Debug Information

```
DOM Content Loaded, starting initialization...
Debug panel initialized
Tab containers found: IG1=true, IG2=true, IG3=true
Starting to load CIS Controls...
Starting to load CIS Controls...
Fetching cis_controls.json...
Fetch response status: 200
JSON parsed successfully
Found 18 controls
Starting questionnaire initialization...
```

CIS RAM Assessment Questionnaire

Complete this questionnaire to assess your organization's compliance with CIS RAM controls.

Save Draft | Export PDF | Show Edit History

Assessment | Risk Matrix | Reports

IG1 (Basic) | **IG2 (Foundational)** | IG3 (Organizational)

Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/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.

Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, 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.

IG1 IG2 IG3

Requirements:

- [ ] Document all enterprise assets
- [ ] Include network address, hardware address, and machine name
- [ ] Record asset owner and department
- [ ] Track network connection approval status
- [ ] Use MDM tools for mobile devices
- [ ] Maintain accuracy and currency of inventory

Asset Types:

End-User Devices Network Devices Non-Computing/IoT Devices Servers

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 1.2: Address Unauthorized Assets

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

IG1 IG2 IG3

Requirements:

- [ ] Implement weekly unauthorized asset detection
- [ ] Remove unauthorized assets from network
- [ ] Deny remote connection capability
- [ ] Quarantine unauthorized assets
- [ ] Document remediation actions
- [ ] Review and update process regularly

Asset Types:

End-User Devices Network Devices Non-Computing/IoT Devices Servers

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 1.3: Utilize an Active Discovery Tool

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

IG2 IG3

Requirements:

- [ ] Deploy active discovery tools

- [ ] Configure daily or more frequent scanning
- [ ] Cover all network segments
- [ ] Maintain tool updates
- [ ] Document scanning configurations
- [ ] Review and analyze results

Asset Types:

Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging

Use DHCP logging on all DHCP servers or IP address management tools to update enterprise asset inventory. Review and use DHCP logs to update enterprise asset inventory quarterly, or more frequently.

IG2 IG3

Requirements:

- [ ] Enable DHCP logging on all servers
- [ ] Configure IP address management tools
- [ ] Review logs quarterly or more often
- [ ] Update asset inventory based on logs
- [ ] Maintain log retention policy
- [ ] Document review process

Asset Types:

Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 1.5: Use a Passive Asset Discovery Tool

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

IG3

Requirements:

- [ ] Deploy passive discovery tools
- [ ] Configure continuous monitoring
- [ ] Review results weekly or more often
- [ ] Update asset inventory based on findings
- [ ] Compare with active discovery results
- [ ] Document discrepancies and investigate

Asset Types:

Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 2: Inventory and Control of Software Assets

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

Safeguard 2.1: Establish and Maintain a Software Inventory

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the number of installations, versions, and the installation owner.

IG1 IG2 IG3

Requirements:

- [ ] Document all licensed software
- [ ] Record software title and publisher
- [ ] Track install dates and business purpose
- [ ] Monitor number of installations
- [ ] Maintain version information
- [ ] Document installation owners

Asset Types:

Applications Operating Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.2: Ensure Authorized Software is Currently Supported

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance.

IG1 IG2 IG3

Requirements:

- [ ] Verify software support status
- [ ] Remove or upgrade unsupported software
- [ ] Document necessary exceptions
- [ ] Implement mitigating controls
- [ ] Review exceptions periodically
- [ ] Maintain risk acceptance documentation

Asset Types:

Applications Operating Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.3: Address Unauthorized Software

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

IG1 IG2 IG3

Requirements:

- [ ] Detect unauthorized software
- [ ] Remove unauthorized software
- [ ] Document necessary exceptions
- [ ] Review monthly or more frequently
- [ ] Track remediation actions
- [ ] Update software inventory

Asset Types:

Applications Operating Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.4: Utilize Automated Software Inventory Tools

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

IG2 IG3

Requirements:

- [ ] Deploy automated inventory tools
- [ ] Configure automated discovery
- [ ] Document installed software
- [ ] Maintain tool updates
- [ ] Review inventory reports
- [ ] Integrate with asset management

Asset Types:

Applications Operating Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.5: Allowlist Authorized Software

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed.

IG2 IG3

Requirements:

- [ ] Implement application allowlisting
- [ ] Configure execution controls
- [ ] Maintain authorized software list

- [ ] Monitor execution attempts
- [ ] Block unauthorized software
- [ ] Review and update allowlist

Asset Types:

Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.6: Allowlist Authorized Libraries

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process.

IG3

Requirements:

- [ ] Implement library allowlisting
- [ ] Configure library controls
- [ ] Maintain authorized library list
- [ ] Monitor loading attempts
- [ ] Block unauthorized libraries
- [ ] Review and update library controls

Asset Types:

Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 2.7: Allowlist Authorized Scripts

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute.

IG3

Requirements:

- [ ] Implement script allowlisting
- [ ] Use digital signatures
- [ ] Configure version control
- [ ] Monitor script execution
- [ ] Block unauthorized scripts
- [ ] Review and update controls

Asset Types:

Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 3: Data Protection

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

Safeguard 3.1: Establish and Maintain a Data Management Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define data sensitivity levels
- [ ] Identify data owners
- [ ] Document handling procedures
- [ ] Set retention limits
- [ ] Establish disposal requirements
- [ ] Review annually

Asset Types:

Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.2: Establish and Maintain a Data Inventory

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

IG1 IG2 IG3

Requirements:

- [ ] Create data inventory
- [ ] Classify sensitive data
- [ ] Document data locations
- [ ] Track data flows
- [ ] Update inventory annually
- [ ] Prioritize sensitive data

Asset Types:

Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.3: Configure Data Access Control Lists

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

IG1 IG2 IG3

Requirements:

- [ ] Implement access control lists
- [ ] Base access on need-to-know

- [ ] Configure file system permissions
- [ ] Set database access controls
- [ ] Manage application permissions
- [ ] Review access regularly

Asset Types:

Data Applications Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.4: Enforce Data Retention

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

IG1 IG2 IG3

Requirements:

- [ ] Implement retention policies
- [ ] Set minimum retention periods
- [ ] Set maximum retention periods
- [ ] Automate retention enforcement
- [ ] Monitor compliance
- [ ] Document exceptions

Asset Types:

Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.5: Securely Dispose of Data

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

IG1 IG2 IG3

Requirements:

- [ ] Define disposal procedures
- [ ] Match method to sensitivity
- [ ] Document disposal actions
- [ ] Verify secure disposal
- [ ] Train personnel
- [ ] Maintain disposal logs

Asset Types:

Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.6: Encrypt Data on End-User Devices

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

IG1 IG2 IG3

Requirements:

- [ ] Deploy disk encryption
- [ ] Protect encryption keys
- [ ] Verify encryption status
- [ ] Monitor compliance
- [ ] Handle recovery scenarios
- [ ] Document exceptions

Asset Types:

Data End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.7: Establish and Maintain a Data Classification Scheme

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as 'Sensitive,' 'Confidential,' and 'Public,' and classify their data according to those labels.

