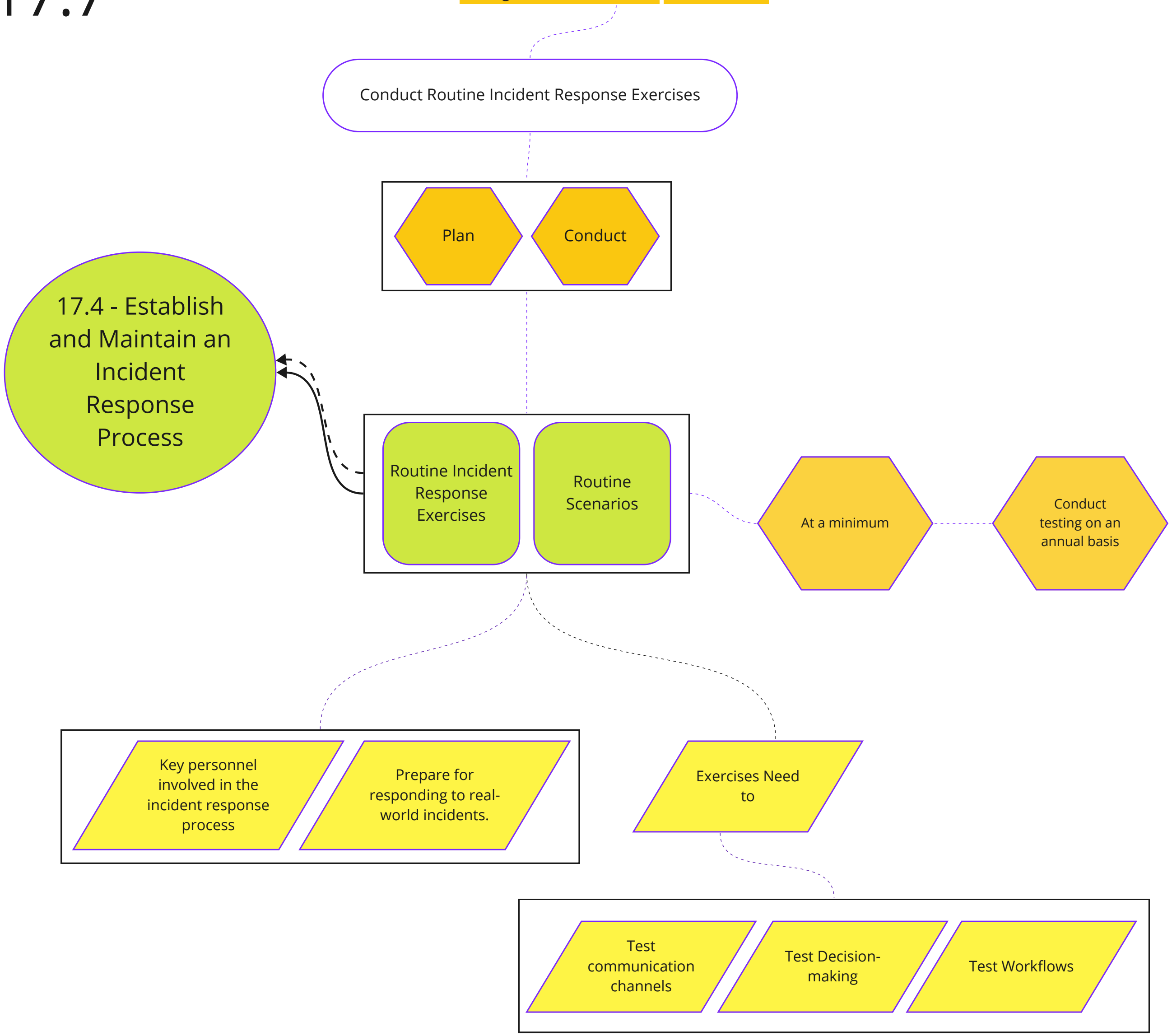
Incident Response Planning

N/A

Group Validated

17.7

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.



Conduct Routine Incident Response Exercises

Plan

Conduct

17.4 - Establish and Maintain an Incident Response Process

Routine Incident Response Exercises

Routine Scenarios

At a minimum

Conduct testing on an annual basis

Key personnel involved in the incident response process

Prepare for responding to real-world incidents.

