Analog Informatics™ Corporation

CMMC Requirements to Feature Mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Canonical map of Cybersecurity Maturity Model Certification (**CMMC**) Level 1, Level 2, and Level 3 requirements to the Analog Informatics Corporation (**AIC**) kitted package modules. Companion to the CMMC Solutions Price List. Each row gives the official requirement identifier and short name, the kit role, how the kit meets or supports the requirement, availability, and what the organization still does by hand. Implementation depth for engineers also lives in the CMMC Level 2 enclave kit coverage and customer responsibility matrix.

Authority sources (public). Requirement identifiers and short names follow 32 CFR 170.14. Level 1 has 15 requirements, one for each security requirement in Federal Acquisition Regulation (**FAR**) clause 52.204-21 paragraph (b)(1), with identifiers such as `AC.L1-b.1.i`. Level 2 practices are the 110 National Institute of Standards and Technology (**NIST**) Special Publication 800-171 Rev 2 security requirements as assessed under CMMC Level 2. Level 3 rows are the selected NIST SP 800-172 enhanced requirements assessed under CMMC Level 3, plus themes that remain permanently organizational.

Kit Role Legend

Kit Role	Meaning
Performs	On AIC-managed systems and kit paths, the named feature carries out the requirement. The organization covers systems outside the kit.
Assists	The kit supplies the tool, workflow, or record. People carry out the requirement.
Records	The requirement is physical, personnel, or policy work. The Assessment Binder stores the organization's record of it.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Availability Legend

Availability	Meaning
Available now	The feature ships in the kit for that level today.
Available now, wider scope planned	The feature ships today on kit paths; broader coverage is on the roadmap.
Planned	The feature is on the roadmap and not in the kit today.
Organization	No kit feature carries out the requirement. The organization performs it.

The last column of every table lists what the organization still does by hand.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Modules in the Kitted Packages

Module	What It Is in This Map	In Which Package
Assessment Binder	Auditor-facing living binder and evidence package surface	Level 1, 2, 3
Current State Compliance (**CSC**)	Admin ledger of control-oriented findings and rescan	Level 1, 2, 3
Privileged Identity Management (**PIM**)	Credential lifecycle / vaulted identities	Level 2, 3
Privileged Access Management (**PAM**)	Session Connect / Open, Jump, recording (Level 3 only), command restriction	Level 2, 3
Privileged User Management (**PUM**)	Privilege Elevation and Delegation Management (**PEDM**): cross-platform endpoint privilege elevation, delegation, least-privilege enforcement, application and command control, just-in-time (**JIT**) elevation, and privileged activity auditing on Windows, Apple Mac, and Unix/Linux	Level 2, 3
Identity Governance and Administration (**IGA**)	Account lifecycle and periodic access review designations in the Level 2 / 3 kit	Level 2, 3
Audit	Privileged-action and session-related audit records on AIC paths; Windows Event Log / syslog when configured	Level 2, 3
Document sharing vault (**AIC secure share**)	Secure store and share for FCI / CUI in the AIC Server (5 named users on Level 1; 25 on Level 2 / 3). Extra named users = **AIC-SHARE**	Level 1, 2, 3
Training and attestation (**AIC-TRAIN-ATTEST**)	Assign documents; collect signed attestation (25 seats)	Level 2, 3
Secure Application Launch (**AIC-APP-LAUNCH**)	Launch apps with injected credentials the user does not see	Level 2, 3

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Module	What It Is in This Map	In Which Package
Jump / recording	Session Connect broker; Level 2 base unrecorded; Level 3 isolated Jump with session recording; extra capacity **AIC-JUMP-EXT** on Level 3	Level 2, 3
Incident Response (**IR**)	IR module on the Level 2 / 3 package	Level 2, 3
Federal Information Processing Standards (**FIPS**) cryptography	FIPS-oriented crypto on AIC crypto paths	Level 2, 3
Internal Managed Systems (**AIC-EP-INT**)	In-enclave managed seats (Security Technical Implementation Guide (**STIG**) image workstations and servers)	Level 1: AIC Server only; Level 2 / 3: 25 included
External Managed Systems (**AIC-EP-EXT**) / configuration compliance	Security configuration assessment of connecting systems by direct connection or the configuration compliance agent; attest, inspect, and optional block	Add-on on all levels when workstations connect
Governed mail	Secure email server for FCI or CUI, included on Level 1, Level 2, and Level 3. Each named user has one email account.	Level 1, 2, 3