IG2 IG3

Requirements:

- [ ] Define classification levels
- [ ] Create classification criteria
- [ ] Label data appropriately
- [ ] Document handling requirements
- [ ] Train users on scheme
- [ ] Review and update regularly

Asset Types:

Data Documentation

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.8: Document Data Flows

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process.

IG2 IG3

Requirements:

- [ ] Map data flows
- [ ] Include service providers
- [ ] Document transmission methods
- [ ] Identify data transformations
- [ ] Review flow diagrams
- [ ] Update documentation

Asset Types:

Data Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.9: Encrypt Data on Removable Media

Encrypt data on removable media.

IG2 IG3

Requirements:

- [ ] Implement media encryption
- [ ] Secure encryption keys
- [ ] Verify encryption
- [ ] Control media access
- [ ] Track encrypted media
- [ ] Handle lost media

Asset Types:

Data Removable Media

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.10: Encrypt Sensitive Data in Transit

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

IG2 IG3

Requirements:

- [ ] Identify sensitive data
- [ ] Implement transport encryption
- [ ] Use strong protocols
- [ ] Manage certificates
- [ ] Monitor encryption use
- [ ] Handle encryption failures

Asset Types:

Data Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.11: Encrypt Sensitive Data at Rest

Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data.

IG2 IG3

Requirements:

- [ ] Identify storage locations
- [ ] Implement storage encryption

- [ ] Protect encryption keys
- [ ] Verify encryption
- [ ] Monitor data at rest
- [ ] Handle key rotation

Asset Types:

Data Servers Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity

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

IG3

Requirements:

- [ ] Define sensitivity levels
- [ ] Implement segmentation
- [ ] Configure access controls
- [ ] Monitor data flows
- [ ] Enforce separation
- [ ] Review segmentation

Asset Types:

Data Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.13: Deploy a Data Loss Prevention Solution

Deploy an automated data loss prevention (DLP) solution on enterprise assets, including assets connected to the enterprise network but not owned by the enterprise, where feasible, to alert when unauthorized data leave the enterprise.

IG3

Requirements:

- [ ] Deploy DLP solution
- [ ] Configure alert rules
- [ ] Monitor data transfers
- [ ] Handle violations
- [ ] Update DLP policies
- [ ] Train users on policies

Asset Types:

Data Network End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 3.14: Log Sensitive Data Access

Log sensitive data access, including modification and disposal.

IG3

Requirements:

- [ ] Enable access logging
- [ ] Track modifications
- [ ] Record disposal actions
- [ ] Review access logs
- [ ] Maintain audit trail
- [ ] Alert on violations

Asset Types:

Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 4: Secure Configuration of Enterprise Assets and Software

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

Safeguard 4.1: Establish and Maintain a Secure Configuration Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define baseline configurations
- [ ] Document configuration standards
- [ ] Implement automated enforcement
- [ ] Monitor for deviations
- [ ] Review and update baselines
- [ ] Maintain change control

Asset Types:

End-User Devices Network Devices Servers Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG1 IG2 IG3

Requirements:

- [ ] Define network baselines
- [ ] Document network configurations
- [ ] Secure network protocols
- [ ] Disable unused services
- [ ] Review configurations annually
- [ ] Maintain network documentation

Asset Types:

Network Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets

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

IG1 IG2 IG3

Requirements:

- [ ] Enable automatic locking
- [ ] Set inactivity timeouts
- [ ] Configure mobile device timeouts
- [ ] Enforce screen locks
- [ ] Monitor compliance
- [ ] Handle exceptions

Asset Types:

End-User Devices Servers

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 4.4: Implement and Manage a Firewall on Servers

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

IG1 IG2 IG3

Requirements:

- [ ] Deploy server firewalls
- [ ] Configure rule sets
- [ ] Enable logging
- [ ] Review rules regularly
- [ ] Monitor firewall status
- [ ] Update firewall policies

Asset Types:

Servers

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Implement and manage a host-based firewall on end-user devices, where supported.

IG1 IG2 IG3

Requirements:

- [ ] Deploy endpoint firewalls
- [ ] Configure default deny
- [ ] Define allowed services
- [ ] Enable logging
- [ ] Monitor compliance
- [ ] Update rule sets

Asset Types:

End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 4.6: Securely Manage Enterprise Assets and Software

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS).

IG1 IG2 IG3

Requirements:

- [ ] Use secure protocols
- [ ] Implement access controls
- [ ] Enable secure management
- [ ] Monitor administrative access
- [ ] Document procedures
- [ ] Maintain audit logs

Asset Types:

End-User Devices Network Devices Servers Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software

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

IG1 IG2 IG3

Requirements:

- [ ] Identify default accounts
- [ ] Change default passwords
- [ ] Disable unnecessary accounts
- [ ] Monitor account usage
- [ ] Document exceptions
- [ ] Review regularly

Asset Types:

End-User Devices Network Devices Servers Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Identify unnecessary services
- [ ] Document required services
- [ ] Disable unused services
- [ ] Remove unnecessary software

- [ ] Verify system functionality
- [ ] Monitor for new services

Asset Types:

End-User Devices Servers Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets

Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or filtering all DNS traffic to only use enterprise-approved DNS servers.