Exercises Need to

Test communication channels

Test Decision-making

Test Workflows

Process Oriented Safeguard

IG2

Incident Response

Recover

Incident Response Planning

N/A

Group Validated

17.8

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Process Oriented Safeguard

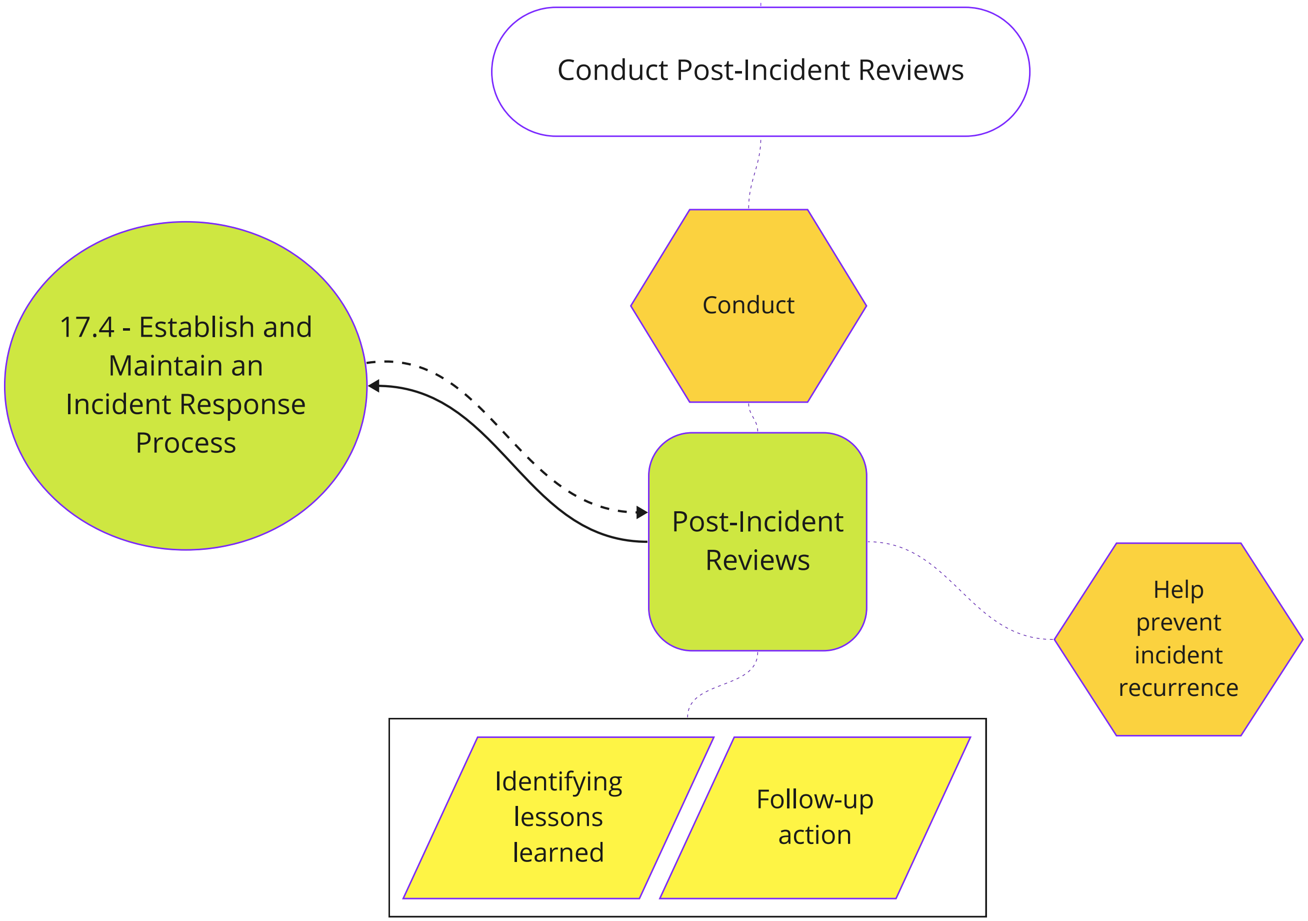
IG2

Incident Response

Recover

Incident Response Planning

N/A



Conduct Post-Incident Reviews

Conduct

17.4 - Establish and Maintain an Incident Response Process

Post-Incident Reviews

Help prevent incident recurrence

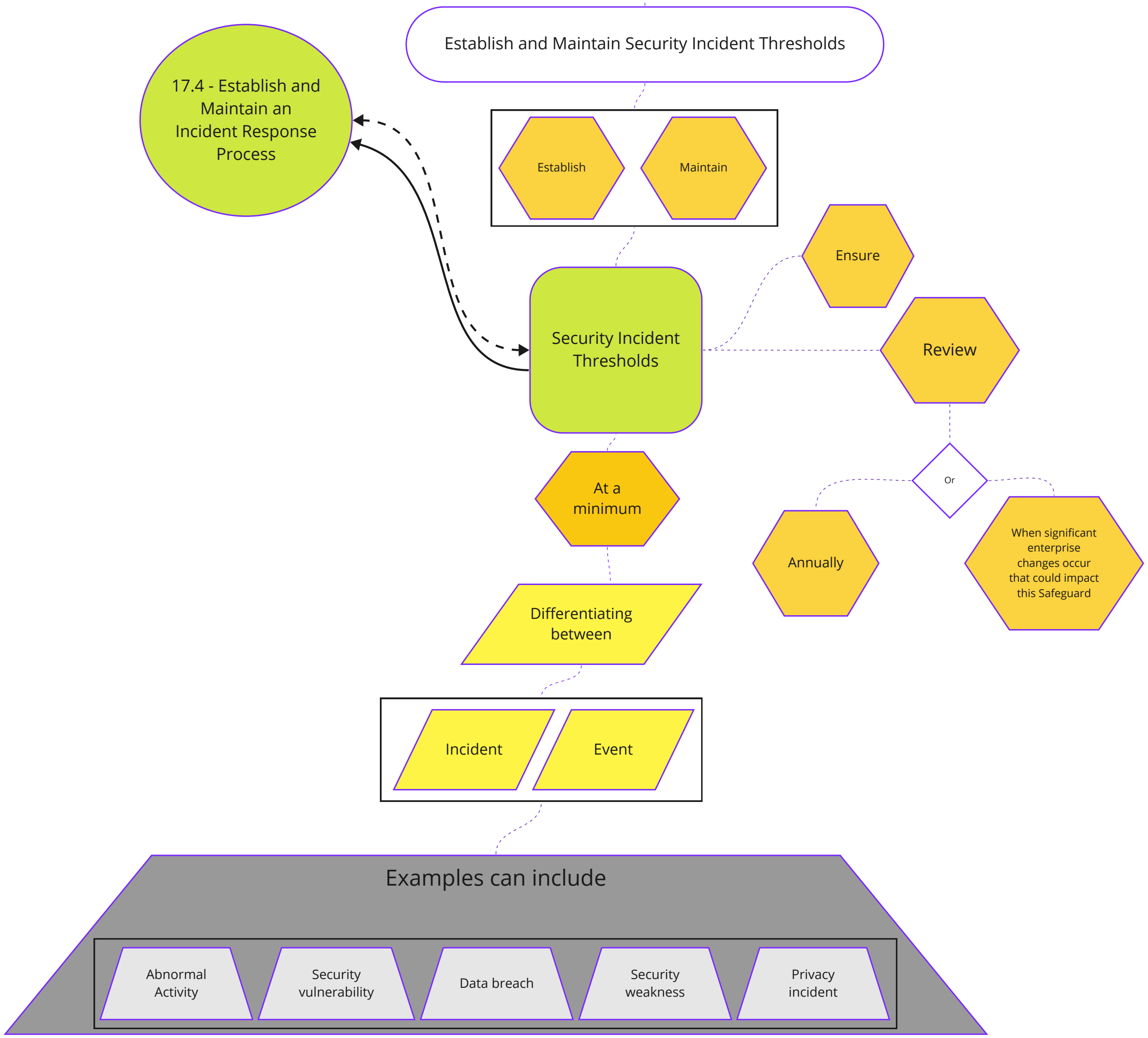
Identifying lessons learned

Follow-up action

Group Validated

17.9

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.



Establish and Maintain Security Incident Thresholds

Establish

Maintain

17.4 - Establish and Maintain an Incident Response Process

Security Incident Thresholds

Ensure

Review

Or

Annually

When significant enterprise changes occur that could impact this Safeguard

At a minimum

Differentiating between

Incident

Event

Examples can include

Abnormal Activity

Security vulnerability

Data breach

Security weakness

Privacy incident

Process Oriented Safeguard

IG3

Incident Response

Recover

Incident Response Planning

N/A

CONTROL 18

Penetration Testing

Safeguards Total 5 — IG1 0/5 — IG2 3/5 — IG3 5/5

Overview

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.

Group Validated

18.1

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.

