Kyūdō

SOVEREIGNTY-GRADE AI · GRC

CMMC Level 2 Readiness Checklist

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · READ THIS FIRST

Six things your C3PAO will check before they will book the assessment.

This document is a working operational checklist, not a primer. It assumes your organization handles Controlled Unclassified Information (CUI) on behalf of the Department of Defense (now Department of War) and needs CMMC Level 2 certification under DFARS 252.204-7021 to remain eligible for contract awards. If you are still trying to determine whether CMMC applies to your organization or which level you need, this is the wrong document; start with the CMMC Final Rule (32 CFR Part 170) and the Acquisition Rule (48 CFR), or talk to your contracting officer.

If you are already past that point and you are working toward a C3PAO assessment in the next 90 to 180 days, this checklist walks the gates you must clear, the controls that must be fully met before you walk into the assessment room, and the documentation an assessor will require on day one. Six gates exist. If any of the six is uncertain, the C3PAO will either decline to book the assessment or you will fail it. The gates are listed in priority order — do not work the lower-numbered ones until the higher-numbered ones are solved.

Gate	What it tests
1	CUI scope is defined, defensible, and minimized. The boundary diagram, asset inventory, and data flow diagram exist and match each other.
2	System Security Plan (SSP) is current, accurate, and complete — every one of the 110 practices is documented, with implementation status, responsible party, and reference to the policy or technical control. CA.L2-3.12.4 is non-negotiable; an inadequate SSP fails the assessment by itself.
3	All 5-point and 3-point controls are MET. None can be on a POA&M (with the narrow SC.L2-3.13.11 exception). Failure on any 5- or 3-point control disqualifies you from Conditional Certification.
4	All six non-deferrable 1-point controls are MET: AC.L2-3.1.20, AC.L2-3.1.22, CA.L2-3.12.4, PE.L1-3.10.3, PE.L1-3.10.4, PE.L1-3.10.5. These cannot be POA&M'd regardless of point value.
5	DoDAM (DoD Assessment Methodology) score is at least 88 of 110. Below 88 you cannot achieve even Conditional Certification.
6	POA&M (if any) covers only 1-point items, has specific remediation actions, owners, evidence plans, and completion dates within 180 days.

Sections 1 through 4 of this guide cover the upstream work — scoping, the SSP, the assessment process, scoring. Sections 5 and 6 are the operational checklists, organized by domain (5) and by

the gates above (6). Section 7 is the Microsoft Security stack mapping for organizations on Microsoft 365 GCC High and Azure Government. Section 8 is the Kyūdō continuous-readiness model. Appendices include the complete 110-practice list with point values, the non-POA&M-eligible controls, and a 30/60/90 pre-assessment checklist.

Where the timing pressure comes from

The CMMC Final Rule (32 CFR Part 170) became effective December 16, 2024. The DFARS Acquisition Rule (48 CFR) became effective November 10, 2025, kicking off Phase 1 of a four-phase, three-year rollout. Phase 1 (Nov 2025 – Nov 2026): Level 1 and Level 2 self-assessments at award. Phase 2 (Nov 2026 – Nov 2027): Level 2 C3PAO certifications required at award. Phase 3 (Nov 2027 – Nov 2028): Level 3 DIBCAC assessments added. Phase 4 (from Nov 10, 2028): full implementation across all DoD contracts touching FCI or CUI.

If your organization will need a C3PAO certification by November 10, 2026, you should be in Stage 1 or Stage 2 of the C3PAO assessment process by August 2026. C3PAO capacity is constrained — booking pressure increases sharply in the second half of 2026. Plan for assessment scheduling at least three months before your target award date.

01 · FOUNDATIONS

CMMC Level 2 in 2026.

What CMMC Level 2 actually is

CMMC Level 2 is the certification path for Department of Defense contractors and subcontractors that process, store, or transmit Controlled Unclassified Information (CUI) on non-federal systems. The 110 security requirements at Level 2 are a one-to-one mapping to NIST SP 800-171 Revision 2, which has been a DFARS contractual requirement under DFARS 252.204-7012 since 2017. CMMC adds the formal verification process — self-assessment for non-prioritized acquisitions, third-party C3PAO certification for prioritized acquisitions — plus an annual affirmation of continuous compliance posted in the Supplier Performance Risk System (SPRS).

Three sub-levels of Level 2 exist in practice: Level 2 (Self-Assessment), valid one year, available for non-prioritized acquisitions; Level 2 (C3PAO), valid three years, the default for most prioritized acquisitions; and Level 2 (Conditional), a temporary 180-day status that allows operation while POA&M items are closed before a closeout assessment converts the status to Final.

The 14 control domains and 110 practices

The 110 practices are distributed across 14 domains. Some domains carry far more weight than others — Access Control (22 practices) and System and Communications Protection (16 practices) together represent more than a third of the entire framework. The four densest domains — AC, SC, IA, and AU — are where most assessment findings concentrate. The chart of all 14 follows.

Domain	Code	Practices	Focus area
Access Control	AC	22	Authorized access to systems, accounts, and information; remote access; mobile devices; external systems; CUI flow control.
Awareness and Training	AT	3	Security awareness training and role-based training; insider threat awareness.
Audit and Accountability	AU	9	Audit log creation, review, retention, protection, time synchronization, alerting, and reduction.
Configuration Management	CM	9	Baseline configurations, change control, security impact analysis, least functionality, application allow-listing.

Domain	Code	Practices	Focus area
Identification and Authentication	IA	11	User identification, authentication, MFA, replay-resistant authentication, identifier management, password complexity, FIPS-validated cryptography.
Incident Response	IR	3	Incident handling capability, tracking and reporting, testing the response.
Maintenance	MA	6	Controlled system maintenance, tools, remote maintenance, personnel.
Media Protection	MP	9	Media access, marking, transport, sanitization; portable storage controls.
Personnel Security	PS	2	Screening before access; access protection during termination/transfer.
Physical Protection	PE	6	Physical access authorizations, escort/monitor visitors, audit logs of physical access, alternate work sites.
Risk Assessment	RA	3	Risk assessment, vulnerability scanning, vulnerability remediation.
Security Assessment	CA	4	System Security Plan; security control assessment; POA&M; continuous monitoring.
System and Communications Protection	SC	16	Boundary protection, cryptographic protection, FIPS validation, separation of duties at the network layer, mobile code, VoIP, collaborative computing devices.
System and Information Integrity	SI	7	Flaw remediation, malicious code protection, security alert response, monitoring, intrusion detection.

Source — NIST SP 800-171 Rev 2; CMMC 2.0 model documentation. Practice counts are authoritative.

Why Rev 2, not Rev 3

NIST published SP 800-171 Revision 3 in May 2024, which restructures the framework to 97 requirements (consolidating from 110). However, the DoD has explicitly stated that CMMC Level 2 assessments continue to be conducted against Revision 2 until further rulemaking. As of April 2026, every C3PAO assessment uses the Rev 2 control set and the NIST SP 800-171A assessment methodology. Plan against Rev 2; the eventual transition to Rev 3 will be

communicated through the rulemaking process and is not expected before late 2027 at the earliest.

Self-assessment vs. C3PAO assessment

Whether your organization needs a self-assessment or a C3PAO assessment depends on the contract, not on your preference. The contracting officer determines the requirement and includes the appropriate clause (DFARS 252.204-7021) in the solicitation. Three patterns exist.

Path	Validity	Conducted by	Typical contract type
Level 2 (Self)	1 year	Senior official of the Organization Seeking Assessment (OSA), submitted to SPRS	Non-prioritized acquisitions — lower-sensitivity CUI; primarily Phase 1 contracts during the rollout.
Level 2 (C3PAO)	3 years	Authorized CMMC Third-Party Assessment Organization	Prioritized acquisitions — most CUI-handling contracts; the default after Phase 2 begins November 10, 2026.
Level 2 (Conditional)	180 days	C3PAO at initial assessment; C3PAO performs closeout assessment within the 180-day window	Any organization that scored ≥88 on initial assessment and has eligible 1-point items on POA&M; closeout converts to Final.

If your organization holds active or expected DoD contracts that touch CUI and you do not yet know which path applies, work with your contracting officer to determine the required certification level. Subcontractors must also comply at the level required by the prime contractor's contract — prime contractors are responsible for ensuring subcontractor compliance throughout the supply chain.