IG2 IG3

Requirements:

- [ ] Configure DNS settings
- [ ] Use trusted DNS servers
- [ ] Filter DNS traffic
- [ ] Monitor DNS queries
- [ ] Update DNS configurations
- [ ] Handle DNS failures

Asset Types:

End-User Devices Network Devices Servers

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Configure lockout thresholds
- [ ] Enable automatic lockout
- [ ] Set device-specific limits
- [ ] Monitor failed attempts
- [ ] Implement recovery process
- [ ] Document exceptions

Asset Types:

End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Enforce remote wipe capability on portable end-user devices, where supported. Example implementations include Microsoft InTune Wipe and Apple Device Management Lost Mode.

IG2 IG3

Requirements:

- [ ] Enable remote wipe
- [ ] Configure MDM solutions
- [ ] Test wipe capability
- [ ] Document procedures
- [ ] Train IT staff
- [ ] Maintain audit logs

Asset Types:

End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Separate enterprise workspaces from personal workspaces on mobile end-user devices, where supported. Example implementations include using an enterprise mobility management (EMM) or mobile device management (MDM) solution.

IG2 IG3

Requirements:

- [ ] Implement workspace separation
- [ ] Configure containerization
- [ ] Enforce data segregation
- [ ] Monitor compliance
- [ ] Update policies
- [ ] Train users

Asset Types:

End-User Devices

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 5: Account Management

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

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

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

IG1 IG2 IG3

Requirements:

- [ ] Create account inventory
- [ ] Include user and admin accounts
- [ ] Record account metadata
- [ ] Validate quarterly
- [ ] Document authorization
- [ ] Maintain accuracy

Asset Types:

Users Accounts

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 5.2: Use Unique Passwords

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

IG1 IG2 IG3

Requirements:

- [ ] Enforce password length
- [ ] Implement complexity rules
- [ ] Enable MFA where possible
- [ ] Prevent password reuse
- [ ] Monitor compliance
- [ ] Train users

Asset Types:

Users Accounts

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 5.3: Disable Dormant Accounts

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

IG1 IG2 IG3

Requirements:

- [ ] Monitor account activity
- [ ] Identify dormant accounts
- [ ] Disable after 45 days
- [ ] Document exceptions
- [ ] Review regularly
- [ ] Maintain audit logs

Asset Types:

Users Accounts

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

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

IG1 IG2 IG3

Requirements:

- [ ] Separate admin accounts
- [ ] Limit privileged access
- [ ] Monitor admin usage
- [ ] Enforce separation
- [ ] Document procedures
- [ ] Review regularly

Asset Types:

Users Accounts Administrators

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts

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

IG2 IG3

Requirements:

- [ ] Create service account inventory
- [ ] Document ownership
- [ ] Review quarterly
- [ ] Validate authorization
- [ ] Track purpose
- [ ] Maintain documentation

Asset Types:

Service Accounts

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 5.6: Centralize Account Management

Centralize account management through a directory or identity service.

IG2 IG3

Requirements:

- [ ] Implement directory service
- [ ] Centralize authentication
- [ ] Manage access centrally
- [ ] Synchronize accounts
- [ ] Monitor directory health
- [ ] Maintain backups

Asset Types:

Users Accounts Directory Services

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 6: Access Control Management

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

Safeguard 6.1: Establish an Access Granting Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define access request process
- [ ] Implement approval workflow
- [ ] Automate access granting
- [ ] Document decisions
- [ ] Maintain audit trail
- [ ] Review periodically

Asset Types:

Users Access Control

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.2: Establish an Access Revoking Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define revocation process
- [ ] Implement immediate disable

- [ ] Automate access removal
- [ ] Preserve audit trails
- [ ] Verify access removal
- [ ] Document actions

Asset Types:

Users Access Control

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.3: Require MFA for Externally-Exposed Applications

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

IG1 IG2 IG3

Requirements:

- [ ] Identify external applications
- [ ] Enable MFA support
- [ ] Configure SSO integration
- [ ] Monitor MFA usage
- [ ] Handle exceptions
- [ ] Review compliance

Asset Types:

Applications Authentication

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.4: Require MFA for Remote Network Access

Require MFA for remote network access.

IG1 IG2 IG3

Requirements:

- [ ] Configure VPN MFA
- [ ] Enable remote MFA
- [ ] Monitor remote access
- [ ] Log authentication attempts
- [ ] Review access logs
- [ ] Handle failures

Asset Types:

Network Authentication

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.5: Require MFA for Administrative Access

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

IG1 IG2 IG3

Requirements:

- [ ] Enable admin MFA
- [ ] Configure all assets
- [ ] Include third-party systems
- [ ] Monitor admin access
- [ ] Review compliance
- [ ] Document exceptions

Asset Types:

Administrators Authentication

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Document auth systems

- [ ] Include remote providers
- [ ] Review annually
- [ ] Update inventory
- [ ] Track changes
- [ ] Maintain documentation

Asset Types:

Authentication Authorization

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.7: Centralize Access Control

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

IG2 IG3

Requirements:

- [ ] Implement central directory
- [ ] Configure SSO
- [ ] Integrate applications
- [ ] Monitor service health
- [ ] Maintain backups
- [ ] Document architecture

Asset Types:

Authentication Authorization

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 6.8: Define and Maintain Role-Based Access Control

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

IG2 IG3

Requirements:

- [ ] Define access roles
- [ ] Document permissions
- [ ] Review annually
- [ ] Update as needed
- [ ] Maintain documentation
- [ ] Verify compliance

Asset Types:

Access Control Authorization

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 7: Continuous Vulnerability Management

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

Safeguard 7.1: Establish and Maintain a Vulnerability Management Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define vulnerability process
- [ ] Document procedures
- [ ] Establish timelines
- [ ] Review annually
- [ ] Update as needed
- [ ] Train personnel

Asset Types:

Applications Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 7.2: Establish and Maintain a Remediation Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define remediation strategy
- [ ] Prioritize vulnerabilities
- [ ] Set timelines
- [ ] Review monthly
- [ ] Track progress
- [ ] Document exceptions

Asset Types:

Applications Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 7.3: Perform Automated Operating System Patch Management

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

IG1 IG2 IG3

Requirements:

- [ ] Deploy patch management
- [ ] Automate OS updates
- [ ] Schedule monthly
- [ ] Monitor compliance
- [ ] Handle failures
- [ ] Document exceptions

Asset Types:

Operating Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 7.4: Perform Automated Application Patch Management