1. Level 1 - Federal Contract Information (FCI)

Package: AIC-CMMC-L1. Kit center: Assessment Binder, Current State Compliance (CSC), one Internal Managed System (the AIC Server), document sharing vault (AIC secure share; 5 named users). Configuration compliance for connecting systems (AIC-EP-EXT) by direct connection or the configuration compliance agent. Extra vault named users = AIC-SHARE. Governed mail is included. Each named user has one FCI email account.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L1-b.1.i	Authorized Access Control	Performs	Only people with a kit account and an assigned role can sign in, through your directory or a local account, with MFA. RBAC checks every console page. Vault documents open only for named users.	Available now, wider scope planned	Grant and remove access on systems the kit does not manage.
AC.L1-b.1.ii	Transaction & Function Control	Performs	Each role allows only its assigned console functions. Each vault folder and document carries named-user permissions.	Available now, wider scope planned	Limit transactions and functions on other systems.
AC.L1-b.1.iii	External Connections	Performs	Configuration compliance checks each connecting system and can block one that fails. Conditional access limits sign-in by country and network address.	Available now, wider scope planned	Approve and document connections to external systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L1-b.1.iv	Control Public Information	Records	The Assessment Binder stores the organization's record.	Organization	Review and approve what is posted on public systems.
IA.L1-b.1.v	Identification	Performs	Every user is a named person from your directory or a local account. Each enrolled system has its own Agent identity.	Available now, wider scope planned	Give each user and device a unique identity on other systems.
IA.L1-b.1.vi	Authentication	Performs	Sign-in checks your directory or a local password, then MFA. Repeated failures lock the account.	Available now, wider scope planned	Set password and MFA policy on other systems.
MP.L1-b.1.vii	Media Disposal	Records	The Assessment Binder stores the organization's record.	Organization	Wipe or destroy media that held FCI with physical tools and a witnessed procedure.
PE.L1-b.1.viii	Limit Physical Access	Records	The Assessment Binder stores the organization's record.	Organization	Control locks, badges, and facility boundaries.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
PE.L1-b.1.ix	Manage Visitors & Physical Access	Records	The Assessment Binder stores the organization's record.	Organization	Escort visitors, monitor their activity, keep physical access logs, and manage keys and badges.
SC.L1-b.1.x	Boundary Protection	Performs	The secure enclave has an isolated network and a secure gateway. Kit traffic is encrypted with TLS through a cryptographic module that holds a FIPS 140-3 certificate.	Available now, wider scope planned	Operate the firewalls and routers at the organization's boundary.
SC.L1-b.1.xi	Public-Access System Separation	Records	The Assessment Binder stores the organization's record.	Organization	Put public-facing systems on their own subnetwork.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SI.L1-b.1.xii	Flaw Remediation	Assists	Configuration compliance reports flaws on enrolled systems. Fix-It repairs known settings, Current State Compliance Rescan confirms the repair, and product updates are signed.	Available now, wider scope planned	Patch every host on schedule.
SI.L1-b.1.xiii	Malicious Code Protection	Assists	Configuration compliance reports whether antimalware is installed and running, and flags the system for IT when it is not.	Organization	Select and operate antimalware or Endpoint Detection and Response (EDR) software.
SI.L1-b.1.xiv	Update Malicious Code Protection	Records	The Assessment Binder stores the organization's record.	Organization	Update antimalware signatures and engines.
SI.L1-b.1.xv	System & File Scanning	Records	The Assessment Binder stores the organization's record.	Organization	Schedule periodic scans and real-time scans of files from outside sources.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

2. Level 2 - Controlled Unclassified Information (CUI)

Package: **AIC-CMMC-L2**. Includes Level 1 tools plus Privileged Identity Management (**PIM**), Privileged Access Management (**PAM**), Privileged User Management (**PUM**), Identity Governance and Administration (**IGA**), Audit, document sharing vault (**AIC secure share**; 25 named users), training and attestation (**AIC-TRAIN-ATTEST**; 25), Secure Application Launch (**AIC-APP-LAUNCH**), session Connect through Jump, command restriction, Incident Response (**IR**), and Federal Information Processing Standards (**FIPS**) cryptography. Seat floors: 25 Internal Managed Systems, 25 email, 25 share, 25 train-and-attest.

