CIS Control 6: Access Control Management

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

Why is this CIS Control Critical?

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

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

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

6.1: Establish an Access Granting Process

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

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

Dependencies

- None

Inputs

1. Enterprise process for granting access to enterprise assets

Operations

1. Check to see if Input 1 exists:

    1. If the enterprise has an access granting process, M1 = 1
    2. If the enterprise does not have an access granting process, M1 = 0

2. Using Input 1, check to see if the process includes, at a minimum, a way to grant access upon new hire, rights grat, and role change of a user:

    1. For each element that is included, assign a value of 1. Sum the value of the elements included. (M2)

Measures

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

Metrics

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

Completeness of Process

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

6.2: Establish an Access Revoking Process

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

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

Dependencies

- None

Inputs

1. Enterprise process for revoking access to enterprise assets

Operations

1. Check to see if Input 1 exists:

    1. If the enterprise has an access revoking process, set M1 = 1.

    2. If the enterprise does not have an access revoking process, set M1 = 0.

2. Using Input 1, check to see if the process includes, at a minimum, a way to revoke access upon termination, rights revocation, and role change of a user:
    1. For each element that is included, assign a value of 1. Sum the value of the elements included (M2).

Measures

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

Metrics

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

Completeness of Process

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

6.3: Require MFA for Externally-Exposed Applications

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

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

Dependencies

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

Inputs

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

Operations

1. Use Input 1 to identify and enumerate externally exposed and third-party applications.

2. Using the output of Operation 1 and `GV22`, identify and enumerate all user accounts associated with the applications (M1).

3. For each account identified in Operation 2, use `GV3` to:

    1. Identify and enumerate accounts properly configured to require MFA (M2).
    2. Identify and enumerate accounts not properly configured to require MFA (M3).

Measures

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

Metrics

Coverage

Metric	**The percentage of externally exposed and third-party application accounts properly configured for MFA**
Calculation	`M2 / M1`

6.4: Require MFA for Remote Network Access

Require MFA for remote network access.

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

Dependencies

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

Inputs

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

Operations

1. Using `GV1` as a guide, identify and enumerate all authorized remote assets (M1).

2. For each asset identified in Operation 1, check configurations `GV3`:

    1. Identify and enumerate assets properly configured to require MFA (M2).
    2. Identify and enumerate assets not properly configured to require MFA (M3).

Measures

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

Metrics

Coverage

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

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 service provider.

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

Dependencies

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

Inputs

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

Operations

1. Using `GV22`, identify and enumerate all administrative accounts (M1).

2. For each administrative account identified in Operation 1, check configurations in `GV3`:

    1. Identify and enumerate administrative accounts properly configured to require MFA (M2).

    2. Identify and enumerate administrative accounts not properly configured to require MFA (M3).

Measures

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

Metrics

Coverage

Metric	**The percentage of administrative accounts properly configured to require MFA**
Calculation	`M2 / M1`

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

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

Asset Type	Security Function	Implementation Groups
Software	Identify	2, 3

Dependencies

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

Inputs

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

Operations

1. Check if the enterprise maintains a `GV23` Authentication and Authorization System Inventory of all on-site and remote service providers:
    1. If the inventory exists, M1 = 1.

   2. If the inventory does not exist or is not provided, M1 = 0.

2. Use `GV5` to identify and enumerate authorized authentication and authorization systems within the enterprise.

3. Use the output of Operation 2 to compare to the existing inventory `GV23`:

   1. Identify and enumerate systems that are authorized and currently in the inventory (M2).
   2. Identify and enumerate systems that are authorized and not currently in the inventory (M3).
   3. Identify and enumerate systems that are not authorized but listed in the current inventory (M4).

4. Compare the date of Input 3 to the current date and capture the timeframe in months (M6).

Measures

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

Metrics

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

Accuracy Score

Metric	**What percentage of the authorized authentication and authorization systems are accounted for in the current enterprise inventory?**
Calculation	`M2 / M5`

Metric	**What percentage of unauthorized authentication and authorization systems are accounted for in the current enterprise inventory?**
Calculation	`M4 / M5`

6.7: Centralize Access Control

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

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

Dependencies

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

Inputs

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

Operations

1. Use `GV5` to identify all directory and SSO services.

2. Use `GV1` to identify and enumerate assets that support directory and SSO services (M1).

3. Check the output of Operations 1 and 2 to ensure each asset is covered by at least one directory or SSO service:

    1. Identify and enumerate assets that are covered by at least one directory or SSO service (M2).
    2. Identify and enumerate assets that are not covered by at least one directory or SSO service (M3).

Measures

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

Metrics

Coverage

Metric	**The percentage of assets that can support directory and SSO service covered by at least one directory or SSO service.**
Calculation	`M2 / M1`

6.8: Define and Maintain Role-Based Access Control

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

Asset Type	Security Function	Implementation Groups
Users	Govern	3

Dependencies

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Inputs

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

Operations

1. Determine whether the enterprise has a process for assigning role-based access control:

    1. If the process exists, M1 = 1
    2. If the process does not exist, M1 = 0

2. Use `GV22` and check if each account is assigned a role or group as outlined by the role-based access control process:

    1. Identify and enumerate accounts that are assigned a role or group (M3)
    2. Identify and enumerate accounts that are not assigned a role or group (M4)

3. Compare the date in Input 3 to the current date and capture the timeframe in months (M5)

Measures

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

Metrics

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

Coverage

Metric	**The percentage of account inventory with a properly assigned role or group.**
Calculation	`M3 / M2`