Process Oriented Safeguard

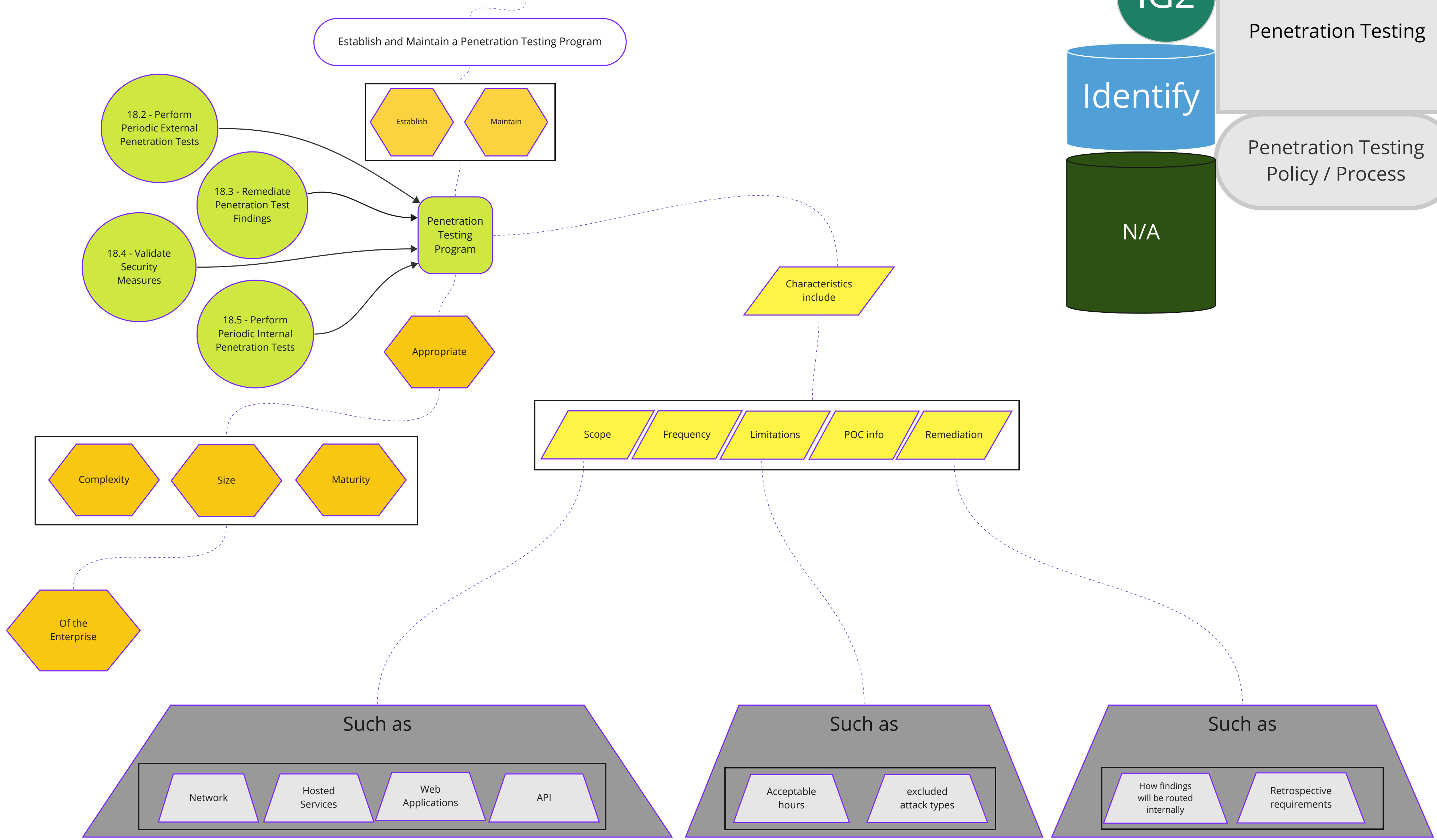
IG2

Penetration Testing

Identify

Penetration Testing Policy / Process

N/A



Establish and Maintain a Penetration Testing Program

Establish

Maintain

Penetration Testing Program

18.2 - Perform Periodic External Penetration Tests

18.3 - Remediate Penetration Test Findings

18.4 - Validate Security Measures

18.5 - Perform Periodic Internal Penetration Tests

Appropriate

Complexity

Size

Maturity

Of the Enterprise

Characteristics include

Scope

Frequency

Limitations

POC info

Remediation

Such as

Network

Hosted Services

Web Applications

API

Such as

Acceptable hours

excluded attack types

Such as

How findings will be routed internally

Retrospective requirements

Group Validated

18.2

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.