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

IG1 IG2 IG3

Requirements:

- [ ] Deploy patch management
- [ ] Automate app updates
- [ ] Schedule monthly

- [ ] Monitor compliance
- [ ] Handle failures
- [ ] Document exceptions

Asset Types:

Applications

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

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

IG2 IG3

Requirements:

- [ ] Deploy scanning tools
- [ ] Configure authentication
- [ ] Schedule quarterly
- [ ] Use SCAP compliance
- [ ] Review results
- [ ] Track remediation

Asset Types:

Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Deploy external scanners
- [ ] Schedule monthly
- [ ] Use SCAP compliance
- [ ] Monitor exposure
- [ ] Review results
- [ ] Track remediation

Asset Types:

Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 7.7: Remediate Detected Vulnerabilities

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

IG2 IG3

Requirements:

- [ ] Follow remediation process
- [ ] Address monthly
- [ ] Prioritize fixes
- [ ] Verify remediation
- [ ] Document actions
- [ ] Track metrics

Asset Types:

Applications Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 8: Audit Log Management

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

Safeguard 8.1: Establish and Maintain an Audit Log Management Process

Establish and maintain an audit log management process that defines the enterprise's logging requirements. This process should specify the types of systems and applications that should log, log level requirements, and the required retention duration for each log type. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

IG1 IG2 IG3

Requirements:

- [ ] Define logging requirements
- [ ] Specify retention periods
- [ ] Document log levels
- [ ] Review annually
- [ ] Update process
- [ ] Train personnel

Asset Types:

Logs Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.2: Collect Audit Logs

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

IG1 IG2 IG3

Requirements:

- [ ] Enable system logging
- [ ] Configure log collection
- [ ] Verify logging status
- [ ] Monitor collection
- [ ] Handle failures
- [ ] Document exceptions

Asset Types:

Logs Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.3: Ensure Adequate Audit Log Storage

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

IG1 IG2 IG3

Requirements:

- [ ] Calculate storage needs
- [ ] Allocate space
- [ ] Monitor usage

- [ ] Configure retention
- [ ] Handle capacity issues
- [ ] Archive as needed

Asset Types:

Logs Storage

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.4: Standardize Time Synchronization

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

IG1 IG2 IG3

Requirements:

- [ ] Configure NTP servers
- [ ] Synchronize time sources
- [ ] Monitor drift
- [ ] Handle failures
- [ ] Document configuration
- [ ] Verify compliance

Asset Types:

Systems Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.5: Collect Detailed Audit Logs

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

IG2 IG3

Requirements:

- [ ] Enable detailed logging
- [ ] Include required fields
- [ ] Configure sources
- [ ] Monitor collection
- [ ] Protect log data
- [ ] Review regularly

Asset Types:

Logs Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.6: Collect DNS Query Audit Logs

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

IG2 IG3

Requirements:

- [ ] Enable DNS logging
- [ ] Configure collection
- [ ] Store securely
- [ ] Review regularly
- [ ] Monitor queries
- [ ] Alert on anomalies

Asset Types:

DNS Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.7: Collect URL Request Audit Logs

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

IG2 IG3

Requirements:

- [ ] Enable URL logging
- [ ] Configure proxies
- [ ] Store securely

- [ ] Review regularly
- [ ] Monitor requests
- [ ] Alert on violations

Asset Types:

Web Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.8: Collect Command-Line Audit Logs

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

IG2 IG3

Requirements:

- [ ] Enable command logging
- [ ] Configure shells
- [ ] Store securely
- [ ] Review regularly
- [ ] Monitor commands
- [ ] Alert on suspicious

Asset Types:

Systems Shells

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.9: Centralize Audit Logs

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

IG2 IG3

Requirements:

- [ ] Deploy central logging
- [ ] Configure forwarding
- [ ] Ensure delivery
- [ ] Monitor collection
- [ ] Protect transport
- [ ] Verify integrity

Asset Types:

Logs Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.10: Retain Audit Logs

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

IG2 IG3

Requirements:

- [ ] Configure retention
- [ ] Maintain 90 days
- [ ] Protect storage
- [ ] Archive older logs
- [ ] Monitor space
- [ ] Handle capacity

Asset Types:

Logs Storage

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.11: Conduct Audit Log Reviews

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

IG3

Requirements:

- [ ] Schedule reviews
- [ ] Define anomalies
- [ ] Document findings
- [ ] Investigate alerts
- [ ] Track resolution

- [ ] Update processes

Asset Types:

Logs Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 8.12: Collect Service Provider Logs

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

IG3

Requirements:

- [ ] Identify providers
- [ ] Enable logging
- [ ] Configure collection
- [ ] Monitor events
- [ ] Review regularly
- [ ] Store securely

Asset Types:

Logs Services

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 9: Email and Web Browser Protections

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

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

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

IG1 IG2 IG3

Requirements:

- [ ] Inventory browsers/clients
- [ ] Verify vendor support
- [ ] Update automatically
- [ ] Remove unsupported
- [ ] Monitor compliance
- [ ] Document exceptions

Asset Types:

Applications Browsers Email

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 9.2: Use DNS Filtering Services

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

IG1 IG2 IG3

Requirements:

- [ ] Implement DNS filtering
- [ ] Update block lists
- [ ] Monitor requests
- [ ] Handle exceptions
- [ ] Review logs
- [ ] Document policies

Asset Types:

DNS Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 9.3: Maintain and Enforce Network-Based URL Filters

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

IG1 IG2 IG3

Requirements:

- [ ] Deploy URL filtering
- [ ] Update categories
- [ ] Maintain block lists
- [ ] Monitor access
- [ ] Handle exceptions
- [ ] Review effectiveness

Asset Types:

Web Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Restrict unauthorized browser and email client extensions/add-ons/plugins.

IG2 IG3

Requirements:

- [ ] Inventory extensions
- [ ] Approve additions

- [ ] Remove unauthorized
- [ ] Monitor usage
- [ ] Update policies
- [ ] Document exceptions

Asset Types:

Browsers Email

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 9.5: Implement DMARC

Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to prevent spoofing and validate email.

