CIS Control 14: Security Awareness and Skills Training

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

Why is this CIS Control Critical?

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

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

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

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

14.1: Establish and Maintain a Security Awareness Program

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

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

Dependencies

- None

Inputs

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

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

14.2: Train Workforce Members to Recognize Social Engineering Attacks

Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.

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

Dependencies

- None

Inputs

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

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

14.3: Train Workforce Members on Authentication Best Practices

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

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

Dependencies

- None

Inputs

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

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

14.4: Train Workforce on Data Handling Best Practices

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

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

Dependencies

- None

Inputs

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

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

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 the mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

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

Dependencies

- None

Inputs

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

Operations

1. Check enterprise to determine if Input 1 exists

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

2. For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training

   1. Identify and enumerate members who have completed at least initial training (M3)
   2. Identify and enumerate members who have not completed any training (M4)

3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training

4. For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to the current date. Capture timeframe in months.

   1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from the current date (M5)
   2. Identify and enumerate members whose most recent training date is greater than twelve months from the current date (M6)

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

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

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

Dependencies

- None

Inputs

1. Recognizing and Reporting Security Incidents training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

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

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

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

Dependencies

- None

Inputs

1. How to Identify and Report if Their Enterprise Assets are Missing Security Updates training module
2. `GV43`: List of workforce members

3. List of most recent module training completion dates for each workforce member

Operations

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

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

Train workforce members on the dangers of connecting to and transmitting data over insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

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

Dependencies

- None

Inputs

1. Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

Operations

1. Check enterprise to determine if Input 1 exists

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

2. For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training

    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)

3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training

4. For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to the current date. Capture timeframe in months.

    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from the current date (M5)

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

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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

14.9: Conduct Role-Specific Security Awareness and Skills Training

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

Asset Type	Security Function	Implementation Groups
Users	Protect	2, 3

Dependencies

- None

Inputs

1. Role-Specific Security Awareness and Skills Training module
2. `GV43`: List of workforce members
3. List of most recent module training completion dates for each workforce member

Operations

1. Check enterprise to determine if Input 1 exists

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

2. For every member of the workforce in Input 2 `GV43`, determine whether the member has completed training

    1. Identify and enumerate members who have completed at least initial training (M3)
    2. Identify and enumerate members who have not completed any training (M4)

3. For every member of the workforce identified in Operation 2.1, identify the date of most recently completed module training

4. For every member of the workforce identified in Operation 2.1, use the output of Operation 4 and compare the date to the current date. Capture timeframe in months.

    1. Identify and enumerate members whose most recent training date is less than or equal to twelve months from the current date (M5)
    2. Identify and enumerate members whose most recent training date is greater than twelve months from the current date (M6)

Measures

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

Metrics

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

Initial Training Compliance

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

Up to Date Training

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