Practice identifiers use the CMMC Level 2 form (`AC.L2-3.1.1` and siblings) matching NIST SP 800-171 Rev 2.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.1	Authorized Access Control	Performs	Only people with a kit account and an assigned role can sign in, with MFA. RBAC checks every console page and interface. PIM releases a vaulted privileged password only to an approved user, and PAM connects that user only to an approved target. Vault documents open only for named users.	Available now	Grant and remove access on systems the kit does not manage.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.2	Transaction & Function Control	Performs	Each role allows only its assigned console functions. PAM approval policies set which systems and protocols each user reaches. Command restriction blocks a disallowed command as it is typed. Secure Application Launch starts only approved applications.	Available now	Define the functions each role needs.
AC.L2-3.1.3	Control CUI Flow	Performs	Data classification marks FCI and CUI, checks each person's clearance before release, and records every release. The document sharing vault and governed mail keep CUI on kit paths.	Available now, wider scope planned	Control the flow of CUI on systems outside the kit.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.4	Separation of Duties	Assists	Administrator, approver, auditor, and user are separate roles, and privileged access goes through an approval workflow. IGA access review shows who holds each role.	Available now	Decide which duties must be separated, and assign people to roles.
AC.L2-3.1.5	Least Privilege	Performs	PUM grants administrator rights for one task and removes them afterward, so users keep no standing administrator rights. PIM checks out privileged passwords for a limited time and rotates them. PAM approvals expire.	Available now	Apply least privilege on systems the kit does not manage.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.6	Non-Privileged Account Use	Performs	Privileged accounts live in the PIM vault. People sign in with their own everyday identity and check out a privileged account, or request elevation, only when a task needs it.	Available now	Issue separate everyday accounts on systems outside the kit.
AC.L2-3.1.7	Privileged Functions	Performs	PUM stops a non-privileged user from running a privileged function until a request is approved and a signed grant is issued. Every privileged action is written to the audit log with the person's name.	Available now	Review privileged activity on schedule.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.8	Unsuccessful Logon Attempts	Performs	The console locks an account after repeated failed sign-ins. Conditional access and threat feeds block sign-in attempts from denied locations and known bad addresses.	Available now	Set lockout on systems outside the kit.
AC.L2-3.1.9	Privacy & Security Notices	Records	A logon banner for every managed host is planned. Today the Assessment Binder stores the banner text and where it is set.	Planned	Set logon banners on each system.
AC.L2-3.1.10	Session Lock	Assists	Console sessions end after an idle timeout.	Available now, wider scope planned	Set a pattern-hiding screen lock on each workstation.
AC.L2-3.1.11	Session Termination	Performs	Sessions end at an idle timeout and at an absolute time limit. Signing out revokes the session on the server, so its token cannot be reused.	Available now	Set session termination on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.12	Control Remote Access	Performs	PAM brokers SSH, RDP, and VNC sessions in the browser, so privileged remote access takes one approved, audited path. Conditional access checks country, network address, and MFA before the session starts.	Available now, wider scope planned	Control remote access through the organization's VPN and other paths.
AC.L2-3.1.13	Remote Access Confidentiality	Performs	Console, Agent, and session traffic is encrypted with TLS through AWS-LC, which holds a FIPS 140-3 certificate.	Available now	Encrypt remote access paths outside the kit.
AC.L2-3.1.14	Remote Access Routing	Assists	When Jump is deployed, privileged remote sessions route through it as the managed access point.	Organization	Route all other remote access through managed access points.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.15	Privileged Remote Access	Performs	Each PAM session needs approval before it starts. PUM elevation needs approval and a signed grant. Command restriction blocks disallowed SSH commands as they are typed.	Available now	Authorize privileged remote access on other paths.
AC.L2-3.1.16	Wireless Access Authorization	Records	The Assessment Binder stores the organization's record.	Organization	Authorize wireless access before connections are allowed.
AC.L2-3.1.17	Wireless Access Protection	Records	The Assessment Binder stores the organization's record.	Organization	Protect wireless access with authentication and encryption.
