



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 21 ES-C2M2 Exercise 2

Rick White, Ph.D.
University of Colorado, Colorado
Springs



1

Esc

1



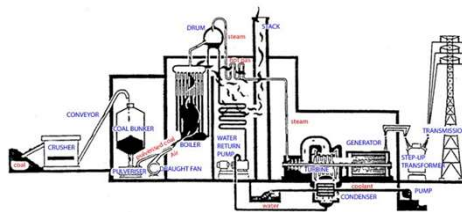
University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

You are the System Security
Officer for "Anywhere Power".



2

Esc

2

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

- Let's move on to Step 2 in the ES-C2M2 Process and "Analyze Identified Gaps".
- This time we will look at Domain 3, "Identity and Access Management".

3 Esc

3

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

- Let's say that access control to all system components is maintained by your system administrator.
- Your system administrator maintains user name and password protection over all components.
- Your system administrator establishes accounts during in-processing for all new employees requiring access.

4 Esc

4

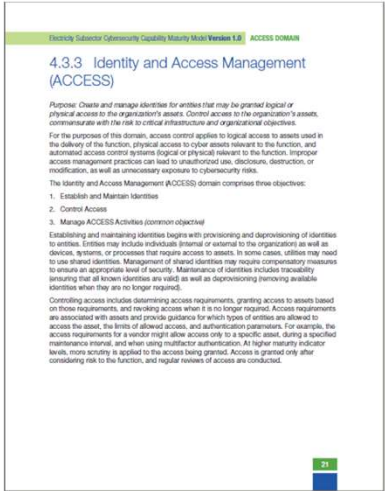


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


ES-C2M2 Exercise 2

- Conversely, your system administrator deletes those accounts when employees out-process.
- To make certain all accounts remain current, the system automatically issues a password reset to all employees every 90 days.



5
Esc

5

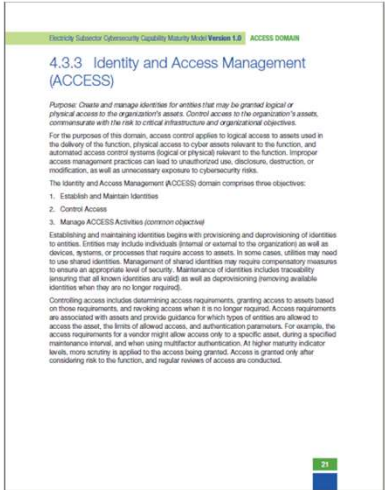


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

Given this description, what Domain Objectives remain to achieve Maturity Level 1 certification for Domain Objective 3.1, “Establish and Maintain Identities”?



6
Esc

6

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 1?

1. Establish and Maintain Identities

MIL1	a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)
	b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)
	c. Identities are deprovisioned when no longer required
MIL2	d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)
	e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity
	f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

7

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 1?

1. Establish and Maintain Identities

MIL1	a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)
	b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)
	c. Identities are deprovisioned when no longer required
MIL2	d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)
	e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity
	f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

8


- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 1?

1. Establish and Maintain Identities

MIL1	<ul style="list-style-type: none"> a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities) b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys) c. Identities are deprovisioned when no longer required
MIL2	<ul style="list-style-type: none"> d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access) e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	<ul style="list-style-type: none"> g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

9



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

The best answer in this case is “none”; the plant already meets the requirements for Maturity Level 1.

Priority Subsector Cybersecurity Capability Maturity Model Version 1.0 | ACCESS DOMAIN

4.3.3 Identity and Access Management (ACCESS)

Purpose: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

For the purposes of this domain, access control applies to logical access to assets used in the delivery of the function, physical access to cyber assets relevant to the function, and automated access control systems logical or physical relevant to the function. Improper access management practices can lead to unauthorized use, disclosure, destruction, or modification, as well as unnecessary exposure to cybersecurity risks.

The Identity and Access Management (ACCESS) domain comprises three objectives:

1. Establish and Maintain Identities
2. Control Access
3. Manage ACCESS Activities (common objective)


Establishing and maintaining identities begins with provisioning and deprovisioning of identities to entities. Entities may include individuals (internal or external to the organization) as well as devices, systems, or processes that require access to assets. In some cases, utilities may need to use shared identities. Management of shared identities may require compensatory measures to ensure an appropriate level of security. Maintenance of identities includes traceability (ensuring that all known identities are valid) as well as deprovisioning (removing available identities when they are no longer required).