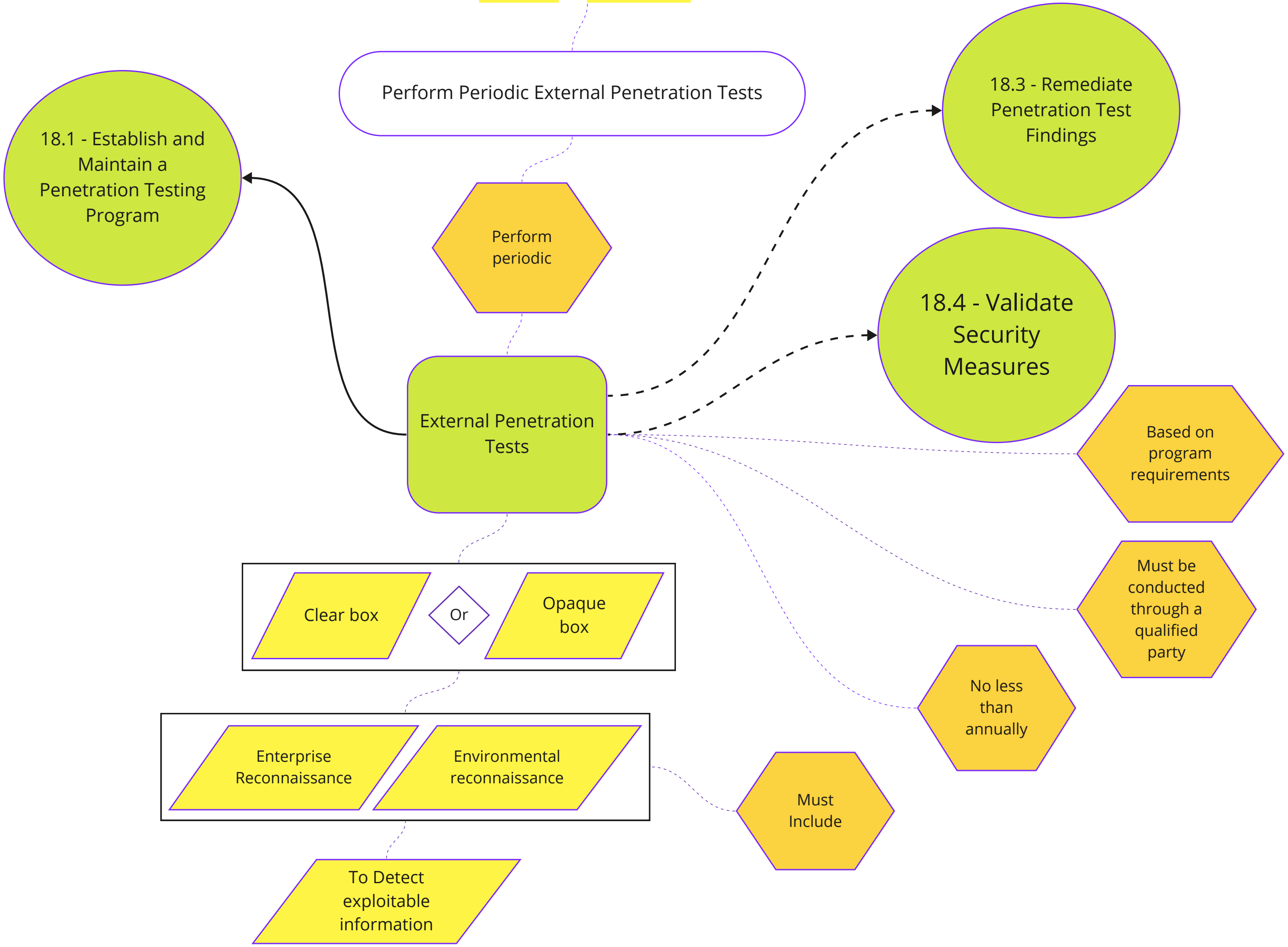
IG2

Identify

Network

Penetration Testing

Penetration Testing Policy / Process



Perform Periodic External Penetration Tests

18.1 - Establish and Maintain a Penetration Testing Program

Perform periodic

18.3 - Remediate Penetration Test Findings

18.4 - Validate Security Measures

External Penetration Tests

Based on program requirements

