Apptega

GUIDE

CMMC v2.13

Compliance Guide (Levels 1—3)

Understanding and Implementing Security Requirements for Defense Contractors

Current as of August 19, 2025

Apptega

Apptega

1. Introduction

CMMC is DoD's program to verify that defense contractors implement required cybersecurity practices to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

The current model establishes three levels: **Level 1** (15 basic safeguarding requirements), **Level 2** (110 requirements aligned to NIST SP 800-171 Rev. 2), and **Level 3** (selected NIST SP 800-172 requirements). CMMC is codified in regulation and supported by official DoD assessment and scoping guides. **This guide is designed to be practical and implementable—use it to plan, build, validate, and continuously improve your CMMC posture.**

1A. Beginner Quick-Start (First 30—90 Days)

Days 1—15 (Initiation & SSP skeleton)

- Appoint Program Lead, ISSO, System Owner(s), TPRM Lead, and a Privacy/Records contact.
- Define the authorization boundary for CUI; draw the data-flow map.
- Start the inheritance register (enterprise/system/cloud service provider).
- Create the SSP skeleton now: overview, boundary narrative, roles, inheritance summary, and brief domain narratives.

Days 16—45 (Tailoring & SSP full draft)

- Run domain workshops to finalize applicability, parameter values, acceptance criteria, and compensating measures.
- Establish identity/MFA, logging, and change control foundations.
- Complete the first full SSP draft by Day 45.

Days 46—90 (Evidence & assessment readiness)

- Populate the Evidence Register; conduct an IR tabletop and a restore drill.
- Perform an internal assessment using assessor-style objectives; update SSP and POA&M.
- Freeze an assessment-ready SSP ≥14 days before any formal assessment.

2. Scope & Alignment

Level 1 (Foundational): basic safeguarding for FCI (annual self-assessment and affirmation).

Level 2 (Advanced): 110 practices for CUI (self-assessment or certification per contract).

Level 3 (Expert): selected additional practices for higher-risk environments (certification).

SSP timing: skeleton Days 1–15, full draft by Day 45, freeze ≥14 days pre-assessment.

Inheritance: document clearly what enterprise/CSP covers and how service-level settings were verified.

Apptega

3. Domains & Practices

Each domain includes intent, minimums, how to implement (procedural/technical/contractual), evidence, acceptance criteria highlights with CMMC practice IDs, common failures, and an internal audit plan. SSP timing guidance is included where relevant.

AC — Access Control

Intent: Limit access to authorized users/processes and enforce least privilege.

Minimums: Account lifecycle control; separation of duties; session control; remote and portable media protections.

Implement — Procedural: Role catalog; joiner–mover–leaver within 24 hours; quarterly access reviews; privileged access approvals; break-glass governance.

Implement — Technical: SSO + MFA; PAM/JIT elevation with session recording; network segmentation; device trust for remote access; scoped API tokens and service principals.

Implement — Contractual: Provider admin access logging; audit/cooperation rights.

- **Evidence:** RBAC matrix; access recertification sign-offs; PAM/JIT recordings; SSO/VPN configurations.
- **Acceptance Criteria (examples):**
  - **AC.L2-3.1.1** — All accounts mapped to roles; access reviews ≤90 days; deprovisioning ≤24 hours; orphaned accounts = 0.
  - **AC.L2-3.1.12** — Idle timeout ≤15 minutes; absolute session ≤12 hours.
  - **AC.L2-3.1.21** — Portable storage restricted; only approved encrypted media; DLP blocks unapproved devices.
- **Common Failures:** Shared admin credentials; stale service accounts; weak timeouts; unmanaged tokens.
- **Internal Audit Plan:** Sample 25 users and 10 admins; validate least privilege, MFA coverage, recerts, session/JIT controls.
- **SSP placement:** Summarize AC in the SSP skeleton; expand with parameters and evidence by Day 45.

AT — Awareness & Training

Intent: Ensure personnel understand CUI handling and security duties.

Implement — Procedural/Technical: Role-based curricula; phishing/reporting drills; developer secure coding track; LMS tracking and hands-on simulations.