IG2 IG3

Requirements:

- [ ] Configure DMARC
- [ ] Set up SPF
- [ ] Enable DKIM
- [ ] Monitor reports
- [ ] Adjust policies
- [ ] Handle failures

Asset Types:

Email DNS

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 9.6: Block Unnecessary File Types

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

IG2 IG3

Requirements:

- [ ] Define blocked types
- [ ] Configure gateway
- [ ] Monitor attempts
- [ ] Handle exceptions
- [ ] Update policies
- [ ] Document rules

Asset Types:

Email Gateway

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Install anti-malware
- [ ] Configure scanning
- [ ] Enable sandboxing
- [ ] Update signatures
- [ ] Monitor alerts
- [ ] Handle incidents

Asset Types:

Email Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 10: Malware Defenses

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

Safeguard 10.1: Deploy and Maintain Anti-Malware Software

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

IG1 IG2 IG3

Requirements:

- [ ] Install anti-malware
- [ ] Configure real-time
- [ ] Update signatures
- [ ] Enable scanning
- [ ] Monitor status
- [ ] Handle alerts

Asset Types:

Applications Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates

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

IG1 IG2 IG3

Requirements:

- [ ] Enable auto-updates
- [ ] Verify settings
- [ ] Monitor updates
- [ ] Handle failures

- [ ] Document exceptions
- [ ] Review compliance

Asset Types:

Applications Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 10.3: Disable Autorun and Autoplay for Removable Media

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

IG1 IG2 IG3

Requirements:

- [ ] Disable autorun
- [ ] Disable autoplay
- [ ] Configure policies
- [ ] Monitor compliance
- [ ] Handle exceptions
- [ ] Document settings

Asset Types:

Systems Media

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Configure anti-malware software to automatically scan removable media.

IG2 IG3

Requirements:

- [ ] Enable auto-scan
- [ ] Configure policies
- [ ] Monitor scanning
- [ ] Handle alerts
- [ ] Document exceptions
- [ ] Review logs

Asset Types:

Applications Media

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 10.5: Enable Anti-Exploitation Features

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

IG2 IG3

Requirements:

- [ ] Enable DEP/ASLR
- [ ] Configure WDEG
- [ ] Enable SIP
- [ ] Monitor status
- [ ] Handle alerts
- [ ] Document settings

Asset Types:

Systems Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 10.6: Centrally Manage Anti-Malware Software

Centrally manage anti-malware software.

IG2 IG3

Requirements:

- [ ] Deploy central console
- [ ] Configure policies
- [ ] Monitor agents

- [ ] Handle alerts
- [ ] Update settings
- [ ] Document management

Asset Types:

Applications Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 10.7: Use Behavior-Based Anti-Malware Software

Use behavior-based anti-malware software.

IG3

Requirements:

- [ ] Deploy behavior analysis
- [ ] Configure policies
- [ ] Monitor alerts
- [ ] Handle incidents
- [ ] Update rules
- [ ] Document responses

Asset Types:

Applications Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 11: Data Recovery

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

Safeguard 11.1: Establish and Maintain a Data Recovery Process

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

IG1 IG2 IG3

Requirements:

- [ ] Define recovery scope
- [ ] Set priorities
- [ ] Document procedures
- [ ] Review annually
- [ ] Test process
- [ ] Update as needed

Asset Types:

Data Recovery

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 11.2: Perform Automated Backups

Perform automated backups of in-scope enterprise assets. Run backups on both a daily and weekly basis.

IG1 IG2 IG3

Requirements:

- [ ] Configure automation
- [ ] Schedule backups
- [ ] Verify completion
- [ ] Monitor storage
- [ ] Test restores
- [ ] Document failures

Asset Types:

Data Backups

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 11.3: Protect Recovery Data

Protect recovery data. Example implementations include storing data in a secure, encrypted, and immutable format, and limiting access to recovery data to authorized users only.

IG1 IG2 IG3

Requirements:

- [ ] Encrypt backups
- [ ] Restrict access
- [ ] Secure storage
- [ ] Monitor integrity
- [ ] Verify protection
- [ ] Document controls

Asset Types:

Data Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Create isolation

- [ ] Configure replication
- [ ] Monitor status
- [ ] Test isolation
- [ ] Verify access
- [ ] Document architecture

Asset Types:

Data Recovery

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 11.5: Test Data Recovery

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

IG2 IG3

Requirements:

- [ ] Schedule tests
- [ ] Select samples
- [ ] Perform recovery
- [ ] Document results
- [ ] Address issues
- [ ] Update procedures

Asset Types:

Data Recovery

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 12: Network Infrastructure Management

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

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

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

IG1 IG2 IG3

Requirements:

- [ ] Track versions
- [ ] Monitor support
- [ ] Schedule updates
- [ ] Test changes
- [ ] Document versions
- [ ] Review monthly

Asset Types:

Network Infrastructure

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 12.2: Establish and Maintain a Secure Network Architecture

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

IG2 IG3

Requirements:

- [ ] Design segmentation
- [ ] Implement zones
- [ ] Configure access
- [ ] Document design
- [ ] Review annually
- [ ] Update as needed

Asset Types:

Network Architecture

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 12.3: Securely Manage Network Infrastructure

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

IG2 IG3

Requirements:

- [ ] Use secure protocols
- [ ] Implement automation
- [ ] Control changes
- [ ] Monitor access
- [ ] Review logs
- [ ] Document procedures

Asset Types:

Network Infrastructure

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

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

IG2 IG3

Requirements:

- [ ] Create diagrams
- [ ] Document systems
- [ ] Review annually
- [ ] Update changes
- [ ] Maintain versions
- [ ] Control access

Asset Types:

Network Documentation

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Centralize network authentication, authorization, and auditing (AAA) management.

IG2 IG3

Requirements:

- [ ] Deploy AAA system
- [ ] Configure policies
- [ ] Monitor access
- [ ] Review logs
- [ ] Handle incidents
- [ ] Document controls

Asset Types:

Network Authentication

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 12.6: Use of Secure Network Management and Communication Protocols

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 3 (WPA3)).

