CMMC Tabletop, Deck 1

Access Control & Identification

A printable tabletop exercise deck for CMMC Level 2. Draw cards. Discuss the scenario against the practices on the table. Let the inject change the room. Capture findings on the AAR template. Run it in 60 minutes.

Print settings

- US Letter, color or grayscale
- Two-sided, flip on LONG edge
- Scale: 100% (do not 'fit to page')
- Cut along the registration marks between cards

SCENARIO

What happens

Laptop Left in a Hotel Room

At 7:14 a.m., your engineering lead reports that a company laptop containing CUI was…

SCENARIO

What happens

Prime Forwards CUI by Personal Gmail

Your prime contractor's program manager forwards a CDRL update from her personal Gmail to…

SCENARIO

What happens

MSP Rolls Out New MFA App

Your managed service provider deploys a new MFA application across your engineering laptops overnight,…

SCENARIO

What happens

Contractor Account Still Active

A penetration test report from your MSP lands in your inbox. Buried on page…

SCENARIO What happens

Laptop Left in a Hotel Room

At 7:14 a.m., your engineering lead reports that a company laptop containing CUI was left overnight in a hotel room in Huntsville. The room was serviced by housekeeping. The lead is on the way to the airport and needs to know in the next 30 minutes whether to fly home or stay and recover the device.

SCENARIO What happens

Prime Forwards CUI by Personal Gmail

Your prime contractor's program manager forwards a CDRL update from her personal Gmail to your CTO's personal Gmail, copying a vendor you have not yet onboarded. The attachment is marked CUI//SP-PRVCY. She follows up by Teams asking if you got it.

SCENARIO What happens

MSP Rolls Out New MFA App

Your managed service provider deploys a new MFA application across your engineering laptops overnight, citing a vendor end-of-life. No change notice was sent. Three engineers are now locked out of the CUI enclave on the morning of a milestone delivery.

SCENARIO What happens

Contractor Account Still Active

A penetration test report from your MSP lands in your inbox. Buried on page 14: a contractor account belonging to an engineer who left 11 months ago authenticated successfully to the CUI enclave VPN three times this quarter. The contractor denies it.

SCENARIO What happens

IT Admin Shares Credentials

Your IT administrator, covering for a colleague on leave, uses a shared administrator account…

SCENARIO What happens

Subcontractor Demands Elevated Access

A subcontractor performing CUI data analysis claims they need local administrator rights on the…

SCENARIO What happens

Remote Session Left Open

An automated monitoring alert fires at 2:47 a.m.: a remote desktop session into the…

SCENARIO What happens

Cloud Storage Link Forwarded Externally

A customer success manager at your company forwards a shared cloud storage link containing…

SCENARIO What happens

Subcontractor Demands Elevated Access

A subcontractor performing CUI data analysis claims they need local administrator rights on the CUI enclave workstation to install their analysis tools. Their prime contract is silent on access levels. They have a delivery milestone in 48 hours and are escalating to your program manager.

SCENARIO What happens

IT Admin Shares Credentials

Your IT administrator, covering for a colleague on leave, uses a shared administrator account to reset a VPN configuration in the CUI enclave. The shared account has no individual attribution. A security review flags three configuration changes made under that account over the past week with no change tickets.

SCENARIO What happens

Cloud Storage Link Forwarded Externally

A customer success manager at your company forwards a shared cloud storage link containing CUI deliverables to a government contracting officer via personal email for convenience. The link has no expiry and no access log. The contracting officer has forwarded it once already.

SCENARIO What happens

Remote Session Left Open

An automated monitoring alert fires at 2:47 a.m.: a remote desktop session into the CUI enclave has been idle for 6 hours and 12 minutes. The session belongs to a senior engineer who is traveling overseas for a conference. The session has not timed out. No lockout policy is configured.

PRACTICE What's required

AC.L2-3.1.1

Limit System Access

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

P-AC-3-1-1 grid42.ai/tabletop

PRACTICE What's required

AC.L2-3.1.2

Transaction & Function Control

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

P-AC-3-1-2 grid42.ai/tabletop

PRACTICE What's required

IA.L2-3.5.1

Identification

Identify system users, processes acting on behalf of users, and devices.