AC.L2-3.1.18	Mobile Device Connection	Records	The Assessment Binder stores the organization's record.	Organization	Control the connection of mobile devices.
AC.L2-3.1.19	Encrypt CUI on Mobile	Assists	CUI stored in the kit is encrypted with AES-256.	Available now, wider scope planned	Encrypt the storage of phones and laptops.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L2-3.1.20	External Connections	Performs	Configuration compliance checks each connecting system and can block one that fails. Data classification limits release of CUI on kit paths.	Available now, wider scope planned	Approve and document external connections.
AC.L2-3.1.21	Portable Storage Use	Records	The Assessment Binder stores the organization's record.	Organization	Limit portable storage on external systems.
AC.L2-3.1.22	Control Public Information	Records	The Assessment Binder stores the organization's record.	Organization	Review and approve what is posted on public systems.
AT.L2-3.2.1	Role-Based Risk Awareness	Assists	Training and attestation assigns security awareness material from 53 ready-made templates to named people, sends reminders, and stores each signed attestation. Completion reports show who is done.	Available now, wider scope planned	Choose content that fits the environment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AT.L2-3.2.2	Role-Based Training	Assists	The kit assigns templates to the named people in each role, with due dates, reminders, and completion reports.	Available now, wider scope planned	Design the role-based training.
AT.L2-3.2.3	Insider Threat Awareness	Assists	The Insider Threat Awareness template is assigned to named people, and each signed attestation is stored.	Available now, wider scope planned	Run the insider threat program.
AU.L2-3.3.1	System Auditing	Performs	The kit writes audit records for sign-in, access, elevation, sessions, configuration changes, and secret actions. Records go to the Windows Event Log and, as syslog in RFC 5424, CEF, or LEEF format, to your SIEM.	Available now	Set retention, and log systems outside the kit.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AU.L2-3.3.2	User Accountability	Performs	Each record names the person, the action, the target, the outcome, and a request ID, so every action traces to one individual.	Available now	Use named accounts on other systems.
AU.L2-3.3.3	Event Review	Assists	Audit event selection and SIEM forwarding settings let you change which events are logged after each review.	Available now, wider scope planned	Review which events are logged.
AU.L2-3.3.4	Audit Failure Alerting	Performs	The kit alerts when the audit or forwarding pipeline fails.	Available now	Respond to the alert.
AU.L2-3.3.5	Audit Correlation	Assists	A request ID links related records, and forwarding sends them to your SIEM for correlation. The attack report maps blocked attacks to MITRE ATT&CK.	Available now, wider scope planned	Correlate all sources in the SIEM.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AU.L2-3.3.6	Reduction & Reporting	Assists	Audit search, filters, and export reduce records to what a review needs. The Assessment Binder produces reports.	Available now, wider scope planned	Report on sources outside the kit.
AU.L2-3.3.7	Authoritative Time Source	Assists	The server stamps every record in UTC and warns when a clock drifts.	Available now, wider scope planned	Run the authoritative time source.
AU.L2-3.3.8	Audit Protection	Performs	Audit records are insert-only, so they cannot be edited in place. Audit exports are hash-chained, so a changed record is detectable.	Available now	Protect copies in the SIEM and archive.
AU.L2-3.3.9	Audit Management	Performs	Only authorized roles can view or export audit records.	Available now	Limit audit management on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
CM.L2-3.4.1	System Baselining	Assists	Configuration compliance holds a STIG-oriented baseline for each enrolled system and keeps an inventory of enrolled systems.	Available now, wider scope planned	Set baselines and keep inventory for systems outside the kit.
CM.L2-3.4.2	Security Configuration Enforcement	Performs	Configuration compliance checks each setting against the baseline. Fix-It repairs known settings. Findings the kit cannot repair are flagged for IT.	Available now	Fix the flagged findings.
CM.L2-3.4.3	System Change Management	Assists	Kit setting changes are audited with the person's name. Current State Compliance records drift between scans, so an unapproved change shows up.	Available now, wider scope planned	Run change approval.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
CM.L2-3.4.4	Security Impact Analysis	Assists	Current State Compliance Rescan shows the effect of a change on each control.	Organization	Analyze security impact before each change.