Must be conducted through a qualified party

No less than annually

Clear box

Or

Opaque box

Enterprise Reconnaissance

Environmental reconnaissance

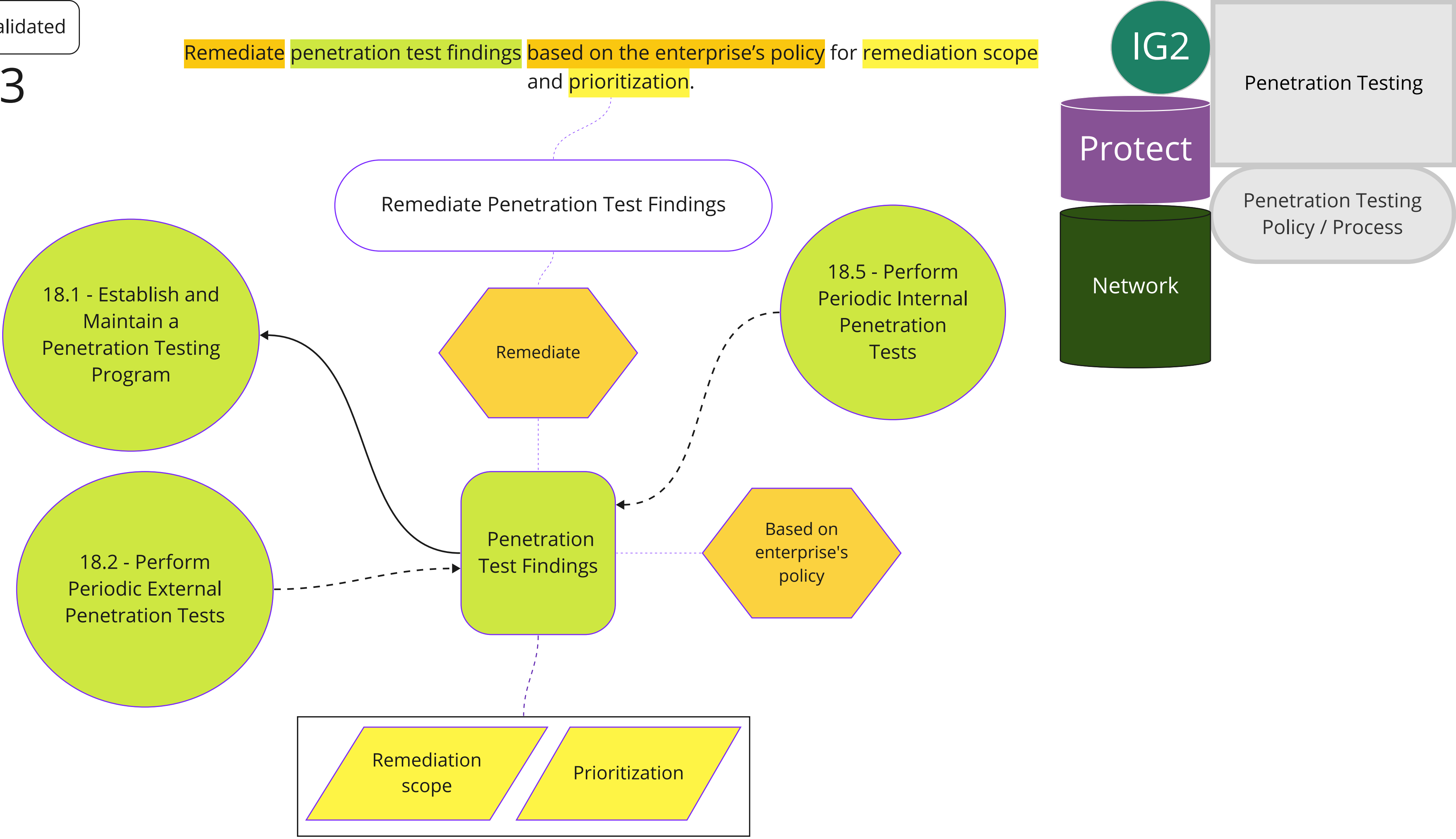
Must Include

To Detect exploitable information

Group Validated

18.3

Remediate penetration test findings based on the enterprise’s policy for remediation scope and prioritization.