- **Evidence:** Completion rosters; test scores; phishing metrics; developer course completions.
- **Acceptance Criteria:** AT.L2-3.2.1 — 100% trained before access; annual refresher; remediation within 10 days after failures.
- **Common Failures:** Generic content; no remediation coaching; training not tied to access enablement.
- **Internal Audit Plan:** Trace 10 new hires and 10 role changes to verified completion records.
- **SSP placement:** Summarize program scope and metrics in the assessment-ready SSP.

AU — Audit & Accountability

Intent: Generate, protect, retain, and use logs to detect and investigate events.

Implement: Logging standard; event taxonomy; SIEM centralization; immutable storage; clock synchronization; alert triage SOP.

- **Evidence:** Log configurations; time-sync proofs; sample admin events; retention settings; alert tickets.
- **Acceptance Criteria:** AU.L2-3.3.1 — Required event set on 100% of in-scope systems; retention ≥12 months online/36 months archive; daily ingestion health alert.
- **Common Failures:** Missing admin events; clock drift; unreviewed alerts; retention gaps.
- **Internal Audit Plan:** Verify events and retention for five critical systems; review alert handling and closure SLAs.

CM — Configuration Management

Intent: Maintain hardened baselines and controlled change.

Implement: Change control with risk rating; emergency path; rollback/testing; CMDB governance; IaC with PR reviews; hardened images; config scanning; drift alerts; SBOM management.

- **Evidence:** Approved change records; hardened images; drift reports; PR trails; inventory accuracy reports.
- **Acceptance Criteria:** CM.L2-3.4.1 and related — Baseline via IaC to 100% scope; drift alerts ≤24 hours; emergency changes documented within 1 business day; inventory accuracy ≥98%.
- **Common Failures:** Manual tweaks; no rollback; ignored drift; stale CMDB.
- **Internal Audit Plan:** Sample 10 changes and compare deployed state to baseline; verify CMDB accuracy.

IA — Identification & Authentication

Intent: Uniquely identify and strongly authenticate users, devices, and services.

Implement: Credential issuance/revocation; secrets management with rotation SLAs; SSO; phishing-resistant MFA where feasible; PAM; device certificates; FIPS-appropriate cryptography.

- **Evidence:** MFA coverage reports; password/secret policies; PAM logs; device certificate inventories.
- **Acceptance Criteria:** IA.L2-3.5.3 — MFA on remote/admin paths; zero shared accounts; secrets within age SLAs; device trust enforced for admin endpoints.
- **Common Failures:** API keys in code; unmanaged service accounts; weak MFA exceptions.
- **Internal Audit Plan:** Review 20 identities and 10 service accounts; check MFA, groups, last login, secret age, device trust.

IR — Incident Response

Intent: Detect, analyze, contain, eradicate, recover, and learn.

Implement: Playbooks (phishing, ransomware, exfiltration, insider, vendor breach); evidence handling SOP; after-action reviews with corrective actions; EDR; SOAR; forensics-ready logging; case management.

- **Evidence:** IR plan; incident tickets; artifacts; AARs with corrective actions; communications records.
- **Acceptance Criteria:** IR.L2-3.6.1 — Tabletop within last 12 months; 24×7 contact path; corrective actions tracked to closure.
- **Common Failures:** Unclear decision rights; no forensics retainer; comms delays; evidence gaps.
- **Internal Audit Plan:** Review three incidents end-to-end including chain-of-custody documentation.

MA — Maintenance

Intent: Perform authorized, controlled maintenance.

Implement: Maintenance windows; approvals; escorted visitors; maintenance logs; secure remote maintenance with MFA and recording; deny-by-default outside windows.

- **Evidence:** Maintenance logs; approvals; session recordings; visitor logs.
- **Acceptance Criteria:** MA.L2-3.7.5 — Remote maintenance sessions recorded and retained ≥12 months; unauthorized maintenance = 0.
- **Common Failures:** Ad-hoc fixes; insecure remote sessions; missing logs.
- **Internal Audit Plan:** Sample five maintenance events; verify approvals, recordings, and post-maintenance sanitation.

MP — Media Protection

Intent: Protect media throughout its lifecycle.

Implement: Media tracking; labeling; chain of custody; approved destruction vendors; full-disk encryption; restricted removable media; TLS for transfers; DLP for exports.