CM.L2-3.4.5	Access Restrictions for Change	Performs	Only authorized roles can change kit settings, and each change is audited.	Available now	Restrict changes on other systems.
CM.L2-3.4.6	Least Functionality	Assists	Configuration compliance flags settings outside the baseline. Secure Application Launch starts only approved applications.	Available now, wider scope planned	Decide which functions are essential.
CM.L2-3.4.7	Nonessential Functionality	Assists	Configuration compliance flags services that are not in the baseline.	Available now, wider scope planned	Remove or disable nonessential programs, ports, and services.
CM.L2-3.4.8	Application Execution Policy	Records	The Assessment Binder stores the organization's record.	Organization	Set the application allow or deny policy.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
CM.L2-3.4.9	User-Installed Software	Records	The Assessment Binder stores the organization's record.	Organization	Control and monitor user-installed software.
IA.L2-3.5.1	Identification	Performs	People come from your directory as named users. Each enrolled system has its own Agent identity. Vaulted accounts are inventoried.	Available now	Identify users and devices on other systems.
IA.L2-3.5.2	Authentication	Performs	Sign-in goes through Active Directory, LDAP, Microsoft Entra ID, Okta, Ping Identity, OpenID Connect, or SAML 2.0. Local passwords are stored as PBKDF2 hashes.	Available now	Authenticate users on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
IA.L2-3.5.3	Multifactor Authentication	Performs	Console sign-in requires MFA. PAM sessions and PUM requests start from that sign-in, so privileged access always passes MFA.	Available now, wider scope planned	Require MFA for network access to other systems.
IA.L2-3.5.4	Replay-Resistant Authentication	Performs	One-time codes and per-session tokens cannot be replayed, and every kit path uses TLS.	Available now	Use replay-resistant sign-in on other systems.
IA.L2-3.5.5	Identifier Reuse	Assists	Each person keeps one durable identity record in the kit, so an identifier is not handed to someone else.	Available now, wider scope planned	Prevent identifier reuse in the directory.
IA.L2-3.5.6	Identifier Handling	Assists	IGA lifecycle and access review show inactive kit accounts so they can be disabled.	Available now, wider scope planned	Disable inactive identities in the identity provider.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
IA.L2-3.5.7	Password Complexity	Performs	PIM generates rotated passwords that meet your complexity policy. Local console passwords must meet a complexity rule.	Available now	Set complexity on other systems.
IA.L2-3.5.8	Password Reuse	Performs	Password history blocks reuse of rotated passwords and local console passwords.	Available now	Set password history on other systems.
IA.L2-3.5.9	Temporary Passwords	Assists	PIM rotates managed account passwords on a schedule, so a shared temporary password does not last.	Available now, wider scope planned	Force temporary password changes on other systems.
IA.L2-3.5.10	Cryptographically-Protected Passwords	Performs	Passwords are stored as PBKDF2 hashes, vaulted secrets are encrypted with AES-256, and passwords travel only over TLS.	Available now	Protect passwords on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
IA.L2-3.5.11	Obscure Feedback	Performs	Password fields are masked, and a failed sign-in returns one generic message that does not say which part was wrong.	Available now	Obscure feedback on other systems.
IR.L2-3.6.1	Incident Handling	Assists	Incident Response records each incident, runs detections, and alerts the right people by email, text message, and ticket.	Available now, wider scope planned	Staff the response team and run each incident.
IR.L2-3.6.2	Incident Reporting	Assists	Incident records keep status and history, and they forward to ticket systems and the SIEM.	Available now, wider scope planned	Report incidents to the Department of Defense as DFARS 252.204-7012 requires.
IR.L2-3.6.3	Incident Response Testing	Assists	Incident Response records can hold the results of tests and tabletop exercises.	Organization	Run tests and tabletop exercises.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
MA.L2-3.7.1	Perform Maintenance	Assists	Maintenance on managed systems can run through PAM sessions, which leave audit records.	Organization	Plan and perform maintenance.
MA.L2-3.7.2	System Maintenance Control	Assists	Maintenance runs through PAM and Jump with approvals. Secure Application Launch starts only approved tools.	Available now, wider scope planned	Control the tools brought on site.
MA.L2-3.7.3	Equipment Sanitization	Records	The Assessment Binder stores the organization's record.	Organization	Sanitize equipment sent off site for maintenance.
MA.L2-3.7.4	Media Inspection	Records	The Assessment Binder stores the organization's record.	Organization	Check media with diagnostic programs before use.