IG2

Penetration Testing

Protect

Penetration Testing Policy / Process

Network

Remediate Penetration Test Findings

18.1 - Establish and Maintain a Penetration Testing Program

Remediate

18.5 - Perform Periodic Internal Penetration Tests

Penetration Test Findings

Based on enterprise's policy

18.2 - Perform Periodic External Penetration Tests

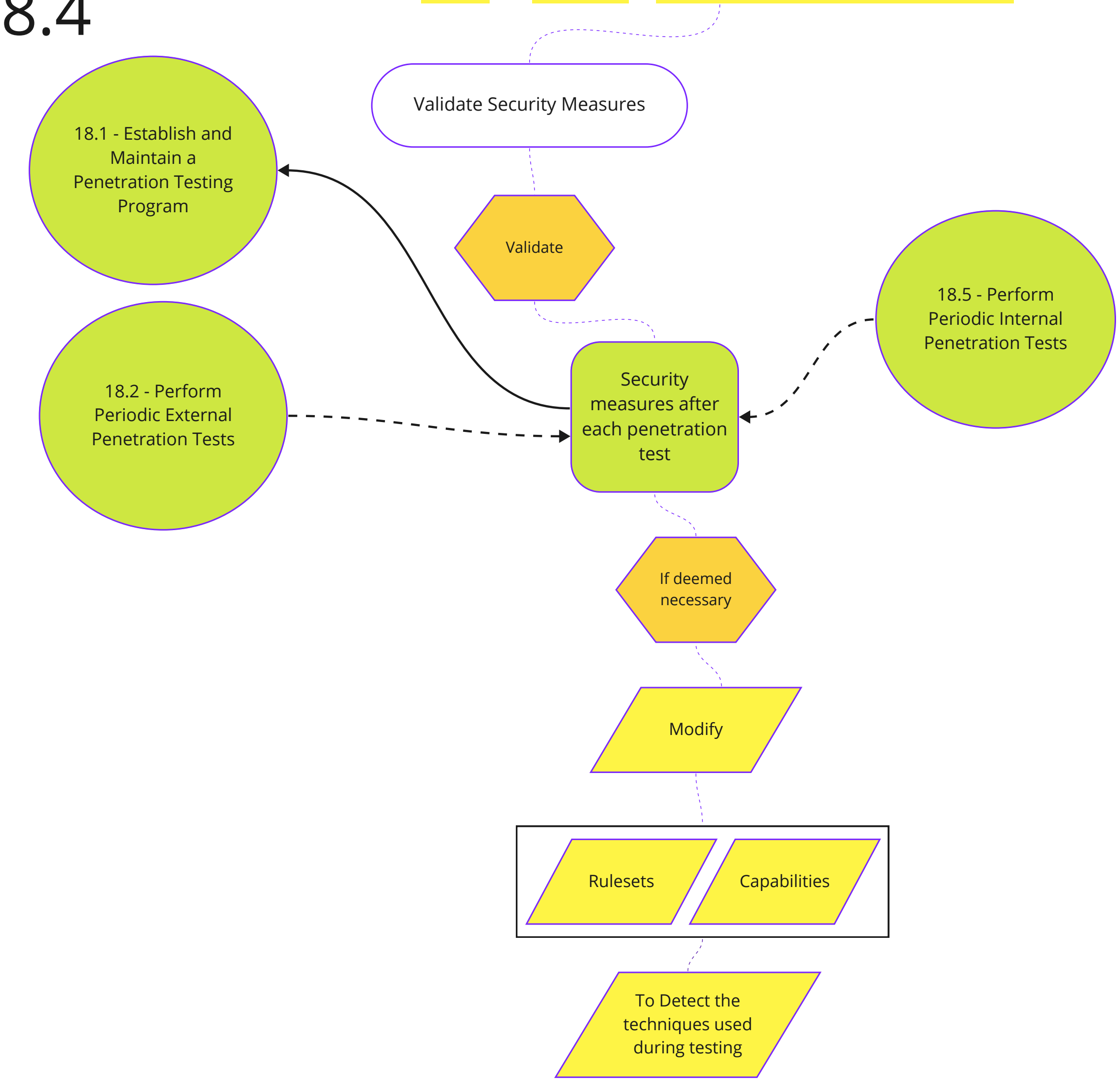
Remediation scope

Prioritization

Group Validated

18.4

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.