- **Evidence:** Media logs; encryption configurations; certificates of destruction; transport records.
- **Acceptance Criteria:** MP.L2-3.8.3 — 100% encrypted portable media; disposal within SLA with certificates.
- **Common Failures:** Lost removable drives; untracked exports; weak disposal processes.
- **Internal Audit Plan:** Trace 10 media items from issuance to disposal; review export logs.

PS — Personnel Security

Intent: Ensure trustworthy personnel and clean separations.

Implement: Tiered background checks; NDAs; offboarding checklist; periodic re-screen for elevated roles; insider risk awareness; automated deprovision; badge disable sync; device wipe.

- **Evidence:** Screening records; offboarding tickets; badge logs; access removal proofs.
- **Acceptance Criteria:** PS.L2-3.9.2 — Deprovision within 24 hours; lingering access = 0; elevated roles re-screened per policy.
- **Common Failures:** Manual offboarding; stale accounts; inconsistent screening.
- **Internal Audit Plan:** Sample 10 exits and 10 elevated-role changes.

PE — Physical Protection

Intent: Limit physical access and protect facilities.

Implement: Badge policy; escorts; CCTV; alarms; locks; tamper-evident seals; environmental sensors; periodic access reviews; drills.

- **Evidence:** Access lists; visitor logs; camera retention settings; environmental test results.
- **Acceptance Criteria:** PE.L2-3.10.1 — Visitor logs retained ≥12 months; badges distinguishable; escorts enforced; environmental tests current.
- **Common Failures:** Shared badges; blind spots; poor retention; uncontrolled deliveries.
- **Internal Audit Plan:** Walkthrough and sample visitor/badge records; spot-check camera coverage.

RA — Risk Assessment

Intent: Identify and treat security risk systematically.

Implement: Enterprise risk register; system risk logs; treatment plans feeding POA&M; risk acceptance criteria; vulnerability scanning; threat modeling; external attack surface monitoring.

- **Evidence:** Risk reports; scan results; decisions and dates; treatment closure proofs.
- **Acceptance Criteria:** RA.L2-3.11.2 — Critical/High findings mitigated within SLA or time-bound acceptance with compensations; residual risk trend tracked.
- **Common Failures:** Snapshot-only reviews; no linkage to remediation; stale acceptances.
- **Internal Audit Plan:** Trace five high-risk items from discovery to closure or time-bound acceptance.

CA — Security Assessment

Intent: Plan, conduct, and document assessments.

Implement: Assessment plan; independence appropriate to risk; results and remediation tracking; scripted tests; dashboards for exceptions; rolling assessments.

- **Evidence:** Assessment plans and results; POA&M; risk acceptance memos.
- **Acceptance Criteria:** CA.L2-3.12.1 and related — Each practice mapped to assessment objectives with linked evidence; assessment-ready SSP frozen ≥14 days before assessment.
- **Common Failures:** Paper-only attestations; stale POA&M; unmanaged exceptions.
- **Internal Audit Plan:** Confirm latest SAR, active POA&M management, and closure proofs.

SC — System & Communications Protection

Intent: Protect communications and enforce system boundaries.

Implement: Key management SOP; network zoning; secure API rules; data egress policy; TLS/SSH standards; WAF; IDS/IPS; micro-segmentation; DNS security; email protections; DLP where appropriate.

- **Evidence:** Cipher configurations; key rotation logs; segmentation diagrams; WAF/IDS rules; egress/ACL records.
- **Acceptance Criteria:** SC.L2-3.13.8 — Deny-by-default egress; changes only via approved change records; key rotation within policy; strong cipher usage across in-scope assets.
- **Common Failures:** Legacy ciphers; flat networks; unmanaged keys; open egress.
- **Internal Audit Plan:** Validate cipher suites; inspect segmentation against inventory; review egress rules and exceptions.

SI — System & Information Integrity

Intent: Detect and correct flaws; resist malicious code; monitor anomalies.

Implement: Patch SLAs by severity; exception register; integrity baselines; EDR/AV; file integrity monitoring; vulnerability scanning; anomaly detection.