IG2 IG3

Requirements:

- [ ] Configure 802.1X
- [ ] Enable WPA3
- [ ] Secure protocols
- [ ] Monitor compliance
- [ ] Handle exceptions
- [ ] Document settings

Asset Types:

Network Protocols

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG2 IG3

Requirements:

- [ ] Configure VPN
- [ ] Enable AAA
- [ ] Monitor access
- [ ] Review logs
- [ ] Handle incidents
- [ ] Document policies

Asset Types:

Network VPN

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG3

Requirements:

- [ ] Create admin network
- [ ] Isolate resources
- [ ] Restrict access
- [ ] Monitor usage
- [ ] Document setup
- [ ] Review security

Asset Types:

Network Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 13: Network Monitoring and Defense

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

Safeguard 13.1: Centralize Security Event Alerting

Centralize security event alerting across enterprise assets for collection, correlation, and analysis. Security event alerting should be coordinated with collection, processing, and escalation workflows.

IG1 IG2 IG3

Requirements:

- [ ] Deploy SIEM
- [ ] Configure alerts
- [ ] Correlate events
- [ ] Define workflows
- [ ] Monitor system
- [ ] Document procedures

Asset Types:

Security Monitoring

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution

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

IG2 IG3

Requirements:

- [ ] Install HIDS

- [ ] Configure rules
- [ ] Monitor alerts
- [ ] Update signatures
- [ ] Handle incidents
- [ ] Document deployment

Asset Types:

Security Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.3: Deploy a Network Intrusion Detection Solution

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

IG2 IG3

Requirements:

- [ ] Deploy NIDS
- [ ] Configure sensors
- [ ] Monitor traffic
- [ ] Update signatures
- [ ] Handle alerts
- [ ] Document setup

Asset Types:

Security Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.4: Perform Traffic Filtering Between Network Segments

Perform traffic filtering between network segments, where appropriate.

IG2 IG3

Requirements:

- [ ] Define segments
- [ ] Configure filters
- [ ] Monitor traffic
- [ ] Review rules
- [ ] Handle violations
- [ ] Document policies

Asset Types:

Network Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.5: Manage Access Control for Remote Assets

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

IG2 IG3

Requirements:

- [ ] Define policies
- [ ] Check compliance
- [ ] Verify updates
- [ ] Monitor access
- [ ] Handle exceptions
- [ ] Document controls

Asset Types:

Remote Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.6: Collect Network Traffic Flow Data

Collect network traffic flow data. Example implementations include Protocol Independent Flow Information Export (IPFIX) or NetFlow protocol, where appropriate.

IG2 IG3

Requirements:

- [ ] Configure NetFlow
- [ ] Collect data
- [ ] Store flows
- [ ] Analyze traffic
- [ ] Monitor patterns
- [ ] Document collection

Asset Types:

Network Monitoring

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.7: Deploy a Network Intrusion Prevention Solution

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

IG3

Requirements:

- [ ] Deploy NIPS
- [ ] Configure rules
- [ ] Monitor traffic
- [ ] Block threats
- [ ] Handle alerts
- [ ] Document deployment

Asset Types:

Security Network

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.8: Deploy a Host-Based Intrusion Prevention Solution

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

IG3

Requirements:

- [ ] Install HIPS
- [ ] Configure EDR
- [ ] Monitor hosts
- [ ] Block threats
- [ ] Handle alerts
- [ ] Document setup

Asset Types:

Security Systems

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.9: Deploy Port-Level Access Control

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

IG3

Requirements:

- [ ] Configure 802.1x
- [ ] Deploy NAC
- [ ] Manage certificates
- [ ] Monitor access
- [ ] Handle failures
- [ ] Document controls

Asset Types:

Network Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.10: Perform Application Layer Filtering

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

IG3

Requirements:

- [ ] Deploy proxy
- [ ] Configure filtering
- [ ] Monitor traffic
- [ ] Update rules
- [ ] Handle violations
- [ ] Document policies

Asset Types:

Network Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 13.11: Tune Security Event Alerting Thresholds

Tune security event alerting thresholds monthly, or more frequently.

IG3

Requirements:

- [ ] Review alerts
- [ ] Adjust thresholds
- [ ] Monitor effectiveness
- [ ] Document changes

- [ ] Handle false positives
- [ ] Update monthly

Asset Types:

Security Monitoring

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 14: Security Awareness and Skills Training

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

Safeguard 14.1: Establish and Maintain a Security Awareness Program

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

IG1 IG2 IG3

Requirements:

- [ ] Define program
- [ ] Create content
- [ ] Schedule training

- [ ] Track completion
- [ ] Update annually
- [ ] Document program

Asset Types:

Users Training

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks

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

IG1 IG2 IG3

Requirements:

- [ ] Create materials
- [ ] Conduct training
- [ ] Test knowledge
- [ ] Track results
- [ ] Update content
- [ ] Document progress

Asset Types:

Users Training

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.3: Train Workforce Members on Authentication Best Practices

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

IG1 IG2 IG3

Requirements:

- [ ] Develop content
- [ ] Train staff
- [ ] Test understanding
- [ ] Monitor compliance
- [ ] Update materials
- [ ] Document training

Asset Types:

Users Authentication

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.4: Train Workforce on Data Handling Best Practices

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices.

IG1 IG2 IG3

Requirements:

- [ ] Create guidelines
- [ ] Train employees
- [ ] Test knowledge
- [ ] Monitor practices
- [ ] Update content
- [ ] Document procedures

Asset Types:

Users Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

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

IG1 IG2 IG3

Requirements:

- [ ] Identify risks

- [ ] Create training
- [ ] Conduct sessions
- [ ] Test awareness
- [ ] Update materials
- [ ] Document incidents

Asset Types:

Users Data

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.6: Train Workforce Members on Cybersecurity Responsibilities

Train workforce members on their cybersecurity responsibilities and related policies, procedures, and agreements. Example responsibilities include acceptable use, access control, password management, and handling of sensitive data. Conduct training at hire and, at a minimum, annually.

IG1 IG2 IG3

Requirements:

- [ ] Define roles
- [ ] Create training
- [ ] Conduct annually
- [ ] Test compliance
- [ ] Update content
- [ ] Document completion

Asset Types:

Users Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.7: Train Workforce Members to Recognize and Report Security Incidents

Train workforce members to recognize potential security incidents and how to report such incidents.