MA.L2-3.7.5	Nonlocal Maintenance	Performs	A PAM maintenance session starts only after MFA at console sign-in, and it ends at the session timeout.	Available now, wider scope planned	Require MFA for nonlocal maintenance on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
MA.L2-3.7.6	Maintenance Personnel	Assists	Each vendor session needs approval, command restriction limits what the vendor can run, and the session leaves an audit record.	Available now, wider scope planned	Escort maintenance staff on site.
MP.L2-3.8.1	Media Protection	Assists	The document sharing vault protects digital CUI with named-user access, encryption, and classification markings.	Available now, wider scope planned	Protect paper and removable media.
MP.L2-3.8.2	Media Access	Performs	The vault checks named-user permissions and clearance before CUI opens.	Available now, wider scope planned	Limit access to physical media.
MP.L2-3.8.3	Media Disposal	Records	The Assessment Binder stores the organization's record.	Organization	Sanitize or destroy media.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
MP.L2-3.8.4	Media Markings	Performs	Data classification applies CUI markings to documents in the vault and messages in governed mail.	Available now, wider scope planned	Mark physical media.
MP.L2-3.8.5	Media Accountability	Records	The Assessment Binder stores the organization's record.	Organization	Control media during transport.
MP.L2-3.8.6	Portable Storage Encryption	Performs	Data the kit stores is encrypted with AES-256, and data it moves is protected by TLS, through AWS-LC cryptography.	Available now	Encrypt media transported outside the kit.
MP.L2-3.8.7	Removable Media	Records	The Assessment Binder stores the organization's record.	Organization	Control removable media.
MP.L2-3.8.8	Shared Media	Records	The Assessment Binder stores the organization's record.	Organization	Prohibit portable storage with no identifiable owner.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
MP.L2-3.8.9	Protect Backups	Assists	Data the kit stores is encrypted with keys the organization holds, so backup copies of kit data stay encrypted.	Available now, wider scope planned	Protect backup copies.
PS.L2-3.9.1	Screen Individuals	Records	The workforce roster records who is in scope, and the Assessment Binder stores screening records.	Organization	Screen people before they get access to CUI.
PS.L2-3.9.2	Personnel Actions	Assists	Disabling a person revokes their kit sessions and access at once. IGA access review confirms the access was removed.	Available now, wider scope planned	Run transfer and termination steps.
PE.L2-3.10.1	Limit Physical Access	Records	The Assessment Binder stores the organization's record.	Organization	Limit physical access.
PE.L2-3.10.2	Monitor Facility	Records	The Assessment Binder stores the organization's record.	Organization	Protect and monitor the facility.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
PE.L2-3.10.3	Escort Visitors	Records	The Assessment Binder stores the organization's record.	Organization	Escort visitors and monitor their activity.
PE.L2-3.10.4	Physical Access Logs	Records	The Assessment Binder stores the organization's record.	Organization	Keep physical access logs.
PE.L2-3.10.5	Manage Physical Access	Records	The Assessment Binder stores the organization's record.	Organization	Manage physical access devices.
PE.L2-3.10.6	Alternative Work Sites	Records	The Assessment Binder stores the organization's record.	Organization	Enforce safeguards at alternate work sites.
RA.L2-3.11.1	Risk Assessments	Assists	Current State Compliance findings and the risk register in the Assessment Binder feed the risk assessment.	Organization	Perform the risk assessment.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
RA.L2-3.11.2	Vulnerability Scan	Assists	A vulnerability analysis add-on is planned. Network scan and known default credential detection are available now.	Planned	Run a vulnerability scanner.
RA.L2-3.11.3	Vulnerability Remediation	Assists	Current State Compliance lists findings. Fix-It repairs known settings, other findings are flagged for IT, and open items become POA&M entries.	Available now, wider scope planned	Remediate the findings.
CA.L2-3.12.1	Security Control Assessment	Assists	Current State Compliance rescans each control, and the Assessment Binder holds the results.	Available now, wider scope planned	Assess controls periodically.
CA.L2-3.12.2	Operational Plan of Action	Assists	The Assessment Binder holds the POA&M and the risk register.	Organization	Own and maintain the plan.
CA.L2-3.12.3	Security Control Monitoring	Performs	Current State Compliance rescans controls and records drift.	Available now, wider scope planned	Monitor controls outside the kit.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