- **Evidence:** Patch dashboards; EDR/FIM coverage; exceptions; scan results; remediation tickets.
- **Acceptance Criteria:** SI.L2-3.14.1 — Patch SLA adherence; EDR/FIM coverage ≥99%; mean time to patch critical within target; exceptions time-bound with compensations.
- **Common Failures:** Shadow IT; unsupported OS; stale exceptions; scanning blind spots.
- **Internal Audit Plan:** Sample 20 hosts for patch levels and coverage; verify exception justifications and expiry.

4. Authorization Boundary & Data-Flow Mapping

Describe components, interfaces, trust zones, external services, and where CUI flows, rests, and leaves. Maintain records of processing (sources, stores, transmissions, recipients). Update on material change. Include the diagram and narrative in the SSP skeleton by Day 15, keep synchronized through the Day-45 full draft, and confirm in the pre-assessment freeze.

5. System Security Plan (SSP) — Canonical Narratives

Write the SSP as cohesive prose covering: overview/mission use; boundary and inventory; CUI categories and lifecycle; roles and governance; inheritance and verification of service-level settings; domain implementations; identity/MFA, zoning/egress, cryptography, logging, backups, vulnerability management; assessment status and findings; change and baselines; vendors and sub-tiers.

When to create/update the SSP

- Create the SSP skeleton in Days 1–15.
- Complete the full SSP draft by Day 45 (post-tailoring workshops).
- Freeze an assessment-ready SSP ≥14 days before internal/external assessments.
- Update upon boundary/technology/CUI changes or after POA&M closures that materially change narratives.

6. Applicability, Acceptance Criteria & Assessment Mapping

Maintain a definitive record for each Level-2 practice stating applicability, implementation summary, parameter values, measurable acceptance criteria, assessment objectives, inheritance type, and a pointer to evidence.

Example excerpt (illustrative):

Practice ID	Title	Applicable	Implementation Summary	Parameters	Acceptance Criteria	Inheritance	Evidence
AC.L2-3.1.1	Limit system access	Y	RBAC via SSO; least privilege; JIT admin	Idle 15m; lockout 5/30m	Users mapped; recert ≤90d; deprovision ≤24h; orphaned=0	System	GRC/AC/Recert_Q2.csv
AU.L2-3.3.1	Create audit records	Y	Unified SIEM; admin events; immutable storage	Retention 12m/36m	Required events 100%; daily ingestion alert	Hybrid	SecOps/SIEM/health.png
IA.L2-3.5.3	Use MFA	Y	MFA on remote/ admin; SCIM deprovision	—	100% coverage; exceptions ≤30d with approval	Enterprise	IAM/MFA_Coverage.csv
SC.L2-3.13.8	Managed interfaces	Y	Firewalls/WAF; egress ACLs; deny-by-default	Block outbound except approved	All outbound via managed gateways; CRs for changes; logs ≥12m	Hybrid	Net/Firewall/Ruleset.yaml
SI.L2-3.14.1	Flaw remediation	Y	Patch SLAs; vuln scans; exception register	Crit 15d; High 30d	SLA met or time-bound exception with compensations	System	VM/Dashboard.png

7. Control Parameter Defaults

- **Sessions & Access:** Idle 15 minutes; absolute 12 hours; failed attempts 5 within 30 minutes; lockout 30 minutes; admin JIT 60 minutes.
- **Cryptography:** TLS 1.2+ with strong suites; at-rest AES-256; key rotation every 12 months; keys in KMS/HSM.
- **Logging:** Required event set; retention 12 months online / 36 months archive; clock drift ≤5 minutes; daily ingestion health alerts.
- **Patching:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90; exceptions ≤90 days with compensations.
- **Backups (if applicable):** Daily incrementals; weekly full; immutability 30 days; quarterly restore test meeting RTO/RPO.
- **Identity:** Deprovision ≤24 hours; service accounts owned and rotated ≤90 days; device trust required for admin endpoints.
- **Data Handling (CUI):** Labeling; approved export channels; deletion within 30 days after trigger.
- **Vendors:** Incident notice ≤72 hours; SBOM on request; annual reassessment; right to audit.