IG1 IG2 IG3

Requirements:

- [ ] Define incidents
- [ ] Create procedures
- [ ] Train staff
- [ ] Test reporting
- [ ] Update process
- [ ] Document incidents

Asset Types:

Users Incidents

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.8: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

IG2 IG3

Requirements:

- [ ] Create guidance
- [ ] Train users
- [ ] Test knowledge
- [ ] Monitor reports
- [ ] Update procedures
- [ ] Document issues

Asset Types:

Users Updates

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 14.9: Conduct Role-Specific Security Awareness and Skills Training

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP Top 10 vulnerability awareness and prevention training for web developers, and advanced social engineering awareness for high-profile roles.

IG2 IG3

Requirements:

- [ ] Identify roles
- [ ] Design training
- [ ] Conduct sessions
- [ ] Test skills
- [ ] Update content
- [ ] Document progress

Asset Types:

Users Training

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these

providers are protecting those platforms and data appropriately.

Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

Establish and maintain an inventory of service providers. The inventory should include the enterprise's assessment of risk for each service provider, and various compliance requirements or other regulations that apply to each service provider.

IG1 IG2 IG3

Requirements:

- [ ] Create inventory
- [ ] Assess risks
- [ ] Document compliance
- [ ] Review regularly
- [ ] Update changes
- [ ] Maintain records

Asset Types:

Vendors Services

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and

decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

IG2 IG3

Requirements:

- [ ] Define policy
- [ ] Set standards
- [ ] Review annually
- [ ] Update changes
- [ ] Document procedures
- [ ] Train staff

Asset Types:

Vendors Policies

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.3: Classify Service Providers

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk.

IG2 IG3

Requirements:

- [ ] Define criteria
- [ ] Assess providers

- [ ] Assign levels
- [ ] Document decisions
- [ ] Review regularly
- [ ] Update classifications

Asset Types:

Vendors Risk

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.4: Ensure Service Provider Contracts Include Security Requirements

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. Include security requirements in request for proposals.

IG2 IG3

Requirements:

- [ ] Define requirements
- [ ] Update contracts
- [ ] Review compliance
- [ ] Monitor adherence
- [ ] Document changes
- [ ] Handle violations

Asset Types:

Vendors Contracts

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.5: Assess Service Providers

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes.

IG2 IG3

Requirements:

- [ ] Define assessments
- [ ] Review reports
- [ ] Evaluate compliance
- [ ] Document findings
- [ ] Track remediation
- [ ] Update records

Asset Types:

Vendors Compliance

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.6: Monitor Service Providers

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

IG2 IG3

Requirements:

- [ ] Define monitoring
- [ ] Track compliance
- [ ] Review changes
- [ ] Assess risks
- [ ] Document issues
- [ ] Handle incidents

Asset Types:

Vendors Monitoring

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 15.7: Securely Decommission Service Providers

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

IG2 IG3

Requirements:

- [ ] Define process
- [ ] Remove access
- [ ] Recover data
- [ ] Verify completion
- [ ] Document actions
- [ ] Update inventory

Asset Types:

Vendors Decommissioning

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 16: Application Software Security

Manage the security life cycle of all in-house developed and acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Safeguard 16.1: Establish and Maintain a Secure Application Development Process

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

IG1 IG2 IG3

Requirements:

- [ ] Define process
- [ ] Document standards
- [ ] Train developers
- [ ] Review code
- [ ] Test security
- [ ] Update annually

Asset Types:

Applications Development

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy, a process for validating and triaging vulnerability reports, a process for tracking

remediation, and a method for communicating the status of identified vulnerabilities to stakeholders.

IG1 IG2 IG3

Requirements:

- [ ] Create process
- [ ] Handle reports
- [ ] Validate issues
- [ ] Track fixes
- [ ] Communicate status
- [ ] Document procedures

Asset Types:

Applications Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.3: Perform Root Cause Analysis on Security Vulnerabilities

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis should be performed to ensure adequate corrective actions are taken to prevent reoccurrence of similar vulnerabilities.

IG1 IG2 IG3

Requirements:

- [ ] Analyze vulnerabilities
- [ ] Identify causes

- [ ] Document findings
- [ ] Implement fixes
- [ ] Prevent recurrence
- [ ] Track progress

Asset Types:

Applications Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Establish and manage an updated inventory of third-party components used in development, often referred to as a 'bill of materials,' as well as components slated for future use. This inventory should include any risks that each third-party component could pose to the enterprise's security posture.

IG2 IG3

Requirements:

- [ ] Create inventory
- [ ] Track components
- [ ] Assess risks
- [ ] Monitor updates
- [ ] Document dependencies
- [ ] Update regularly

Asset Types:

Applications Components

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Use up-to-date and trusted third-party software components. Example implementations include using current versions of third-party libraries, frameworks, and software development kits (SDKs), as well as validating the authenticity of the components through digital signatures or other mechanisms.

IG2 IG3

Requirements:

- [ ] Verify versions
- [ ] Check signatures
- [ ] Update components
- [ ] Monitor alerts
- [ ] Document changes
- [ ] Handle vulnerabilities

Asset Types:

Applications Components

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

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

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process should include setting timelines for addressing vulnerabilities based on their severity, as well as a process for tracking identified vulnerabilities and their remediation status.

IG2 IG3

Requirements:

- [ ] Define ratings
- [ ] Set priorities
- [ ] Track remediation
- [ ] Monitor progress
- [ ] Update process
- [ ] Document decisions

Asset Types:

Applications Security

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.7: Use Standard Hardening Configuration Templates for Application Infrastructure

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

IG2 IG3

Requirements:

- [ ] Define templates
- [ ] Apply hardening
- [ ] Test configurations
- [ ] Monitor compliance
- [ ] Document exceptions
- [ ] Review regularly

Asset Types:

Applications Infrastructure

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.8: Separate Production and Non-Production Systems

Maintain separate environments for production and non-production systems.

IG2 IG3

Requirements:

- [ ] Define environments
- [ ] Isolate systems
- [ ] Control access
- [ ] Manage data
- [ ] Document setup
- [ ] Monitor separation

Asset Types:

Applications Infrastructure

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.9: Train Developers in Application Security Concepts and Secure Coding

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training should be based on the organization's secure coding standards, security requirements, and common vulnerabilities.