P-IA-3-5-1 grid42.ai/tabletop

PRACTICE What's required

IA.L2-3.5.3

Multifactor Authentication

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

P-IA-3-5-3 grid42.ai/tabletop

PRACTICE What's required

AC.L2-3.1.2

Assessment objectives

- The types of transactions and functions that authorized users are permitted to execute are defined.
- System access is limited to the defined types of transactions and functions for authorized users.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.1

Assessment objectives

- Authorized users are identified.
- Processes acting on behalf of authorized users are identified.
- Devices (and other systems) authorized to connect to the system are identified.
- System access is limited to authorized users, processes, and devices.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.3

Assessment objectives

- Privileged accounts are identified.
- Multifactor authentication is implemented for local access to privileged accounts.
- Multifactor authentication is implemented for network access to privileged accounts.
- Multifactor authentication is implemented for network access to non-privileged accounts.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.1

Assessment objectives

- System users are identified.
- Processes acting on behalf of users are identified.
- Devices accessing the system are identified.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.3

CUI Flow Control

Control the flow of CUI in accordance with approved authorizations.

PRACTICE What's required

AC.L2-3.1.5

Least Privilege

Employ the principle of least privilege, including for specific security functions and privileged accounts.

PRACTICE What's required

AC.L2-3.1.7

Privileged Function Execution

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

PRACTICE What's required

AC.L2-3.1.12

Remote Access Sessions

Monitor and control remote access sessions.

PRACTICE What's required

AC.L2-3.1.5

Assessment objectives

- Privileged accounts are identified.
- Access to privileged accounts is authorized in accordance with the principle of least privilege.
- Security functions are identified.
- Access to security functions is authorized.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.3

Assessment objectives

- Information flow control policies are identified.
- Methods and enforcement mechanisms for controlling the flow of CUI are identified.
- Designated sources and destinations for CUI within the system and between interconnected systems are identified.
- Authorizations for controlling the flow of CUI are identified.
- Approved authorizations for controlling the flow of CUI are enforced.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.12

Assessment objectives

- Remote access sessions are permitted based on the types of remote access authorized and users or devices authorized to use remote access.
- Remote access sessions are monitored.
- Remote access sessions are controlled.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.7

Assessment objectives

- Privileged functions are identified.
- Non-privileged users are prevented from executing privileged functions.
- The execution of privileged functions is captured in audit logs.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.20

External System Connections

Verify and control/limit connections to external systems.

PRACTICE What's required

AC.L2-3.1.22

Public-Facing CUI Control

Control CUI posted or processed on publicly accessible systems.

PRACTICE What's required

IA.L2-3.5.2

Authentication

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

PRACTICE What's required

IA.L2-3.5.4

Replay-Resistant Authentication

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

PRACTICE What's required

AC.L2-3.1.22

Assessment objectives

- Individuals authorized to post or process CUI on publicly accessible systems are identified.
- Procedures to ensure CUI is not posted or processed on publicly accessible systems are in place.
- Organizational CUI posted on publicly accessible systems is reviewed.
- CUI posted on publicly accessible systems is removed if discovered.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

AC.L2-3.1.20

Assessment objectives

- Connections to external systems are identified.
- The use of external systems is verified.
- Connections to external systems are controlled.
- The use of external systems is limited.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.4

Assessment objectives

- Replay-resistant authentication mechanisms are identified.
- Replay-resistant authentication is implemented for network access to privileged accounts.
- Replay-resistant authentication is implemented for network access to non-privileged accounts.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.2

Assessment objectives

- The identity of each user is authenticated or verified as a prerequisite to system access.
- The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.
- The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.5

Identifier Management

Identify and authenticate organizational users, the processes acting on behalf of organizational users, or devices.

PRACTICE What's required

IA.L2-3.5.7

Password Complexity

Enforce a minimum password complexity and change of characters when new passwords are created.

PRACTICE What's required

IA.L2-3.5.10

Cryptographically-Protected Passwords

Store and transmit only cryptographically-protected passwords.