The annual affirmation

CMMC certification, whether self-assessment or C3PAO, is not a one-time event. DFARS 252.204-7021 requires an affirming official — a senior official of the contractor designated for this purpose — to file an annual affirmation in SPRS attesting to continuous compliance. The affirmation is per covered information system; each system that processes, stores, or transmits FCI or CUI in performance of the contract has its own CMMC unique identifier (UID) in SPRS, and each requires an annual affirmation.

If continuous compliance lapses during the year, the contractor is exposed to False Claims Act risk if the lapse is not disclosed. The Department of Justice has been increasingly active here since 2024, with several cases against contractors who maintained current CMMC status in SPRS while failing to maintain compliance. The annual affirmation is a legal commitment, not a paperwork formality.

02 · SCOPE

Define the CUI boundary aggressively. Minimize it before everything else.

The single most consequential decision you make in CMMC preparation is where you draw the CUI boundary. Every system inside the boundary must implement the 110 practices. Every system outside is out of scope. The boundary determines the cost, complexity, and timeline of the entire program.

Most CMMC failures trace to scope decisions made early. Organizations that scope their entire enterprise into the boundary spend three to four times more on implementation, take twelve months longer to certify, and produce SSPs that are difficult to maintain. Organizations that scope a discrete enclave — a specific environment that handles CUI, with controlled flows in and out — reduce the implementation surface to something tractable. Both approaches are valid; the first is rarely the right answer.

Asset categories

CMMC scoping uses five asset categories. Each category has a specific obligation under the assessment. Knowing the category of every asset in your environment is foundational — the C3PAO will sample assets across categories during the assessment.

Category	Definition	Assessment obligation
CUI Assets	Process, store, or transmit CUI; or provide security protections for systems that do.	Fully assessed against all applicable practices.
Security Protection Assets	Provide security functions or capabilities to the contractor's CUI environment, regardless of whether they process CUI directly (firewalls, SIEM, MFA brokers, vulnerability scanners).	Fully assessed against all applicable practices.
Contractor Risk Managed Assets	Capable of, but not intended to, process, store, or transmit CUI; the contractor manages the risk through policy, configuration, and monitoring.	Documented in the SSP; not directly assessed unless the C3PAO determines they are not adequately

Category	Definition	Assessment obligation
		controlled.
Specialized Assets	OT, IoT, government-furnished equipment, restricted information systems, test equipment.	Documented in the SSP; risk-managed; not directly assessed.
Out-of-Scope Assets	Cannot process, store, or transmit CUI by design (physical or logical separation, no connectivity to CUI).	Documented in the SSP as out of scope; not assessed.

Source — CMMC Assessment Scope Guide for Level 2 (DoD CIO, current edition).

Three artifacts the assessor reads first

The C3PAO will request three scoping artifacts at the start of the engagement. These artifacts must exist, must be current, and must be internally consistent — if the boundary diagram shows three subnets and the asset inventory shows assets in five subnets, that is a Day 1 finding.

Artifact	What it must contain
Network boundary diagram	All systems inside the CUI boundary; all systems providing security protection; all enclaves; all interconnections to internal and external systems; the points where CUI enters or leaves the boundary.
CUI asset inventory	Every CUI Asset and Security Protection Asset by hostname, IP, function, owner, and category. Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets in separate sheets/tabs with rationale. Inventory must reconcile to the boundary diagram.
CUI data flow diagram	How CUI enters the boundary (email, file transfer, customer portal, contract awards), where it is stored (file shares, databases, document management systems), how it moves between systems within the boundary, and how it exits (deliverables to the government, deletion, archive).

Scope minimization patterns that work

Three architectural patterns reduce scope materially. None is appropriate for every organization, but at least one usually applies.

1. Enclave architecture. Build a discrete CUI enclave — a separate subscription, tenant, or environment — that handles all CUI processing. Use Microsoft 365 GCC High plus Azure Government for organizations on the Microsoft stack; the FedRAMP Moderate Equivalent or High accreditation of those services is what makes them suitable for CUI. Production CUI work happens in the enclave; the corporate environment stays out of scope.
2. Email separation. Many small contractors only handle CUI in email and file transfers. Routing all CUI-bearing email through a separately-licensed CUI mail platform (e.g., PreVeil with end-to-end encryption, GCC High Exchange Online) keeps the corporate email environment out of scope. Outlook itself can remain on commercial Microsoft 365.
3. Engineering enclave. For contractors performing CUI work in CAD, simulation, or other engineering tools, run those tools in dedicated workstations or virtual desktops within the CUI enclave. Day-to-day office work happens in commercial Microsoft 365; CUI work happens via VDI in the enclave.

FedRAMP Moderate Equivalent or High is required for cloud services in scope

Per DFARS 252.204-7012(b)(2)(ii)(D), any cloud service provider that processes, stores, or transmits CUI must meet FedRAMP Moderate Equivalent (with attestation by an accredited 3PAO) or be FedRAMP Moderate or High authorized. Microsoft 365 GCC High and Azure Government are authorized at FedRAMP High; Microsoft 365 Commercial is not authorized at FedRAMP Moderate, and Microsoft 365 GCC is at Moderate but explicitly not approved for CUI subject to ITAR or specific export-controlled CUI categories. Choose the tenant tier carefully — retrofitting from Commercial to GCC High mid-program costs months and hundreds of thousands of dollars.

If you operate AWS workloads handling CUI, AWS GovCloud is the equivalent FedRAMP-High path. For Google, Google Workspace Enterprise has FedRAMP Moderate Equivalent attestations; consult the FedRAMP Marketplace for current authorizations.

03 · SYSTEM SECURITY PLAN

The SSP is the assessment. Get it right or fail.

The System Security Plan is the document the C3PAO assessor reads before they walk into your environment, returns to throughout fieldwork, and references in the assessment report. It is the master artifact. CA.L2-3.12.4 — 'Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems' — is one of the six 1-point controls that cannot be POA&M'd. An inadequate SSP fails the assessment by itself, regardless of how well the technical controls are implemented.

Most organizations underestimate the SSP. The version that survived the early DFARS 7012 self-attestation period — a few dozen pages, one paragraph per control family, references to corporate policies — is not what a C3PAO will accept. CMMC SSPs are typically 150 to 400 pages, with each of the 110 practices addressed individually with an implementation description specific enough that an assessor could verify it without further inquiry.

What the SSP must contain

NIST SP 800-18 (Guide for Developing Security Plans for Federal Information Systems) defines the structure. CMMC adds further specificity through the assessment methodology in NIST SP 800-171A. The SSP must contain at minimum:

Section	What it documents
System identification	System name, owner, identification number, status (operational/under development), system type, environment (cloud/on-prem/hybrid).
System operational status	Operational, under development, undergoing major modification.
Information system type	Major application, general support system.
General description and purpose	What the system does, business function, who uses it.
System environment	Hardware, software, firmware. Cloud service providers, FedRAMP authorization status of each. Network topology with the boundary diagram embedded or referenced.
System interconnections	Every interconnection to other systems, with the type of CUI exchanged, the protocol, the security controls protecting the connection, and the agreement (ISA/MOU) that governs it.

Section	What it documents
Applicable laws, regulations, policies, standards	DFARS 7012, the CMMC Final Rule, applicable CUI categories with their specific safeguarding requirements, organizational policies.
Information system security plan responsibility	System owner, ISSO, ISSM, affirming official.
Implementation of each of the 110 practices	For each practice: implementation status (Implemented, Partially Implemented, Planned, Not Applicable), responsible party, description of implementation specific to your environment, references to supporting policies and procedures.
Authorization and approval	Signature of the affirming official; date; review cadence.

How to write a defensible practice description

The single biggest SSP failure mode is generic practice descriptions that simply paraphrase the NIST SP 800-171 control text. ‘We control access to organizational systems’ is not an implementation description. The assessor needs to know how, with what tools, with what evidence.