CA.L2-3.12.4	System Security Plan	Assists	The Assessment Binder supports the SSP with a narrative wizard.	Organization	Write and maintain the SSP.
SC.L2-3.13.1	Boundary Protection	Performs	The secure enclave has an isolated network and a secure gateway. Governed mail and data classification release controls govern what leaves the boundary.	Available now, wider scope planned	Operate the boundary firewalls.
SC.L2-3.13.2	Security Engineering	Assists	The enclave comes preconfigured, with separate administration and Agent paths.	Available now, wider scope planned	Engineer the rest of the environment.
SC.L2-3.13.3	Role Separation	Performs	Role checks separate the administrator console from user and Agent functions.	Available now	Separate user and administrator functions on other systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SC.L2-3.13.4	Shared Resource Control	Performs	Vault documents open only for named users. PAM sessions use vaulted credentials without showing them to the user.	Available now, wider scope planned	Prevent unauthorized transfer through shared resources elsewhere.
SC.L2-3.13.5	Public-Access System Separation	Records	The Assessment Binder stores the organization's record.	Organization	Design the public-facing subnetwork.
SC.L2-3.13.6	Network Communication by Exception	Assists	The enclave network sits behind a secure gateway. Conditional access blocks sign-in from denied countries, networks, and threat feeds.	Available now, wider scope planned	Set deny-by-default rules on the network.
SC.L2-3.13.7	Split Tunneling	Records	The Assessment Binder stores the organization's record.	Organization	Prevent split tunneling.
SC.L2-3.13.8	Data in Transit	Performs	Kit traffic, including governed mail, is encrypted with TLS through AWS-LC.	Available now	Encrypt CUI in transit outside the kit.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SC.L2-3.13.9	Connections Termination	Performs	Sessions end at idle and absolute timeouts.	Available now	Terminate network connections on other systems.
SC.L2-3.13.10	Key Management	Performs	Keys live in software, an HSM, or your cloud key management service. Each group gets its own key set. Keys rotate, and data is re-encrypted under the new key.	Available now	Manage keys outside the kit.
SC.L2-3.13.11	CUI Encryption	Performs	Server paths use AWS-LC, which holds a FIPS 140-3 certificate. The Agent uses the operating system's validated cryptography.	Available now	Use validated cryptography on other systems.
SC.L2-3.13.12	Collaborative Device Control	Records	The Assessment Binder stores the organization's record.	Organization	Control collaborative computing devices.
SC.L2-3.13.13	Mobile Code	Records	The Assessment Binder stores the organization's record.	Organization	Control mobile code.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SC.L2-3.13.14	Voice over Internet Protocol	Records	The Assessment Binder stores the organization's record.	Organization	Control Voice over Internet Protocol (VoIP).
SC.L2-3.13.15	Communications Authenticity	Performs	TLS authenticates each session, and session tokens are bound to the signed-in user.	Available now	Protect session authenticity on other systems.
SC.L2-3.13.16	Data at Rest	Performs	Stored secrets and vault documents are encrypted with AES-256-GCM.	Available now	Protect CUI at rest outside the kit.
SI.L2-3.14.1	Flaw Remediation	Assists	Configuration compliance reports flaws on enrolled systems. Current State Compliance Rescan confirms each repair, and product updates are signed.	Available now, wider scope planned	Patch hosts on schedule.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SI.L2-3.14.2	Malicious Code Protection	Assists	Configuration compliance reports whether antimalware is running, and flags the system for IT when it is not.	Organization	Operate antimalware or EDR software.
SI.L2-3.14.3	Security Alerts & Advisories	Assists	Threat indicator feeds and Current State Compliance findings bring alerts into the console.	Available now, wider scope planned	Subscribe to security advisories and act on them.
SI.L2-3.14.4	Update Malicious Code Protection	Records	The Assessment Binder stores the organization's record.	Organization	Update antimalware signatures.
SI.L2-3.14.5	System & File Scanning	Records	The Assessment Binder stores the organization's record.	Organization	Schedule periodic and real-time scans.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SI.L2-3.14.6	Monitor Communications for Attacks	Assists	Threat feeds block sign-in from known bad addresses, Incident Response runs detections, the attack report maps blocked attacks to MITRE ATT&CK, and records go to your SIEM.	Available now, wider scope planned	Monitor traffic outside the kit.
SI.L2-3.14.7	Identify Unauthorized Use	Assists	Detections flag unusual sign-in and privileged activity, and session and audit records show what each person did.	Available now, wider scope planned	Define authorized use.