Controlling access includes determining access requirements, granting access to assets based on those requirements, and denying access when it is no longer required. Access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters. For example, the access requirements for a vendor might allow access only to a specific asset, during a specified maintenance interval, and when using multifactor authentication. At higher maturity indicator levels, more scrutiny is applied to the access being granted. Access is granted only after considering risk to the function, and regular reviews of access are conducted.

10

Esc

10

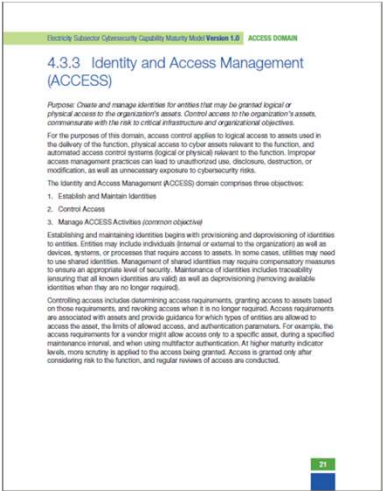


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

Given the same circumstances, what Domain Objectives are required to achieve MIL2 certification within Domain Objective 3.1, “Establish and Maintain Identities”?



11

Esc

11

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 2?

1. Establish and Maintain Identities

MIL1	<ul style="list-style-type: none"> a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities) b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys) c. Identities are deprovisioned when no longer required
MIL2	<ul style="list-style-type: none"> d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access) e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	<ul style="list-style-type: none"> g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

12

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 2?

1. Establish and Maintain Identities

MIL1	<ul style="list-style-type: none"> a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities) b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys) c. Identities are deprovisioned when no longer required
MIL2	<ul style="list-style-type: none"> d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access) e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	<ul style="list-style-type: none"> g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

13


- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.1 Maturity Level 2?

1. Establish and Maintain Identities

MIL1	<ul style="list-style-type: none"> a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities) b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys) c. Identities are deprovisioned when no longer required
MIL2	<ul style="list-style-type: none"> d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access) e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	<ul style="list-style-type: none"> g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

14

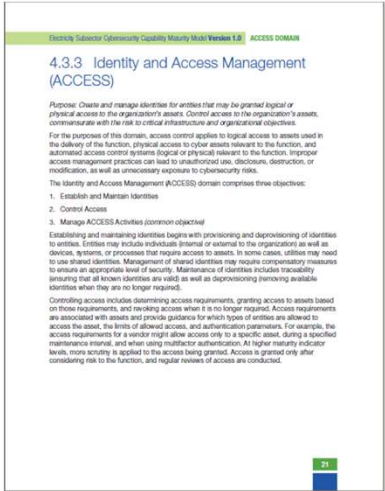


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


ES-C2M2 Exercise 2

- **The correct answer in this case is that you need to complete Domain Objectives “d” and “e”.**
- None of these actions are described as current practice.
- I would contend that current practice already includes Domain Objective “f”.



15
Esc

15

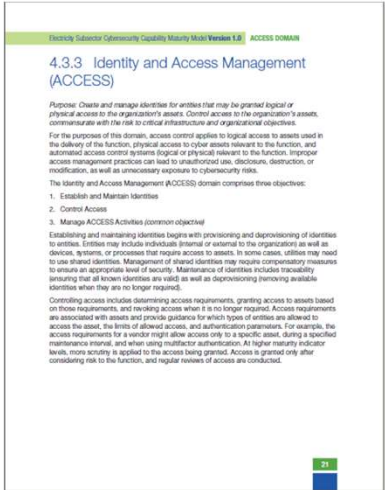


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

- Let's use the same description, but this time let's look at Domain Objective 3.2, “Control Access”
- **Based on stated requirements, what Maturity Level would you assess this plant's current state of practice?**



16
Esc

16

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

How would you evaluate Domain 3.2 maturity? ML1?