Weak SSP entry	Strong SSP entry
AC.L2-3.1.1 — Limit access to authorized users. Implementation: We use Active Directory to manage user accounts and group memberships.	AC.L2-3.1.1 — Limit access to authorized users. Implementation: User accounts and access entitlements are managed in Microsoft Entra ID (GCC High tenant). New accounts are provisioned via the HRIS-to-Entra ID joiner workflow (procedure SEC-PROC-IAM-001) within 1 business day of HRIS hire date. Access entitlements are managed through Entra ID Governance access packages, with approval workflows requiring manager and CUI-system owner approval for any access package granting CUI system access. Conditional Access policies (Policy IDs CA-001 through CA-014, exported quarterly to the SSP appendix) enforce device compliance and MFA for all access. Quarterly access reviews are conducted via Entra ID Governance; review reports are retained in SharePoint at /CUI-Compliance/Access-

Weak SSP entry	Strong SSP entry
	Reviews.

The strong entry tells the assessor exactly what to look for: where the policies live, where to pull evidence, how the operational mechanism works. The assessor can verify the entry against the artifacts; the weak entry leaves the assessor with no path to verification, which becomes a finding.

SSP maintenance during the cycle

The SSP is not a one-time deliverable. NIST SP 800-171 requires periodic update; CMMC reinforces this through the annual affirmation. Practice CM.L2-3.4.3 (‘Track, review, approve or disapprove, and audit changes to organizational systems’) connects to SSP maintenance — every change to the in-scope environment that affects security must be reflected in the SSP. The SSP cannot lag the environment; an SSP that is out of date with the environment will be flagged at the C3PAO assessment, the annual affirmation, or both.

Establish an SSP update cadence: quarterly review at minimum, plus event-driven updates for any material change to the environment. Each version should have a changelog at the front, the affirming official's approval signature, and the date. The C3PAO will compare the most recent version to the prior version and look for evidence the SSP is being maintained, not just rebuilt before the assessment.

04 · SCORING AND POA&M

88 to pass. 110 to be done. 180 days to close.

CMMC Level 2 uses the DoD Assessment Methodology (DoDAM) scoring system. Each of the 110 practices is worth 1, 3, or 5 points. The maximum possible score is 110. The minimum to achieve Conditional Certification is 88 — 80% of the total. To achieve Final Certification, all 110 points must be MET; any deficiencies must be closed within the 180-day Conditional window.

Point values — what counts and what does not

Of the 110 practices, the distribution by point value drives the practical math of pre-assessment readiness. Most of the score comes from a relatively small number of high-value controls.

Point value	Approximate count	What they cover
5 points	~14 practices	The most critical controls: MFA (IA.L2-3.5.3), FIPS-validated cryptography (IA.L2-3.5.10, SC.L2-3.13.11), boundary protection (SC.L2-3.13.1), encryption of CUI at rest and in transit, malicious code protection. Failure on any 5-point control disqualifies you from Conditional Certification.
3 points	~48 practices	High-value controls: account management, separation of duties, least privilege, audit logging configuration, baseline configurations, vulnerability management, incident response. Failure on any 3-point control disqualifies you from Conditional Certification (with the narrow SC.L2-3.13.11 partial-credit exception).
1 point	~48 practices	Lower-impact controls. Most can be POA&M'd if the organization has scored ≥88 overall. Six specific 1-point controls cannot (see below).

Counts approximate; refer to the official DoDAM scoring methodology for authoritative point assignments per practice. SC.L2-3.13.11 (CUI encryption) is the one 5-point control that may be partially credited (3 points) and POA&M'd if encryption is present but not FIPS-validated.

The six 1-point controls that cannot be POA&M'd

Independent of point value, six specific 1-point controls are explicitly excluded from POA&M eligibility under 32 CFR §170.21(a)(2). If any of these is NOT MET at the time of assessment, Conditional Certification cannot be granted regardless of overall score. These six should be at the top of any pre-assessment readiness review.

Practice	Title	What it requires
AC.L2-3.1.20	External Connections	Verify and control/limit connections to and use of external systems. Documented external system connections, security review of each, formal approval.
AC.L2-3.1.22	Public Information	Control CUI posted or processed on publicly accessible systems. Procedure for public-facing content review; separation of CUI from public-facing systems.
CA.L2-3.12.4	System Security Plan	Develop, document, and periodically update system security plans that describe system boundaries, environments, control implementations, and interconnections. The SSP itself.
PE.L1-3.10.3	Escort Visitors	Escort visitors and monitor visitor activity. Visitor sign-in procedure, badge or visual identification, continuous escort policy, review of visitor logs.
PE.L1-3.10.4	Physical Access Logs	Maintain audit logs of physical access. Visitor logs, badge access logs, retention policy, review cadence.
PE.L1-3.10.5	Manage Physical Access Devices	Control and manage physical access devices. Inventory of badges, keys, and access cards; lifecycle management; revocation upon termination or loss.

Note that PE.L1-3.10.3, PE.L1-3.10.4, and PE.L1-3.10.5 are CMMC Level 1 practices that are also part of Level 2. They appear straightforward but are common failure points for organizations that have not formalized physical-access procedures even though those procedures are clearly within the contractor's control.

Conditional Certification mechanics

If your organization scores ≥88, has met all 5-point and 3-point practices, has met the six non-POA&M-eligible 1-point controls, and has remaining gaps only on POA&M-eligible 1-point items, you qualify for Conditional Level 2 Certification. The window from the date of the Conditional Status determination is 180 days. During that window, you must close every POA&M item and undergo a closeout assessment by the same C3PAO that performed the initial assessment. The closeout assessment evaluates only the items that were on the POA&M; if every item is now MET, the certification converts from Conditional to Final.

If the 180-day window expires without a successful closeout, the Conditional status expires. The certification is lost; the organization must restart the assessment process. There is no extension mechanism. Plan POA&M items aggressively — list only items you are highly confident you can close in 90 days, leaving 90 days of buffer for the closeout assessment scheduling and the C3PAO's review.

How to write a defensible POA&M entry

Each POA&M item must contain: the specific practice that is NOT MET, a clear description of the gap, the remediation actions required, the responsible party, the resources required, the milestone dates, the expected completion date, and the evidence that will be produced when the item is closed. Vague entries are flagged by the C3PAO and may invalidate the POA&M.

Weak POA&M entry	Strong POA&M entry
AC.L2-3.1.21: Limit use of portable storage. Plan: Implement controls. Owner: IT. Date: ASAP.	AC.L2-3.1.21 — Limit Use of Portable Storage. Gap: Removable storage device controls are configured on workstation endpoints (Intune compliance policy DEV-COMP-001) but not enforced on engineering Linux workstations. Remediation: (1) Deploy Microsoft Defender for Endpoint device control policy to engineering Linux endpoints (10 endpoints affected) by 2026-05-15; (2) Update SSP Section 3.1.21 to reflect the expanded coverage by 2026-05-22; (3) Conduct internal verification by IT Security Lead by 2026-05-29. Owner: J. Smith, IT Security Lead. Resources: Defender for Endpoint Linux licenses (already provisioned). Evidence at closeout: Defender for Endpoint policy assignment report showing 100% coverage; updated SSP excerpt; verification record.

What an assessor looks for, by domain.

This is the operational checklist. Each domain section lists the highest-frequency assessment focus areas — not all 110 practices, but the practices most likely to surface findings, plus the practices an assessor will exercise on Day 1. For each focus area, the checklist names what the assessor will ask for, what evidence satisfies the request, and — where a Microsoft signal source is the primary evidence — names the specific Microsoft tool that produces it.

Use this section as a working document. The pre-assessment review should walk every focus area in order, mark each as Ready / Gap / Not Applicable, and assign owners for any Gap finding.

AC — Access Control (22 practices)

Largest domain by practice count. Highest concentration of 5- and 3-point controls. Where most assessment time will be spent. Includes the two non-POA&M-eligible 1-point controls AC.L2-3.1.20 (External Connections) and AC.L2-3.1.22 (Public Information).