PRACTICE What's required

IA.L2-3.5.11

Obscure Authenticator Feedback

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

PRACTICE What's required

IA.L2-3.5.7

Assessment objectives

- Password complexity requirements are defined.
- Password change of characters requirements are defined.
- Password complexity requirements are enforced when new passwords are created.
- Password change of characters requirements are enforced when new passwords are created.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.5

Assessment objectives

- Organizational users are identified.
- Processes acting on behalf of organizational users are identified.
- Devices are identified.
- Organizational users are authenticated.
- Processes acting on behalf of organizational users are authenticated.
- Devices are authenticated.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.11

Assessment objectives

- Authentication information is obscured during the authentication process.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PRACTICE What's required

IA.L2-3.5.10

Assessment objectives

- Passwords are cryptographically protected in storage.
- Passwords are cryptographically protected in transit.

DoD CMMC Assessment Guide L2; NIST SP 800-171A (public domain)

PROCEDURE What to discuss

WHAT would adequate evidence look like for this practice in your environment? Name the artifact, the system it lives in, and the person responsible for producing it.

PROCEDURE What to discuss

WHERE in your environment does this practice apply, and where does it not apply? Is the boundary documented in your system security plan?

PROCEDURE What to discuss

HOW would an assessor sample evidence for this practice across a 6-month period? Walk through the sampling decision out loud.

PROCEDURE What to discuss

WHEN, in the last 12 months, did this practice fail — even briefly? What recovered it? Was that recovery documented?

PROCEDURE What to discuss

How to use this card

Hold this prompt against the drawn Scenario and the four Practice cards on the table. Ask each participant in turn. Capture concrete answers on a sticky note — artifact, system, owner. If the room cannot answer in 60 seconds, that is itself the finding.

PR-02 grid42.ai/tabletop

PROCEDURE What to discuss

How to use this card

Hold this prompt against the drawn Scenario and the four Practice cards on the table. Ask each participant in turn. Capture concrete answers on a sticky note — artifact, system, owner. If the room cannot answer in 60 seconds, that is itself the finding.

PR-01 grid42.ai/tabletop

PROCEDURE What to discuss

How to use this card

Hold this prompt against the drawn Scenario and the four Practice cards on the table. Ask each participant in turn. Capture concrete answers on a sticky note — artifact, system, owner. If the room cannot answer in 60 seconds, that is itself the finding.

PR-04 grid42.ai/tabletop

PROCEDURE What to discuss

How to use this card

Hold this prompt against the drawn Scenario and the four Practice cards on the table. Ask each participant in turn. Capture concrete answers on a sticky note — artifact, system, owner. If the room cannot answer in 60 seconds, that is itself the finding.

PR-03 grid42.ai/tabletop

INJECT What changes

Scope Just Changed

A second business unit using CUI was discovered mid-discussion. It was never added to the SSP. The assessor wants to know in the next 60 minutes whether it's in scope.

INJECT What changes

Documented, Not Implemented

Your assessor rejects the policy you produced as 'documented but not implemented.' Sampling shows the procedure was followed in 2 of 8 cases. Adequacy and sufficiency are now in question.

INJECT What changes

The Author Already Left

The person who wrote your SSP for this practice family left the company two months ago. No transition document exists. The assessor wants to interview the practice owner today.

INJECT What changes

Bid Pressure

A new RFP requires CMMC L2 certification within 90 days. Your readiness assessment had targeted 180 days. The bid response is due Friday. Leadership wants to know what 'good enough' looks like for the bid.

INJECT What changes

How this changes the room

Read this inject out loud after the first response discussion. Do not let the group abandon the original scenario — the inject is added to it. Ask: which decisions made in the first 15 minutes are now wrong, and what would change them back?

IN-02 grid42.ai/tabletop

INJECT What changes

How this changes the room

Read this inject out loud after the first response discussion. Do not let the group abandon the original scenario — the inject is added to it. Ask: which decisions made in the first 15 minutes are now wrong, and what would change them back?

IN-01 grid42.ai/tabletop

INJECT What changes

How this changes the room

Read this inject out loud after the first response discussion. Do not let the group abandon the original scenario — the inject is added to it. Ask: which decisions made in the first 15 minutes are now wrong, and what would change them back?

IN-04 grid42.ai/tabletop

INJECT What changes

How this changes the room

Read this inject out loud after the first response discussion. Do not let the group abandon the original scenario — the inject is added to it. Ask: which decisions made in the first 15 minutes are now wrong, and what would change them back?

IN-03 grid42.ai/tabletop