IG2 IG3

Requirements:

- [ ] Design training
- [ ] Train developers
- [ ] Test knowledge
- [ ] Update content
- [ ] Track completion

- [ ] Document progress

Asset Types:

Applications Training

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.10: Apply Secure Design Principles in Application Architectures

Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of 'never trust user input.' Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

IG2 IG3

Requirements:

- [ ] Define principles
- [ ] Review designs
- [ ] Validate input
- [ ] Implement controls
- [ ] Document architecture
- [ ] Test security

Asset Types:

Applications Architecture

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.11: Leverage Vetted Modules or Services for Application Security Components

Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms.

IG2 IG3

Requirements:

- [ ] Identify components
- [ ] Evaluate options
- [ ] Select modules
- [ ] Implement properly
- [ ] Monitor usage
- [ ] Update as needed

Asset Types:

Applications Components

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 16.12: Implement Code-Level Security Checks

Implement code-level security checks, including peer review, static analysis, and dynamic analysis. Code-level security checks should be integrated into the deployment process.

IG3

Requirements:

- [ ] Configure checks
- [ ] Review code
- [ ] Run analysis
- [ ] Fix issues
- [ ] Document findings
- [ ] Track metrics

Asset Types:

Applications Code

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Safeguard 17.1: Designate Personnel to Manage Incident Handling

Designate one or more people to be responsible for incident handling. These personnel should be skilled in incident response and should be prepared to handle incidents at any time.

IG1 IG2 IG3

Requirements:

- [ ] Assign roles
- [ ] Define responsibilities
- [ ] Train personnel
- [ ] Establish schedules
- [ ] Document procedures
- [ ] Maintain readiness

Asset Types:

Personnel Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Review and update contact information annually, or when significant enterprise changes occur that could impact this Safeguard.

IG1 IG2 IG3

Requirements:

- [ ] Create contact list
- [ ] Include stakeholders
- [ ] Verify information
- [ ] Update annually
- [ ] Document changes
- [ ] Maintain access

Asset Types:

Contacts Documentation

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe requirements and users know how, when, and to whom to report an incident.

IG1 IG2 IG3

Requirements:

- [ ] Define process
- [ ] Set timeframes
- [ ] Train users
- [ ] Monitor reporting
- [ ] Update procedures
- [ ] Document incidents

Asset Types:

Process Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.4: Establish and Maintain an Incident Response Process

Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

IG1 IG2 IG3

Requirements:

- [ ] Define process
- [ ] Assign roles
- [ ] Create plan
- [ ] Review annually
- [ ] Test procedures
- [ ] Update documentation

Asset Types:

Process Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.5: Assign Key Roles and Responsibilities

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.

IG2 IG3

Requirements:

- [ ] Define roles
- [ ] Assign staff
- [ ] Document responsibilities
- [ ] Train personnel
- [ ] Review assignments
- [ ] Update as needed

Asset Types:

Personnel Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.6: Define Mechanisms for Communicating During Incident Response

Define mechanisms for communicating during incident response. Example implementations include contact lists, phone trees, and shared communication channels, such as group chat and instant messaging.

IG2 IG3

Requirements:

- [ ] Define channels
- [ ] Create procedures
- [ ] Test communications
- [ ] Train staff
- [ ] Document methods
- [ ] Update contacts

Asset Types:

Communications Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.7: Conduct Routine Incident Response Exercises

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Update incident response plans and procedures based on exercise results.

IG2 IG3

Requirements:

- [ ] Plan exercises
- [ ] Conduct drills
- [ ] Test procedures
- [ ] Evaluate results
- [ ] Update plans
- [ ] Document lessons

Asset Types:

Training Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.8: Conduct Post-Incident Reviews

Conduct post-incident reviews. Post-incident reviews help improve the enterprise's incident response efforts and provide continuous improvement to the program.

IG2 IG3

Requirements:

- [ ] Review incidents
- [ ] Analyze response
- [ ] Identify improvements
- [ ] Update procedures
- [ ] Document findings
- [ ] Share lessons

Asset Types:

Process Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 17.9: Establish and Maintain Security Incident Thresholds

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal network traffic, abnormal file system activity, or unauthorized use of privileged accounts.

IG2 IG3

Requirements:

- [ ] Define thresholds
- [ ] Set criteria
- [ ] Monitor events
- [ ] Review incidents
- [ ] Update thresholds
- [ ] Document decisions

Asset Types:

Metrics Incident Response

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Safeguard 18.1: Establish and Maintain a Penetration Testing Program

Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, testing methods, testing frequency, documentation of test results, and remediation of findings.

IG2 IG3

Requirements:

- [ ] Define program
- [ ] Set scope
- [ ] Plan tests
- [ ] Document results
- [ ] Track remediation
- [ ] Review annually

Asset Types:

Program Testing

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 18.2: Perform Periodic External Penetration Tests

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be a red team exercise that includes social engineering and physical security testing.

IG2 IG3

Requirements:

- [ ] Schedule tests
- [ ] Define scope
- [ ] Conduct testing
- [ ] Document findings
- [ ] Remediate issues
- [ ] Verify fixes

Asset Types:

External Testing

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 18.3: Remediate Penetration Test Findings

Remediate penetration test findings based on the enterprise's policy and risk rating.

IG2 IG3

Requirements:

- [ ] Review findings
- [ ] Assess risks
- [ ] Prioritize fixes
- [ ] Implement solutions
- [ ] Verify remediation
- [ ] Document actions

Asset Types:

Findings Remediation

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 18.4: Validate Security Measures

Validate security measures after each penetration test. If deemed necessary, modify the penetration testing program based on the test results.

IG3

Requirements:

- [ ] Review measures
- [ ] Test controls
- [ ] Assess effectiveness
- [ ] Update program
- [ ] Document changes
- [ ] Verify improvements

Asset Types:

Security Testing

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...

Safeguard 18.5: Perform Periodic Internal Penetration Tests

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be a red team exercise that includes social engineering and physical security testing. Internal penetration testing must include testing from an unprivileged and privileged user context.

IG3

Requirements:

- [ ] Schedule tests
- [ ] Define scope

- [ ] Conduct testing
- [ ] Document findings
- [ ] Remediate issues
- [ ] Verify fixes

Asset Types:

Internal Testing

Implementation Status:

Select Status

Implementation Evidence:

Describe how this safeguard is implemented, including specific tools, configurations, and processes...