Focus areas

- AC.L2-3.1.1–3.1.2 (account management, transaction enforcement) — user inventory exported from Entra ID with role assignments, group memberships, last sign-in. Service principal inventory. Privileged account list with justification per account.
- AC.L2-3.1.5 (least privilege) — evidence of access reviews on a documented cadence. Entra ID Governance access reviews exports; manager and CUI-owner approval records.
- AC.L2-3.1.7 (privileged functions) — Entra Privileged Identity Management activation logs; documented evidence that privileged role activations require justification and approval.
- AC.L2-3.1.12–3.1.16 (remote access, wireless, mobile) — Conditional Access policies enforcing MFA and device compliance for remote access; documented procedures for mobile device enrollment via Microsoft Intune.
- AC.L2-3.1.20 (external connections) — NON-POA&M-ELIGIBLE — documented inventory of external system connections, security review documentation per connection, formal approval records.
- AC.L2-3.1.21 (portable storage) — Defender for Endpoint device control policies blocking unauthorized USB mass storage; Intune compliance policies.
- AC.L2-3.1.22 (public information) — NON-POA&M-ELIGIBLE — documented public-content review procedure; evidence of CUI separation from public-facing systems; sample public website review records.

AT — Awareness and Training (3 practices)

Small domain, but findings are common because training records are often incomplete.

Focus areas

- AT.L2-3.2.1–3.2.2 (awareness training, role-based training) — LMS training records per individual; CUI-handling-specific training for personnel with CUI access; refresher training cadence (typically annual).
- AT.L2-3.2.3 (insider threat awareness) — documented insider threat awareness module delivered to all personnel; completion records.

AU — Audit and Accountability (9 practices)

Audit logging is a Day 1 assessor focus. The C3PAO will pull sample logs from in-scope systems and verify they contain the required content elements.

Focus areas

- AU.L2-3.3.1–3.3.2 (audit log content, user identification) — logs covering successful and unsuccessful events, user ID, timestamp, action, source, success/failure. Microsoft Sentinel ingestion of Entra ID audit logs, Microsoft 365 Unified Audit Log, Azure Activity Log, Defender XDR investigations.
- AU.L2-3.3.4 (audit failure response) — alerts when audit logging fails; documented response procedure.
- AU.L2-3.3.5 (review and analysis) — documented log review cadence; evidence of analyst review of alerts and incidents in Sentinel.
- AU.L2-3.3.6 (reduction and reporting) — Sentinel workbooks; scheduled reports to security leadership.
- AU.L2-3.3.7 (clock synchronization) — NTP or Azure-managed time sync configuration evidence; NIST-traceable time source.
- AU.L2-3.3.8–3.3.9 (log protection, restricted access) — immutable storage configuration (Azure Storage immutable blobs); restricted access to logs; documented review of who has log access.

CM — Configuration Management (9 practices)

Configuration management is where the SSP environment description meets the technical reality. Drift between the documented baseline and the actual configuration is a common finding.

Focus areas

- CM.L2-3.4.1–3.4.2 (baseline configurations, security settings) — documented baselines per system type; Azure Policy compliance state demonstrating baseline enforcement; Intune device configuration profiles for endpoints; Defender for Cloud regulatory compliance dashboard.
- CM.L2-3.4.3 (change management) — documented change management procedure; evidence of approvals through Azure DevOps or ServiceNow; pipeline run records with approver evidence.

- CM.L2-3.4.5–3.4.6 (access restrictions for change, least functionality) — RBAC scoping for change-affecting roles; documented services and ports baseline; Defender for Cloud network recommendations.
- CM.L2-3.4.7 (nonessential functions) — documented services-disabled list; configuration evidence.
- CM.L2-3.4.8 (application allow-listing) — Microsoft Defender Application Control or AppLocker policies enforcing allow-listing; evidence of the allow-list and recent updates.
- CM.L2-3.4.9 (user-installed software) — Intune managed apps configuration restricting non-administrative software installation; exception process documented.

IA — Identification and Authentication (11 practices)

This is where MFA, FIPS-validated cryptography, and password policies live. IA.L2-3.5.3 (MFA) is one of the highest-impact 5-point controls — a missing or partial implementation here is grounds for assessment failure.

Focus areas

- IA.L2-3.5.1–3.5.2 (user identification, authentication) — Entra ID user identity inventory; service principal identity inventory; documented identity proofing procedures.
- IA.L2-3.5.3 (MFA) — 5-POINT — Conditional Access policies enforcing MFA for ALL privileged accounts and ALL access to CUI systems. Sign-in logs filtered by authentication method showing 100% MFA compliance for in-scope users. FIDO2 / Windows Hello / phishing-resistant methods preferred over SMS.
- IA.L2-3.5.4 (replay-resistant authentication) — Conditional Access enforcement of phishing-resistant MFA for privileged access; documented authentication method policy.
- IA.L2-3.5.5–3.5.6 (identifier management, identifier reuse) — Entra ID identifier lifecycle; documented procedure for handling separated personnel.
- IA.L2-3.5.7–3.5.9 (password complexity, history, prohibition of password reuse) — Entra ID password protection; documented password policy aligned to NIST SP 800-63B current guidance; evidence of enforcement.
- IA.L2-3.5.10 (FIPS cryptography for authenticators) — 5-POINT — evidence that authentication uses FIPS-validated cryptographic modules. For Microsoft cloud, this is satisfied by Entra ID and Windows / Linux GCC High; document the FIPS validation references.
- IA.L2-3.5.11 (authentication feedback) — password input is obscured; authentication failure messages do not reveal whether the username or password was incorrect.

IR — Incident Response (3 practices)

Small domain, high stakes. The assessor will request the incident response plan and evidence of testing within the audit period.

Focus areas

- IR.L2-3.6.1 (incident-handling capability) — documented incident response plan; named IR team with defined roles; integration with Microsoft Sentinel SOAR playbooks.
- IR.L2-3.6.2 (track, document, report) — Sentinel incident records; evidence of incident reporting to designated authorities (DC3, FedRAMP, customer per contract); DFARS 7012 72-hour reporting requirement.
- IR.L2-3.6.3 (test the response) — tabletop exercise records within the past 12 months; live-fire or simulation exercise records (preferred); after-action reports with documented improvements.

MA — Maintenance (6 practices)

Maintenance practices are commonly under-implemented in cloud-first organizations. The assessor will ask how maintenance activities are controlled, who performs them, and what tools they use.

Focus areas

- MA.L2-3.7.1–3.7.2 (controlled maintenance, controls on tools) — documented maintenance procedure; approved tool list; evidence of authorization for each maintenance event.
- MA.L2-3.7.4 (media used for maintenance) — sanitization of media before reconnection.
- MA.L2-3.7.5 (remote maintenance) — MFA for remote maintenance; documented session controls; evidence of approval per session.
- MA.L2-3.7.6 (personnel) — background checks for maintenance personnel; supervised access for personnel without authorization.

MP — Media Protection (9 practices)

Media protection covers both physical media (drives, paper, removable storage) and digital media. The assessor will request the media inventory, transport procedures, and sanitization records.

Focus areas

- MP.L2-3.8.1–3.8.2 (media access, marking) — documented marking procedure for CUI on media; evidence of marking on actual media in scope.
- MP.L2-3.8.3 (media sanitization) — documented sanitization procedure aligned to NIST SP 800-88; certificates of destruction for physical media; evidence for digital sanitization.
- MP.L2-3.8.5–3.8.6 (media transport, cryptographic protection) — FIPS-validated encryption on media in transit; chain of custody for physical transport.
- MP.L2-3.8.7–3.8.8 (removable media use, prohibit unauthorized media) — Defender for Endpoint device control or equivalent; documented exception process.
- MP.L2-3.8.9 (backup media protection) — backup encryption (Azure Backup with customer-managed keys); access controls on backups; documented retention.

PS — Personnel Security (2 practices)

Smallest domain. Both practices are typically straightforward but require documentation.

Focus areas

- PS.L2-3.9.1 (screening) — documented background check procedure; evidence of background checks for personnel with access to CUI; check-on-hire and renewal cadence per contract requirement.
- PS.L2-3.9.2 (terminate or transfer access) — documented separation procedure; evidence of access removal within defined SLA after termination; HRIS-to-Entra deprovisioning workflow.

PE — Physical Protection (6 practices)

Includes three of the six non-POA&M-eligible 1-point controls: PE.L1-3.10.3 (escort visitors), PE.L1-3.10.4 (physical access logs), PE.L1-3.10.5 (manage physical access devices). All are mandatory at the time of assessment.