Validate Security Measures

Validate

Security measures after each penetration test

18.1 - Establish and Maintain a Penetration Testing Program

18.2 - Perform Periodic External Penetration Tests

18.5 - Perform Periodic Internal Penetration Tests

If deemed necessary

Modify

Rulesets

Capabilities

To Detect the techniques used during testing

Process Oriented Safeguard

IG3

Penetration Testing

Protect

Network

Penetration Testing Policy / Process

Group Validated

18.5

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

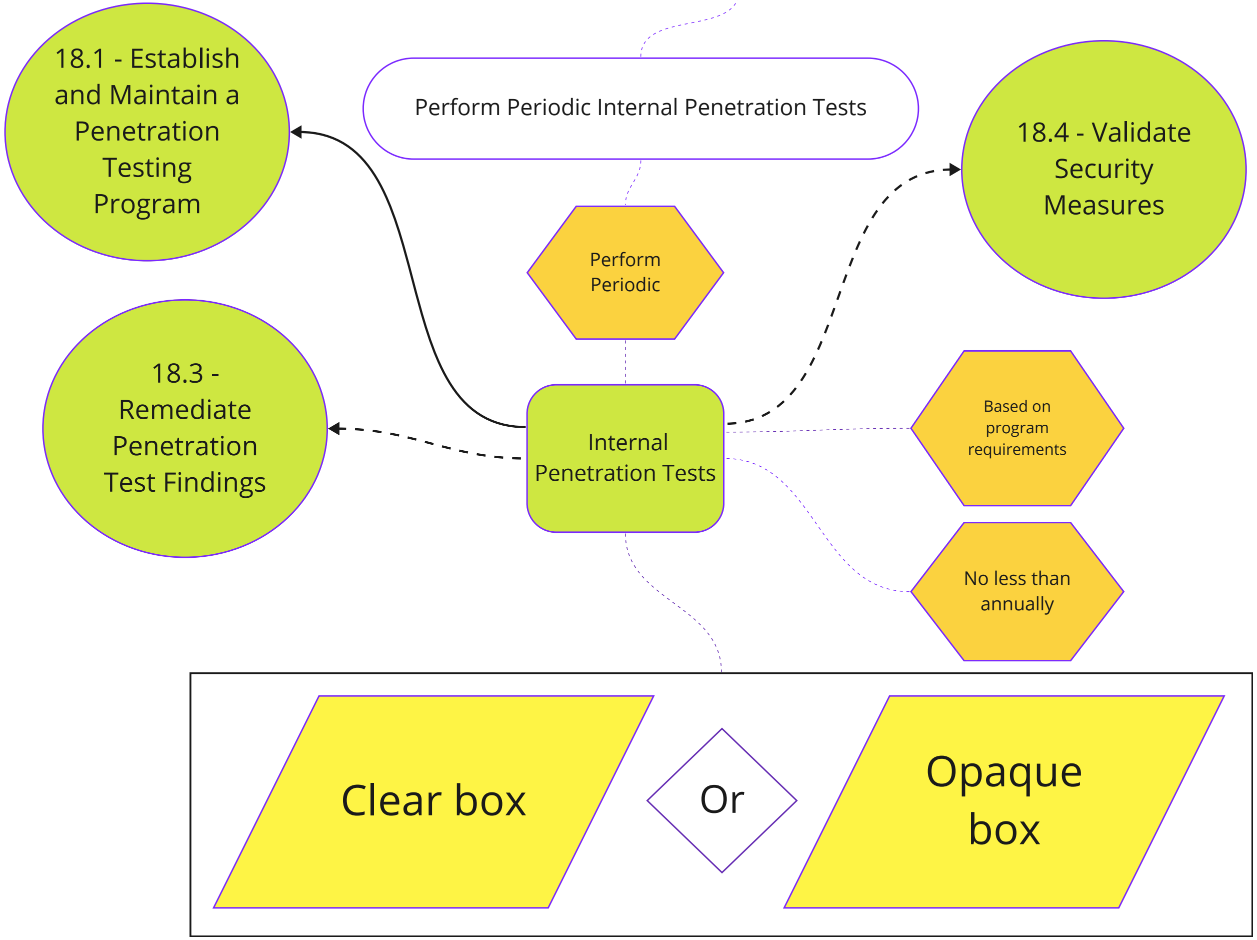
IG3

Identify

N/A

Penetration Testing

Penetration Testing Policy / Process



Perform Periodic Internal Penetration Tests

Perform Periodic

Internal Penetration Tests

18.1 - Establish and Maintain a Penetration Testing Program

18.3 - Remediate Penetration Test Findings

18.4 - Validate Security Measures

Based on program requirements

No less than annually

Clear box

Or

Opaque box