2. Control Access

MIL1	<ul style="list-style-type: none"> a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters) b. Access is granted to identities based on requirements c. Access is revoked when no longer required
MIL2	<ul style="list-style-type: none"> d. Access requirements incorporate least privilege and separation of duties principles e. Access requests are reviewed and approved by the asset owner f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	<ul style="list-style-type: none"> g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval h. Access to assets is granted by the asset owner based on risk to the function i. Anomalous access attempts are monitored as indicators of cybersecurity events

17


- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

How would you evaluate Domain 3.2 maturity? ML2?

2. Control Access

MIL1	<ul style="list-style-type: none"> a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters) b. Access is granted to identities based on requirements c. Access is revoked when no longer required
MIL2	<ul style="list-style-type: none"> d. Access requirements incorporate least privilege and separation of duties principles e. Access requests are reviewed and approved by the asset owner f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	<ul style="list-style-type: none"> g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval h. Access to assets is granted by the asset owner based on risk to the function i. Anomalous access attempts are monitored as indicators of cybersecurity events

18



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

- In this case I would say that your plant is currently at MIL0.
- Maturity Level 0 because it's not clear at all that the plant currently meets Domain Objective "a".
- The plant needs to meet Domain Objective "a" just to achieve MIL 1, "Initiated"

Electricity Subsector Cybersecurity Capability Maturity Model Version 1.0 ACCESS DOMAIN

4.3.3 Identity and Access Management (ACCESS)

Purpose: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets commensurate with the risk to critical infrastructure and organizational objectives.

For the purposes of this domain, access control applies to logical access to assets used in the delivery of the function, physical access to cyber assets relevant to the function, and automated access control systems logical or physical relevant to the function. Improper access management practices can lead to unauthorized use, disclosure, destruction, or modification, as well as unnecessary exposure to cybersecurity risks.

The Identity and Access Management (ACCESS) domain comprises three objectives:

1. Establish and Maintain Identities
2. Control Access
3. Manage ACCESS Activities (common objective)


Establishing and maintaining identities begins with provisioning and deprovisioning of identities to entities. Entities may include individuals (internal or external to the organization) as well as devices, systems, or processes that require access to assets. In some cases, utilities may need to use shared identities. Management of shared identities may require compensatory measures to ensure an appropriate level of security. Maintenance of identities includes reviewing identities to ensure that all known identities are valid as well as deprovisioning (removing available identities) when they are no longer required.

Controlling access includes determining access requirements, granting access to assets based on those requirements, and revoking access when it is no longer required. Access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters. For example, the access requirements for a vendor might allow access only to a specific asset, during a specified maintenance interval, and when using multifactor authentication. At higher maturity indicator levels, more scrutiny is applied to the access being granted. Access is granted only after considering risk to the function, and regular reviews of access are conducted.

19

Esc

19



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

What other requirements would the plant need to meet in order to achieve MIL2, "Performed"?

20

Esc

20

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.2 Maturity Level 2? “d”, “e”, “f”?

2. Control Access

MIL1	<ul style="list-style-type: none"> a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters) b. Access is granted to identities based on requirements c. Access is revoked when no longer required
MIL2	<ul style="list-style-type: none"> d. Access requirements incorporate least privilege and separation of duties principles e. Access requests are reviewed and approved by the asset owner f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	<ul style="list-style-type: none"> g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval h. Access to assets is granted by the asset owner based on risk to the function i. Anomalous access attempts are monitored as indicators of cybersecurity events

21

- Access control to all components maintained by system administrator.
- SA maintains user name and password protection over all components.
- SA establishes accounts for all new employees requiring access.
- SA deletes those accounts when employees out-process.
- Password resets automatically issued to all employees every 90 days.

What actions remain to achieve Domain 3.2 Maturity Level 2? “d” & “f”

2. Control Access

MIL1	<ul style="list-style-type: none"> a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters) b. Access is granted to identities based on requirements c. Access is revoked when no longer required
MIL2	<ul style="list-style-type: none"> d. Access requirements incorporate least privilege and separation of duties principles e. Access requests are reviewed and approved by the asset owner f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	<ul style="list-style-type: none"> g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval h. Access to assets is granted by the asset owner based on risk to the function i. Anomalous access attempts are monitored as indicators of cybersecurity events

22

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ES-C2M2 Exercise 2

Easy as pie!

23
Esc

23

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

24
Esc

24