Focus areas

- PE.L1-3.10.1 (physical access authorizations) — documented authorization process; access list reviewed periodically.
- PE.L1-3.10.3 (escort visitors) — NON-POA&M-ELIGIBLE — visitor sign-in procedure, badging, continuous escort policy, evidence of consistent enforcement (visitor logs).
- PE.L1-3.10.4 (audit logs of physical access) — NON-POA&M-ELIGIBLE — visitor logs, badge access logs, retention policy, periodic review records.
- PE.L1-3.10.5 (manage physical access devices) — NON-POA&M-ELIGIBLE — inventory of badges/keys/access cards, lifecycle management, revocation evidence on termination.
- PE.L2-3.10.2 (monitor physical access) — CCTV or guard monitoring for sensitive areas; retention policy on recordings.
- PE.L2-3.10.6 (alternate work sites) — documented remote-work policy; evidence of controls when CUI is processed off-premises (encryption, VPN, MDM).

RA — Risk Assessment (3 practices)

Vulnerability management is the most-tested area within RA. The assessor will request the vulnerability scanning evidence and remediation timeline.

Focus areas

- RA.L2-3.11.1 (risk assessment) — documented risk assessment methodology; current risk register reviewed within the last 12 months.
- RA.L2-3.11.2 (vulnerability scanning) — Microsoft Defender Vulnerability Management findings; Defender for Cloud recommendations; documented scan cadence (typically monthly minimum); evidence of authenticated scans.
- RA.L2-3.11.3 (vulnerability remediation) — documented remediation SLAs by severity (e.g., 30 days for critical, 90 days for high); evidence of remediation history.

CA — Security Assessment (4 practices)

Includes CA.L2-3.12.4 (the SSP), one of the six non-POA&M-eligible 1-point controls. Also covers internal assessment cadence and continuous monitoring.

Focus areas

- CA.L2-3.12.1–3.12.2 (control assessment, POA&M) — documented internal assessment methodology aligned to NIST SP 800-171A; current internal assessment results; current operational POA&M.
- CA.L2-3.12.3 (continuous monitoring) — documented continuous monitoring strategy; ongoing evidence of control monitoring (Sentinel analytics, Defender for Cloud Secure Score trend).
- CA.L2-3.12.4 (SSP) — NON-POA&M-ELIGIBLE — the SSP itself; current, complete, accurate, approved by the affirming official.

SC — System and Communications Protection (16 practices)

Second-largest domain. Includes multiple 5-point controls (boundary protection, FIPS encryption, transmission protection). FIPS-validated cryptography is a recurring assessor focus — the validation reference must be specific.

Focus areas

- SC.L2-3.13.1–3.13.2 (boundary protection, separation of CUI) — 5-POINT-RANGE — boundary diagram; firewall rule exports; private endpoint topology; documented DMZ architecture.
- SC.L2-3.13.5 (publicly accessible system components) — separation between public-facing and internal systems; documented architecture review.
- SC.L2-3.13.8 (cryptographic protection in transit) — 5-POINT — TLS 1.2+ enforcement evidence; FIPS-validated cipher suites; certificate inventory and rotation.
- SC.L2-3.13.10 (key establishment and management) — Azure Key Vault key inventory; rotation policy; access controls.
- SC.L2-3.13.11 (CUI encryption) — 5-POINT (POA&M-ELIGIBLE if encryption present but not FIPS-validated, then 3 points) — FIPS 140-2 or 140-3 validated cryptographic module evidence per encryption use case; CMVP certificate references.
- SC.L2-3.13.16 (data-at-rest protection) — Azure Storage encryption configuration; Azure SQL TDE; customer-managed keys in Azure Key Vault; M365 sensitivity labels with encryption.

SI — System and Information Integrity (7 practices)

Patch management and malicious code protection are heavily tested. The assessor will pull patch records and verify endpoint protection deployment across the environment.

Focus areas

- SI.L2-3.14.1 (flaw remediation) — documented patch management procedure; SLA by severity; evidence of timely patching from Defender Vulnerability Management or equivalent.

- SI.L2-3.14.2–3.14.3 (malicious code protection, security alerts) — 5-POINT-RANGE — Microsoft Defender for Endpoint and Defender for Office 365 deployment evidence; alert handling records.
- SI.L2-3.14.4–3.14.5 (system monitoring, identifying unauthorized use) — Sentinel detection coverage by MITRE ATT&CK; analytic rule definitions.
- SI.L2-3.14.6–3.14.7 (security alert response, identify unauthorized use) — documented alert response procedure; evidence of alert handling within defined SLAs.

06 · THE SIX GATES

Pre-assessment gates, in priority order.

If you are 30 to 90 days from a C3PAO assessment, walk these gates in order. Each gate must be cleared before the next becomes meaningful. The order matters — working downstream gates while upstream gates remain open is the single most common mistake.

Gate 1 — CUI scope is defined, defensible, and minimized

Test

- Boundary diagram exists, is current within 30 days, names every system inside the CUI boundary.
- CUI asset inventory enumerates every CUI Asset and Security Protection Asset by hostname/IP/owner/category.
- CUI data flow diagram shows how CUI enters, moves through, and exits the boundary.
- All three artifacts reconcile to each other — no asset listed in one but absent from another.
- Cloud services in scope are FedRAMP Moderate Equivalent (with attestation) or FedRAMP Moderate/High authorized.

If Gate 1 is not clear

Stop. Do not proceed to Gate 2. Scope decisions made downstream of an unclear boundary will be invalidated when the boundary is finalized. Re-scope first.

Gate 2 — SSP is current, complete, and accurate

Test

- All 110 practices are documented individually in the SSP, with implementation status, responsible party, and a description specific enough to be verified.
- System environment description matches the network topology; no inconsistencies between SSP and infrastructure-as-code or configuration.
- All system interconnections are documented with type of CUI exchanged, security controls, and governing agreement.
- Affirming official approval signature is current — within the last quarter.
- Changelog reflects ongoing maintenance — the SSP is not a one-time deliverable rebuilt for the assessment.

If Gate 2 is not clear

Stop. The SSP is one of the six non-POA&M-eligible controls (CA.L2-3.12.4). An incomplete or inaccurate SSP fails the assessment regardless of how well technical controls are implemented. Plan a 30-to-60-day SSP completion sprint before proceeding.

Gate 3 — All 5- and 3-point controls are MET

Test

- All ~14 5-point controls are MET. MFA, FIPS-validated cryptography, boundary protection, malicious code protection, encryption at rest and in transit.
- All ~48 3-point controls are MET. Account management, separation of duties, audit logging configuration, baseline configurations, vulnerability management, incident response.
- Exception: SC.L2-3.13.11 may be partially credited if encryption is present but not FIPS-validated — only this one 5-point exception, and only with FIPS gap as the specific deficiency.

If Gate 3 is not clear

Conditional Certification is impossible. Either complete the missing implementations before the assessment, or postpone the assessment. POA&Ms cannot bridge a 5- or 3-point gap.

Gate 4 — The six non-POA&M-eligible 1-point controls are MET

Test

- AC.L2-3.1.20 — external connections inventoried, reviewed, approved.
- AC.L2-3.1.22 — public information separated from CUI; review procedure operational.
- CA.L2-3.12.4 — SSP complete, accurate, current. (Tested in Gate 2.)
- PE.L1-3.10.3 — visitor escort and monitoring policy in force; visitor logs current.
- PE.L1-3.10.4 — physical access logs maintained and reviewed.
- PE.L1-3.10.5 — physical access devices inventoried, lifecycle managed, revocation on termination.

If Gate 4 is not clear

Conditional Certification is impossible regardless of overall score. These six are explicit 32 CFR §170.21(a)(2) exclusions from POA&M eligibility. Address before the assessment.

Gate 5 — DoDAM score is at least 88

Test

- Self-assessment using NIST SP 800-171A methodology produces a score of ≥88.
- Score is recorded in SPRS for the relevant CMMC unique identifier (UID).
- Score reconciles to the SSP — NOT MET findings in the self-assessment correspond to POA&M items.

If Gate 5 is not clear

Below 88, even Conditional Certification is unavailable. Identify the specific gaps producing the score below 88, prioritize remediation of 5- and 3-point gaps first, and re-run the assessment when the score is at or above 88.