3. Level 3 - CUI with Enhanced Requirements

Package: **AIC-CMMC-L3**. Everything in Level 2, plus isolated Jump with session recording, command restriction, and National Institute of Standards and Technology (**NIST**) Special Publication 800-172 mapping in the Assessment Binder. Extra Jump capacity: **AIC-JUMP-EXT**.

Rows below are the 24 selected NIST SP 800-172 enhanced requirements assessed under CMMC Level 3, with identifiers and short names from 32 CFR 170.14.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AC.L3-3.1.2e	Organizationally Controlled Assets	Performs	Configuration compliance checks each connecting system and can block one that fails. Each enrolled system has its own Agent identity, so only systems the organization controls reach the kit.	Available now, wider scope planned	Decide which systems are organization-owned or issued.
AC.L3-3.1.3e	Secured Information Transfer	Assists	Data classification enforces clearances and records each release. The document sharing vault and the isolated Jump carry information between security domains.	Available now, wider scope planned	Define the security domains.
AT.L3-3.2.1e	Advanced Threat Awareness	Assists	Training and attestation assigns the Phishing Awareness and Insider Threat Awareness templates and stores signed attestations.	Organization	Provide advanced-threat content.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
AT.L3-3.2.2e	Practical Training Exercises	Assists	Training and attestation assigns the material and records completion.	Organization	Run practical exercises.
CM.L3-3.4.1e	Authoritative Repository	Assists	The kit keeps an inventory of enrolled systems, with the approved baseline for each.	Available now, wider scope planned	Approve components and maintain the repository.
CM.L3-3.4.2e	Automated Detection & Remediation	Performs	Configuration compliance detects drift automatically, Fix-It repairs known settings, and a failing system can be blocked. Current State Compliance records each finding.	Available now, wider scope planned	Remove or repair components the kit flags.
CM.L3-3.4.3e	Automated Inventory	Assists	The kit inventories enrolled systems. Network scan and known default credential detection find other systems on the network.	Available now, wider scope planned	Inventory systems outside the scan.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
IA.L3-3.5.1e	Bidirectional Authentication	Assists	Each enrolled system has its own Agent identity, which is checked before the Agent connects.	Available now, wider scope planned	Authenticate network devices outside the kit.
IA.L3-3.5.3e	Block Untrusted Assets	Performs	Configuration compliance can block a system that fails its checks. Conditional access blocks sign-in from untrusted locations and addresses.	Available now, wider scope planned	Block unknown components on the network.
IR.L3-3.6.1e	Security Operations Center	Assists	Incident Response detections and alerts, Current State Compliance monitoring, and SIEM forwarding give the security operations center its data.	Available now, wider scope planned	Staff the security operations center.
IR.L3-3.6.2e	Cyber Incident Response Team	Assists	Incident records and alerts by email, text message, and ticket reach the response team quickly.	Available now, wider scope planned	Staff and deploy the response team.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
PS.L3-3.9.2e	Adverse Information	Assists	When the organization directs it, disabling a person revokes their kit sessions and access at once.	Organization	Act on adverse information.
RA.L3-3.11.1e	Threat-Informed Risk Assessment	Assists	Threat indicator feeds are applied at sign-in, and the attack report maps blocked attacks to MITRE ATT&CK, giving the risk assessment current threat data.	Available now, wider scope planned	Choose intelligence sources.
RA.L3-3.11.2e	Threat Hunting	Assists	Recorded Jump sessions can be replayed, and audit search and indicator search give hunters the records they need.	Available now, wider scope planned	Run the hunting program.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
RA.L3-3.11.3e	Advanced Risk Identification	Assists	Current State Compliance and Incident Response analytics, plus SIEM forwarding, surface risk across the kit.	Available now, wider scope planned	Apply analytics outside the kit.
RA.L3-3.11.4e	Security Solution Rationale	Assists	The Assessment Binder maps NIST SP 800-172 and holds the SSP narrative where the rationale is written.	Available now, wider scope planned	Document the rationale.
RA.L3-3.11.5e	Security Solution Effectiveness	Assists	Current State Compliance Rescan tests each control, and the Assessment Binder keeps the results.	Available now, wider scope planned	Assess effectiveness.
RA.L3-3.11.6e	Supply Chain Risk Response	Records	The Assessment Binder stores the organization's record.	Organization	Assess and monitor supply chain risk.
RA.L3-3.11.7e	Supply Chain Risk Plan	Records	The Assessment Binder stores the organization's record.	Organization	Write and maintain the supply chain risk plan.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
CA.L3-3.12.1e	Penetration Testing	Records	The Assessment Binder stores the organization's record.	Organization	Commission penetration testing.
SC.L3-3.13.4e	Isolation	Performs	The isolated Jump separates privileged sessions from the rest of the network and records each SSH, RDP, and VNC session. The secure enclave isolates its network.	Available now, wider scope planned	Isolate systems outside the enclave.
SI.L3-3.14.1e	Integrity Verification	Assists	The kit checks signatures on product updates, and configuration compliance detects changed settings.	Available now, wider scope planned	Verify other security-critical software.
SI.L3-3.14.3e	Specialized Asset Security	Assists	The kit supports operational technology systems, so they can be brought into scope.	Available now, wider scope planned	Bring other specialized assets into scope.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement Id	CMMC Short Name	Kit Role	How the Kit Meets or Supports It	Availability	What the Organization Does by Hand
SI.L3-3.14.6e	Threat-Guided Intrusion Detection	Assists	Threat indicator feeds drive sign-in blocking, detections, and the attack report.	Available now, wider scope planned	Guide hunting outside the kit.

Permanently Organizational / Not Closed by the Kit

Theme	Availability	Why
Physical Protection (**PE**) facility and visitor controls	Organization	Locks, badges, escorts, and physical access devices are real-world controls.
Personnel Security (**PS**) screening depth	Organization	Background investigations are Human Resources (**HR**) or a screening vendor.
Penetration testing	Organization	A skilled adversary emulation engagement; software is not a pen test.
Threat hunting / Security Operations Center (**SOC**) program	Organization	Analyst staffing and hunting methodology are organizational.
Supply-chain / Advanced Persistent Threat (**APT**) supplier program	Organization	Supplier due diligence is an organizational risk program.
Curriculum fitness for Awareness and Training (**AT**)	Organization	Whether content fits the environment is the customer's and the assessor's call.
Host antimalware / Endpoint Detection and Response (**EDR**)	Organization	Configuration compliance is not a substitute for host malicious-code protection.
System Security Plan (**SSP**) ownership and annual affirmation	Organization	Filing obligations remain with the customer.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Related Documents

Document	Role
CMMC Solutions Price List	SKU dollars and kit contents; points here for the full matrix
CMMC SKU provisioning	Developer entitlement shapes (internal)
CMMC Level 2 enclave kit	Assessor package templates
Customer responsibility matrix	Shared / inherited split for engineers
Requirements coverage CSV	Machine-readable Level 2 coverage tags

Version 1.0.0. US English. ASCII hyphens only.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Analog Informatics Corporation

For more information about Analog Informatics Corporation, please go to analoginfo.com.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Revised October 18, 2026 | analoginfo.com