8. Evidence Register

Artifact	Practices	Location/Path	Owner	Format	Retention
Access Recert Q2	AC.*	GRC/ Recerts/2025Q2	IAM Lead	CSV + sign-off PDF	6 years
MFA Coverage Report	IA.L2-3.5.3	IAM/Reports/MFA.csv	IAM Lead	CSV/PNG	3 years
SIEM Rule Pack v5	AU., *IR.*	SecOps/SIEM/rules	SecOps	JSON	Current + 1 year
Restore Drill 2025-05	SI ops	Resilience/ Tests/2025-05	DR Lead	PDF	6 years
Firewall Ruleset	SC.L2-3.13.8	Net/Firewall/Ruleset.yaml	NetSec	YAML	Current + 1 year

9. Continuous Monitoring Plan

- **Daily:** SIEM ingestion health; critical alerts triage; EDR coverage check.
- **Weekly:** Vulnerability scans; failed backups; sample admin activity review.
- **Monthly:** Access review roll-up; config drift review; patch SLA dashboard; egress rule review.
- **Automations:** Open tickets on ingestion failures, missing EDR, encryption drift, MFA gaps, or expired exceptions.
- **Reporting:** Dashboard to Program Lead/ISSO; exceptions have owners and due dates. Include a concise ConMon summary in the assessment-ready SSP before freeze.

10. POA&M Workflow & Risk Acceptance Criteria

Workflow: Identify → Record (severity, owner, due date, milestones) → Treat (remediate/compensate/time-bound accept) → Verify with evidence → Report.

Targets: Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90.

Risk Acceptance: Only with compensating controls, explicit expiry, and leadership approval. Auto-remind 14 days before expiry.

Update SSP narratives when POA&M closures materially change implementations.

11. Cloud & Hosting (Shared Responsibility & Inheritance)

Decide per practice what is inherited (CSP/enterprise), shared, or system-specific. Capture provider attestations, data locations, KMS model, logging/egress controls, incident notice SLAs, and subprocessor transparency. Verify service-level settings (admin-console MFA, log exports, storage encryption, public object defaults). Integrate SSO/MFA and log exports to your SIEM. Document inheritance and verification steps in the SSP full draft.

12. Training & Awareness Program

Onboarding ≤30 days; annual refresh; quarterly micro-modules. Tracks: workforce baseline; Admin/IT; Developers (secure coding/SDLC); Security Ops; Executives; Vendors. Measure completion ≥98%, phishing failure trend down, remediation ≤10 days, and retraining after incidents or role changes. Summarize scope and metrics in the assessment-ready SSP.

13. Supply Chain Coverage

Intake and tier suppliers handling CUI; define required artifacts. Contract for security/privacy clauses; breach and vulnerability notice SLAs; SBOM delivery; right to audit; sub-tier transparency. Monitor renewals, external attack surface, incident sharing, and change notifications. Offboard with data return/destruction and credential/certificate revocation; preserve logs. Name critical suppliers and obligations in the SSP full draft.

14. SDLC Gatekeeping & Pipeline Controls

Embed controls across delivery:

- **Plan:** Threat modeling; security non-functional requirements; acceptance criteria.
- **Build:** SAST/SCA; secrets scanning; artifact signing.
- **Test:** DAST; container and IaC scans.
- **Release:** Change approval; drift checks; rollout/backout plans.
- **Operate:** Observability; WAF/IDS; IaC drift monitors.
- **Blocking gates:** Any failing SAST/SCA/secrets/IaC check blocks merge or release unless a time-bound exception with compensations is approved. Keep pipeline logs and signatures as evidence. Describe SDLC controls in the SSP full draft and confirm in the pre-assessment freeze.

15. Evidence Sampling Plans

- **Access (AC):** Sample 25 users and 10 admins; validate RBAC mapping, MFA status, last login, and deprovision proofs.
- **Changes (CM):** Sample 10 change records; confirm approvals, PR reviews, rollback, and that deployed state matches baseline.
- **Logging (AU):** Sample 5 CUI systems; show required events, retention, and alert handling.
- **Backups/Restores:** Perform 3 restores from different tiers; confirm RTO/RPO met.
- **Vulnerabilities (SI):** Sample 20 hosts; verify patch SLA adherence and exception expiry.
- **Vendors (SC/TPRM):** Review 5 critical vendors; confirm MFA evidence, logging, data location, SBOM, incident notices. Cite sampling strategy and latest results in the assessment-ready SSP.