Gate 6 — POA&M items are well-formed and 180-day-closeable

Test

- Every POA&M item is for a 1-point practice (with the SC.L2-3.13.11 partial-credit exception only).
- None of the six non-POA&M-eligible 1-point controls is on the POA&M.
- Each POA&M item has: specific gap description, remediation actions, responsible party, resources, milestones, expected closure date ≤90 days, evidence at closeout.
- Total POA&M item count is small — ideally fewer than 10 — and the closure plan is realistic in 90 days, leaving 90 days of buffer for the closeout assessment.

If Gate 6 is not clear

Either the POA&M needs cleanup before the assessment, or specific items need to be remediated before assessment so they can be MET rather than NOT MET. A POA&M with too many items, or items that are not credibly closeable in 180 days, signals to the C3PAO that the organization is not actually ready for assessment.

07 · MICROSOFT SECURITY STACK MAPPING

From CMMC practice to Microsoft signal source.

This section maps the highest-frequency CMMC Level 2 practices to specific Microsoft Security stack signal sources for organizations operating in Microsoft 365 GCC High and Azure Government. The mapping covers the practices where Microsoft-native evidence is the most direct and most defensible. Where additional sources exist (third-party MDM, code-scanning tools, separate ticketing systems), they become supplementary evidence for the same practices.

> **Tenant tier matters**
> Microsoft 365 GCC High and Azure Government are FedRAMP High authorized and approved for CUI including ITAR-controlled categories. Microsoft 365 Commercial is NOT authorized at FedRAMP Moderate. Microsoft 365 GCC is FedRAMP Moderate but NOT approved for ITAR or specific export-controlled CUI categories. If you are bidding on contracts with CUI subject to ITAR, deploy in GCC High plus Azure Government from the start — retrofitting from Commercial or GCC mid-program is a multi-quarter, six-figure undertaking.

Identity and access (AC, IA)

Practice	Primary Microsoft signal source
AC.L2-3.1.1–3.1.2 (account management)	Microsoft Entra ID user inventory; service principal inventory; managed identity inventory; HRIS-to-Entra provisioning logs.
AC.L2-3.1.5 (least privilege)	Entra ID Governance access reviews; role assignment exports; access package definitions.
AC.L2-3.1.7 (privileged functions)	Entra Privileged Identity Management activation logs; role catalog; PIM access reviews.
AC.L2-3.1.12–16 (remote/wireless/mobile)	Conditional Access policy export; Microsoft Intune compliance policies; Defender for Cloud Apps remote access governance.
IA.L2-3.5.3 (MFA) — 5-point	Conditional Access MFA enforcement policies; sign-in logs filtered by authentication method showing 100% MFA compliance for in-scope users; Authentication Methods activity report.
IA.L2-3.5.4	Phishing-resistant MFA enforcement (FIDO2, Windows Hello, certificate-

Practice	Primary Microsoft signal source
(replay-resistant authentication)	based); Conditional Access policy targeting privileged accounts.
IA.L2-3.5.10 (FIPS cryptography for authenticators) — 5-point	Microsoft Entra ID FIPS validation references; Windows / Linux GCC High FIPS mode configuration; CMVP certificate references.

Audit logging and monitoring (AU, SI)

Practice	Primary Microsoft signal source
AU.L2-3.3.1–3.3.2 (audit log content)	Microsoft Sentinel ingestion of: Entra ID audit and sign-in logs, M365 Unified Audit Log, Azure Activity Log, Defender XDR investigations. Log retention policy aligned to contractual requirements (typically 1 year minimum).
AU.L2-3.3.4 (audit failure response)	Sentinel analytic rules detecting log ingestion failures; alerting to SOC; documented response procedure.
AU.L2-3.3.5 (review and analysis)	Documented SOC log review cadence; Sentinel workbooks; analyst incident records.
AU.L2-3.3.7 (clock synchronization)	Azure-managed time sync; documented NTP source; NIST-traceable time evidence.
AU.L2-3.3.8–9 (log protection)	Azure Storage immutable blob retention for log archives; restricted RBAC on log workspaces; documented log access list.
SI.L2-3.14.2–3 (malicious code protection) — 5-point range	Microsoft Defender for Endpoint deployment status; Defender for Office 365 mail flow protection; Defender Antivirus configuration baselines; alert handling records.
SI.L2-3.14.4–5 (system monitoring)	Sentinel detection coverage by MITRE ATT&CK technique; analytic rule definitions; hunting query history.
SI.L2-3.14.6–7	Sentinel incident workflow records; documented MTTR per severity; alert

Practice	Primary Microsoft signal source
(security alert response)	escalation evidence.

Configuration and vulnerability (CM, RA, SI)

Practice	Primary Microsoft signal source
CM.L2-3.4.1–2 (baselines)	Azure Policy compliance state over time; Azure Resource Graph baseline queries; Defender for Cloud regulatory compliance dashboard; Intune device configuration profiles for endpoints.
CM.L2-3.4.3 (change management)	Azure DevOps change records; Azure Resource Manager deployment history with approver evidence; documented change-management procedure.
CM.L2-3.4.6 (least functionality)	Defender for Cloud network recommendations; documented services-and-ports baseline; Azure Firewall rule exports.
CM.L2-3.4.8 (allow-listing)	Microsoft Defender Application Control (MDAC) policy; AppLocker policy; Intune app-control policy assignment evidence.
CM.L2-3.4.9 (user-installed software)	Intune managed apps configuration; Endpoint privilege management policies; documented exception process.
RA.L2-3.11.2 (vulnerability scanning)	Microsoft Defender Vulnerability Management findings; authenticated-scan evidence; Defender for Cloud agentless scanning.
RA.L2-3.11.3 (vulnerability remediation)	Defender Vulnerability Management remediation history; SLA tracking by severity; ServiceNow / Jira remediation tickets linked to findings.
SI.L2-3.14.1 (flaw remediation)	Microsoft Update for Business / Intune update rings; Azure Update Manager deployment history; patch compliance reporting.

Cryptography and data protection (SC, MP)

Practice	Primary Microsoft signal source
SC.L2-3.13.8 (cryptography in transit) — 5-	TLS 1.2+ enforcement on Azure Front Door, Application Gateway, App Service; FIPS cipher suite configuration; certificate inventory in Azure Key Vault with expiry monitoring.

Practice	Primary Microsoft signal source
point	
SC.L2-3.13.10 (key management)	Azure Key Vault key inventory; rotation policy configuration; access policy with documented role separation.
SC.L2-3.13.11 (CUI encryption) — 5-point (POA&M-eligible if not FIPS-validated)	FIPS 140-2 / 140-3 CMVP certificate references for the cryptographic modules in use; Azure Storage encryption configuration; Azure SQL TDE; customer-managed keys; sensitivity-label encryption configuration.
SC.L2-3.13.16 (data-at-rest)	Azure Storage encryption settings; Azure SQL Transparent Data Encryption status; Microsoft Purview sensitivity labels with encryption; SharePoint customer key configuration.
MP.L2-3.8.3 (sanitization)	Documented sanitization procedure aligned to NIST SP 800-88; Azure resource decommissioning with attestation.
MP.L2-3.8.5–6 (media transport)	FIPS-validated encryption for media in transit; Microsoft 365 sensitivity labels enforcing encryption on transport.
MP.L2-3.8.7–8 (removable media)	Defender for Endpoint device control policies; Intune compliance policies blocking USB mass storage; documented exception process.
MP.L2-3.8.9 (backup protection)	Azure Backup with customer-managed keys; documented retention; restricted access to backup vaults.

Boundary, network, and incident (SC, IR)

Practice	Primary Microsoft signal source
SC.L2-3.13.1 (boundary protection) — 5-point	Azure Firewall configuration and logs; NSG rule exports; private endpoint topology; Defender for Cloud network recommendations.
SC.L2-3.13.2 (separation)	VNet topology; NSG segmentation; subscription-level boundary diagrams; documented architecture.
SC.L2-3.13.5	Azure Front Door / WAF separation between public-facing and internal

Practice	Primary Microsoft signal source
(publicly accessible components)	systems; documented architecture review.
IR.L2-3.6.1 (IR capability)	Documented IR plan; Sentinel SOAR playbooks; named IR team.
IR.L2-3.6.2 (track, document, report)	Sentinel incident records; DFARS 7012 72-hour reporting evidence; DC3 reporting records as applicable.
IR.L2-3.6.3 (test response)	Tabletop exercise records; live-fire / red-team exercise records (preferred); documented after-action reports.

08 · THE KYŪDŌ MODEL

CMMC is not an event. It is a state.

CMMC certification is a three-year cycle with annual affirmations of continuous compliance. The certification you receive at the C3PAO assessment is a snapshot of your environment on that day. The annual affirmation, due each year between assessments, is a legal commitment that you are still in compliance — with all 110 practices, on every covered information system, throughout the year. The False Claims Act exposure for affirmations that drift from reality is real and is being enforced.

This is the operational reality CMMC was designed to produce: continuous control operation, continuous evidence capture, continuous monitoring of the full control surface. Programs that treat CMMC as an event to prepare for and then return to baseline operations end up producing affirmations that they cannot defend. Programs that operate continuously satisfy the affirmation as a byproduct of how they work.

Pattern 1 — The SSP as a live document

In the conventional pattern, the SSP is a Word document maintained by the CISO's office. It is updated quarterly at best, often only before an assessment or annual affirmation. Practice descriptions are written once and reused across the cycle. When the environment changes — a new tenant, a new SaaS service, a new subprocessor — the SSP often does not update, and drift compounds.

The continuous-readiness pattern treats the SSP as a queryable view over a graph: every practice is a node, every implementation is a node, every policy is a node, every Microsoft signal source is a node. When a Conditional Access policy changes, when a new sensitivity label is deployed, when a new firewall rule is created, the SSP reflects the change automatically. The affirming official's annual signature is on a document that already matches the operating environment, not one that was rebuilt before the affirmation deadline.

Kyūdō's Knowledge Graph operationalizes this pattern. The SSP is one of many views over the graph; the CMMC scoring view, the cross-framework view (CMMC ↔ SOC 2 ↔ ISO 27001 ↔ NIST CSF), and the evidence index are different traversals of the same underlying data.

Pattern 2 — Evidence-on-demand

CMMC assessments and annual affirmations require evidence. Conventional programs assemble evidence at assessment time — export the Conditional Access policies, screenshot the Defender for Cloud Secure Score, pull the access review reports, format them, attach them to a binder. The work is repeated each year and surges before the assessment.

The continuous-readiness pattern reads Microsoft signal continuously — Entra ID for identity, Defender XDR for threats, Sentinel for monitoring, Purview for data protection, Azure Policy for

configuration. Evidence is captured at execution time, hashed, timestamped, and indexed. When the auditor asks ‘is MFA enforced for all CUI-system access?’ the answer is a query over evidence already collected, not a screenshot exercise that begins after the question is asked.

> **One control set, every framework**
> The Secure Controls Framework (SCF) anchors the Kyūdō Knowledge Graph as the meta-framework substrate. SCF includes 1,470+ controls across 80+ frameworks. CMMC Level 2 maps to SCF; SCF maps to NIST SP 800-171, NIST SP 800-53, NIST CSF v2.0, SOC 2, ISO 27001, HIPAA, EU AI Act, and the rest. A single Microsoft Defender for Cloud configuration baseline, a single Sentinel detection record, a single Purview DLP policy execution attests against every framework where the SCF crosswalk holds. Adding a new framework to the portfolio is a graph operation, not a program rebuild.

Pattern 3 — Sovereignty as architecture

CMMC's most consequential architectural constraint is FedRAMP authorization for cloud services in scope. CUI cannot move through systems that are not FedRAMP authorized. Most SaaS GRC platforms are not FedRAMP authorized at the level required for CUI — which means using them for CMMC compliance creates a paradox: the platform that governs your CUI compliance is itself a non-compliant data path.

The continuous-readiness pattern inverts this. The governance layer deploys inside the customer's own security boundary — in regulated organizations on the Microsoft stack, this means inside the customer's Azure Government tenant. Microservices run in customer-owned AKS clusters with private endpoints, system-assigned managed identities, and customer-managed encryption keys. No governance data crosses the tenant boundary. The CMMC scope of the platform is the customer's tenant; the platform itself does not become a separate processor of CUI.

Pattern 4 — Auditor-defensible AI

AI in GRC is now a category-saturated claim. Most platforms position AI as a chat layer over documents. The continuous-readiness pattern requires AI that survives the C3PAO's next question: every AI-produced explanation, mapping, or recommendation must have a source, a confidence level, and a re-performable result.

In Kyūdō, AI is layered. Deterministic functions handle scoring (DoDAM), state transitions (Conditional → Final), SSP rendering, and POA&M tracking. AI functions handle explanation, draft policy generation, control-mapping suggestions, and natural-language traversal of the Knowledge Graph. The two layers never share a trust contract: the deterministic engine produces the answer, AI produces the prose. When an assessor asks ‘how does this control trace to specific evidence?’ the answer is a graph traversal — not a model output.

Where this leaves you

If you are 30 to 90 days from a C3PAO assessment, this guide is a working checklist. Walk the gates in order. Close the gaps. Schedule the assessment when Gate 1 through Gate 6 are all green.

If you have certified — Conditional or Final — and are now operating against the three-year cycle and the annual affirmation, the architecture this section describes is the direction the practice is moving. The marginal cost of maintaining CMMC compliance, supporting the annual affirmation, and adding cross-framework coverage (SOC 2, ISO 27001, NIST CSF, the EU AI Act) should approach zero. If it does not, the bottleneck is the architecture.

Kyūdō is the platform that makes that architecture available to regulated organizations running Microsoft 365 GCC High and Azure Government. The next step, if useful, is a deployment workshop in your tenant. The architecture brief is one click. The conversation is one email.

—

If this is useful, the next step is concrete

Architecture briefing — a 30-minute walkthrough of the Kyūdō deployment in your Azure Government tenant: CMMC scope rendering, SSP automation, evidence flow, and the sovereignty model. → hello@kyudo.ai

Pre-assessment workshop — 90 minutes walking the six gates against your current state, with documented findings and a 90-day remediation plan. → kyudo.ai/workshop

Trust packet — our CMMC posture, FedRAMP authorization references, data-residency statement, and the Microsoft estate dependency map. Available on request.

APPENDIX A · REFERENCE

The 110 practices, the six gates, the dates.

Practices that cannot be POA&M'd at any point value

Six 1-point controls, plus all 3-point and all 5-point controls except SC.L2-3.13.11 (which can be partially credited to 3 points if encryption is present but not FIPS-validated). If any of the six 1-point exclusions, or any 3- or 5-point control, is NOT MET at the time of assessment, Conditional Certification is unavailable.

Practice	Title	Why excluded from POA&M
AC.L2-3.1.20	External Connections	Foundational scope control — organization must demonstrate awareness and control of every external connection at assessment.
AC.L2-3.1.22	Public Information	Foundational CUI separation control — must be operational at assessment.
CA.L2-3.12.4	System Security Plan	The SSP itself — the assessment depends on it; cannot be deferred.
PE.L1-3.10.3	Escort Visitors	Foundational physical access control.
PE.L1-3.10.4	Audit Logs of Physical Access	Foundational physical access accountability.
PE.L1-3.10.5	Manage Physical Access Devices	Foundational physical access lifecycle.
All 5-point practices (~14)	Critical security controls (MFA, FIPS encryption, boundary protection, etc.)	Too high-impact to defer; failure on any one disqualifies Conditional.
All 3-point practices (~48)	High-value security controls	Too high-impact to defer; failure on any one disqualifies Conditional.

CMMC rollout dates to track

Date	Phase	What happens
December 16, 2024	Program Rule	32 CFR Part 170 (the CMMC Program Rule) becomes effective.

Date	Phase	What happens
September 10, 2025	Acquisition Rule published	DFARS 252.204-7021 final rule published in the Federal Register; 60-day clock to enforcement begins.
November 10, 2025	Phase 1 begins	DoD contracting officers may include CMMC clauses in solicitations. Level 1 and Level 2 self-assessments become a condition of award. Some prioritized acquisitions may require Level 2 (C3PAO) under contracting officer discretion.
November 10, 2026	Phase 2 begins	Level 2 (C3PAO) certifications become required at award for prioritized acquisitions. C3PAO capacity expected to be heavily booked through this period.
November 10, 2027	Phase 3 begins	Level 3 (DIBCAC) assessments required for highest-sensitivity programs. Level 2 certification extends to option-period exercises.
November 10, 2028	Phase 4 begins	Full implementation: every DoD contract or option that involves processing, storing, or transmitting FCI or CUI must include the appropriate CMMC level as a condition of award.