16. Level 1 (FCI) — Fast Implementation

Scope systems with only FCI. Implement the FAR 52.204-21 basic safeguarding practices quickly: asset inventory; boundary firewall/NAT; MFA for remote/admin; patch cadence; backups; anti-malware; least privilege; basic logging; physical access controls. Perform annual self-assessment and affirmation. Keep a lightweight SSP-style narrative.

17. Level 3 (Expert) — Additions

Add selected advanced practices for higher risk: deeper telemetry; segmentation; exfiltration resistance; adversary-in-the-middle defenses; enhanced key management; privileged activity constraints; continuous validation. Certification is required; ensure the SSP addresses each addition with supporting evidence.

18. Common Pitfalls

Assuming CSP inheritance without verifying service-level settings; missing parameter values that make practices untestable; enabling logging without alert use-cases or review cadence; weak joiner–mover–leaver; unmanaged service accounts; untested disaster recovery; vague third-party terms; scattered evidence and undefined retention. Address mitigations to these pitfalls in the SSP narratives.

19. Quick Reference Summary

Domain	Core Artifacts	Examples
AC	RBAC matrix; access reviews; PAM/JIT logs	MFA; least privilege; session management
AT	Training matrix; completion records	Role-based training; secure coding
AU	Log standard; SIEM rules; retention configs	Immutable logs; admin event capture
CM	Baseline configs; change records; drift reports	IaC; hardened images; SBOM
IA	MFA policy; secret rotation; device certs	SSO; PAM; service accounts
IR	IR plan; playbooks; AARs	EDR; SOAR; evidence preservation
MA	Maintenance logs; approvals; recordings	Secure remote maintenance
MP	Media logs; encryption; destruction certs	Chain of custody; TLS transfers
PS	Screening; offboarding tickets	JML; badge disable; device wipe
PE	Badge/CCTV logs; visitor logs	Visitor management; locks
RA	Risk reports; scans; treatment	Threat modeling; vuln management
CA	Assessment plans/results; POA&M	Rolling assessments; dashboards
SC	Crypto/KMS records; segmentation	WAF; IDS/IPS; TLS configs
SI	Patch dashboards; EDR/FIM coverage	Integrity checks; anti-malware

20. SPRS Score & CMMC Status

What SPRS is. The Supplier Performance Risk System (SPRS) is DoD's official system where assessment results are recorded for contracting use. For Level 2 self-assessments, post your score in SPRS. For certification assessments, the assessor records results in DoD systems and you provide the required affirmation in SPRS.

What you submit

- **Level 2:** Submit your current assessment score for the in-scope environment, with required metadata (assessment date, CAGE code(s), etc.).
- **Level 1:** Submit the required annual affirmation (Level 1 does not use the 110-point scoring model).

How the Level-2 score is calculated

- Each practice carries a weight of 1, 3, or 5 points.
- Start at 110; subtract the weight for every NOT MET practice.
- Limited partial credit applies only to two practices (MFA and FIPS-validated encryption).
- Valid scores range from −203 to 110.

CMMC program threshold for Level 2

- Conditional status is available at ≥88 (80% of 110) with only permitted practices on a POA&M; all POA&M items must be closed within 180 days to reach Final status.

Posting/refresh rules

- A current score must be in SPRS before award (generally not older than 3 years, unless a solicitation requires newer).
- Post for each covered system in scope and ensure the score aligns to the SSP boundary assessed.
- Access and submission are through PIEE with the appropriate SPRS vendor role.

Practical tips to improve the score quickly

- Close 5-point gaps first.
- If you are near 88, address MFA and FIPS-validated encryption to recover 3 points each when partially implemented.
- Keep the Evidence Register synchronized with each deduction and closure so the SPRS entry is defensible.

21. References & Resources

DoD CIO — CMMC Program (About/Overview)
https://dodcio.defense.gov/CMMC/

CMMC Model Overview — Version 2.13
https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverviewv2.pdf

CMMC Assessment Guide — Level 2, Version 2.13
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf

CMMC Assessment Guide — Level 3
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL3.pdf

DFARS 252.204-7019 (SPRS Posting Requirement)
https://www.acquisition.gov/dfars/252.204-7019

PIEE — SPRS Access for Vendors
https://piee.eb.mil/

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com