Pre-assessment timeline — 30/60/90 days

If your C3PAO assessment is 90 days out, this is the rough cadence to use as a checkpoint.

Days out	Activity
90	Final scope confirmation. SSP version freeze for assessment baseline. Internal NIST SP 800-171A self-assessment with formal scoring. Affirming official approval of SSP.
75	Identify any 5- or 3-point gaps; remediate. Identify any of the six non-POA&M-eligible 1-point gaps; remediate. Begin building the formal POA&M from remaining 1-point gaps.
60	Mock assessment by an internal or external party using the NIST SP 800-171A methodology. Address findings.
45	Documentation freeze for evidence packages — the assessor will receive these before fieldwork.
30	Final POA&M version. Final SSP version. Final evidence packages submitted to the C3PAO. Pre-assessment readiness call with the C3PAO.

Days out	Activity
14–7	Assessor on-site or virtual fieldwork begins. Assessment liaison designated; control owners on standby.
Assessment week	Daily debriefs with the assessor. Real-time response to RFIs.
+30 days	Final assessment report. Conditional or Final Status determination posted to SPRS. POA&M closeout planning begins (if Conditional).
+180 days max	POA&M closeout assessment by the same C3PAO. Conversion from Conditional to Final.

APPENDIX B · AUTHORITATIVE SOURCES

Where to verify and go deeper.

CMMC is governed by federal regulation; primary sources are authoritative and should be consulted directly for any specific compliance question.

Primary regulation

- 32 CFR Part 170 — Cybersecurity Maturity Model Certification (CMMC) Program. The CMMC Program Rule, effective December 16, 2024.
- 48 CFR — Defense Federal Acquisition Regulation Supplement, including DFARS 252.204-7021 (Contractor Compliance with the CMMC Level Requirement) and DFARS 252.204-7025 (Notice of CMMC Level Requirement). Effective November 10, 2025.
- DFARS 252.204-7012 — Safeguarding Covered Defense Information and Cyber Incident Reporting. The pre-existing CUI safeguarding clause that CMMC formalizes.
- FAR 52.204-21 — Basic Safeguarding of Covered Contractor Information Systems (CMMC Level 1 baseline).

NIST publications

- NIST SP 800-171 Revision 2 — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The 110 practices that constitute CMMC Level 2.
- NIST SP 800-171A — Assessment Procedures for the Security Requirements in NIST SP 800-171. The methodology C3PAOs use to evaluate compliance.
- NIST SP 800-172 — Enhanced Security Requirements for Protecting Controlled Unclassified Information. The 24 additional practices for CMMC Level 3.
- NIST SP 800-18 Revision 1 — Guide for Developing Security Plans for Federal Information Systems. SSP structure and content guidance.
- NIST SP 800-88 Revision 1 — Guidelines for Media Sanitization.
- NIST SP 800-63B — Digital Identity Guidelines: Authentication and Lifecycle Management.

DoD and Cyber AB resources

- DoD CIO CMMC website — program documentation, model documentation, scoping guides, and current Phase status.
- Cyber AB Marketplace — the authoritative directory of authorized C3PAOs for engagement.
- CMMC Assessment Process (CAP) — the procedural document governing how C3PAOs conduct assessments.
- Supplier Performance Risk System (SPRS) — where CMMC scores, certifications, and affirmations are recorded.
- DC3 (DoD Cyber Crime Center) — cyber incident reporting per DFARS 7012(c).

Microsoft documentation

- Microsoft 365 GCC High and Azure Government — FedRAMP authorization documentation in the FedRAMP Marketplace.
- Microsoft Service Trust Portal — published assessments, audit reports, and Customer Assurance Service documents for Microsoft cloud services.
- Microsoft Purview Compliance Manager — CMMC Level 2 assessment template with improvement actions mapped to Microsoft 365 GCC High and Azure Government.
- Microsoft Defender for Cloud regulatory compliance dashboard — includes NIST SP 800-171 Rev 2 baseline.
- Microsoft CMMC documentation set — product team guidance for CMMC Level 2 implementation in Microsoft 365 GCC High.

APPENDIX C · GLOSSARY

Terms used in this checklist.

Term	Definition
Affirming Official	The senior official designated by the contractor to file annual affirmations of continuous compliance in SPRS. Replaces the term 'senior company official' from the CMMC proposed rule.
C3PAO	CMMC Third-Party Assessment Organization. Authorized by the Cyber AB to conduct Level 2 assessments. Listed in the Cyber AB Marketplace.
CMMC	Cybersecurity Maturity Model Certification. The DoD's certification program for contractors handling FCI or CUI.
Conditional Status	A temporary 180-day CMMC certification status granted when the contractor scores ≥88, has met all 5- and 3-point practices and the six non-POA&M-eligible 1-point controls, and has eligible 1-point items on a POA&M. Converts to Final upon successful closeout assessment.
CUI	Controlled Unclassified Information. Defined by 32 CFR Part 2002 and the National Archives CUI Registry.
Cyber AB	The CMMC Accreditation Body, formerly the CMMC-AB. Responsible for accrediting C3PAOs and maintaining the assessor ecosystem.
DFARS	Defense Federal Acquisition Regulation Supplement. The DoD's supplement to the FAR. Houses the CMMC contract clauses (252.204-7021, 252.204-7025) and CUI safeguarding clauses (252.204-7012).
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center. Conducts Level 3 assessments. Part of the Defense Contract Management Agency (DCMA).
DoDAM	DoD Assessment Methodology. The point-based scoring system used to evaluate CMMC Level 2 compliance against NIST SP 800-171.
FCI	Federal Contract Information. Unclassified information not intended for public release that is provided by or generated for the government under a contract to develop or deliver a product or service. Lower sensitivity than CUI; CMMC Level 1 applies.
FedRAMP	Federal Risk and Authorization Management Program. The U.S. government's program for authorizing cloud services. Moderate or High authorization is required for cloud services handling CUI.

Term	Definition
FIPS-validated cryptography	Cryptographic modules validated by NIST against FIPS 140-2 or FIPS 140-3 through the Cryptographic Module Validation Program (CMVP). Required for protecting CUI per multiple SP 800-171 controls.
Final Status	The full CMMC Level 2 certification, valid for 3 years. Achieved either by meeting all 110 practices at initial assessment or by closing all POA&M items within the 180-day Conditional window.
GCC High	Microsoft 365 Government Community Cloud High. FedRAMP High authorized; approved for CUI including ITAR-controlled categories. Distinct from Microsoft 365 GCC (Moderate, not approved for ITAR) and Microsoft 365 Commercial.
NIST SP 800-171	The NIST Special Publication that defines the 110 security requirements for protecting CUI in nonfederal systems. Revision 2 (2020) is the current version used by CMMC.
NIST SP 800-171A	The companion assessment methodology to SP 800-171. Defines how each of the 110 practices is evaluated.
OSA	Organization Seeking Assessment. The contractor undergoing CMMC assessment.
POA&M	Plan of Action and Milestones. A formal document tracking remediation of practices that are NOT MET. CMMC restricts POA&M eligibility to specific 1-point items with strict 180-day closure.
Prioritized acquisition	A DoD acquisition that requires Level 2 (C3PAO) certification rather than self-assessment, based on the sensitivity of CUI involved.
SPRS	Supplier Performance Risk System. The DoD system of record for CMMC scores, certifications, affirmations, and CMMC unique identifiers (UIDs).
SSP	System Security Plan. The master document describing system boundaries, environments, control implementations, and interconnections. CA.L2-3.12.4 requires it; an inadequate SSP fails the assessment.
UID	CMMC Unique Identifier. A 10-character code assigned per assessment, recorded in SPRS, and provided to contracting officers with proposals.

is not legal advice. CMMC is governed by federal regulation; consult 32 CFR Part 170, the DFARS Acquisition Rule, your contracting officer, and an authorized C3PAO for compliance-specific guidance. Always reference the official Cyber AB Marketplace for the current authorized C3PAO list.