connvertex

COMPLIANCE · CROSSWALK · v1.0

The Unified Compliance Crosswalk

One control set. One evidence repository. Five audits.

CMMC 2.0 L2 | FedRAMP Moderate | NIST 800-53 | HIPAA | SOC 2

Prepared by Connvertex · Practitioner-led cybersecurity consulting for government. Released April 2026 · connvertex.com

SECTION 01

Document control

Scope, versioning, and the disclaimer that scopes how this document can be used.

Scope and intent

This crosswalk is a practitioner reference. It is the starting control map we use on day one of a unified-compliance engagement. It is not a substitute for a full gap assessment, a signed System Security Plan, or an authoritative reading of the source publications. Control references have been condensed for readability. Consult the primary sources and your assessor for interpretation that binds an audit.

Framework versions referenced

Framework	Version referenced
CMMC 2.0 L2	CMMC v2.0 Level 2 (Nov 2024 rule)
FedRAMP Mod	FedRAMP Moderate baseline (Rev 5)
NIST 800-53	NIST SP 800-53 Rev 5
HIPAA	HIPAA Security Rule (45 CFR 164.300)
SOC 2	AICPA TSC 2017 (2022 points of focus)

Revision history

Version	Date	Change
1.0	April 2026	First public release. Twenty-eight controls across ten domains mapped to five frameworks.

SECTION 02

Contents

SECTION 03

Executive summary

Five frameworks. One operating model. What this document does, why it matters, and how to read it.

Five audits, one control set.

Every compliance program we inherit looks the same at first glance. Separate binders for CMMC, FedRAMP, NIST 800-53, HIPAA, and SOC 2. Separate assessors on different calendars. Separate evidence repositories, separate POA&Ms;, and a remediation backlog that is almost always the same five findings written four different ways.

The fix is not another tool. The fix is the observation that these frameworks overlap by roughly seventy percent at the control layer. A policy written once satisfies all five. An access review run on a quarterly cadence satisfies all five. A single signed SSP and POA&M; pair satisfies all five. Build the program that way and the second, third, and fourth audits are eighty percent cheaper than the first.

This document is the crosswalk we use on day one of a readiness engagement. Twenty-eight controls grouped across ten domains, each mapped to the five frameworks, each paired with the single evidence artifact we expect to see during assessment. Run the program off this sheet and the binders collapse into one.

HOW TO READ THIS DOCUMENT

Sections four and five give you the problem and the principle. Section six is the crosswalk itself: twenty-eight controls grouped into ten domains, each mapped to all five frameworks with the evidence artifact we expect to see during assessment. Sections seven through nine show how to operate the program and how to migrate from parallel tracks.

SECTION 04

The parallel-tracks problem

Five ways a conventional multi-framework program breaks. Each of these is recoverable, but only after the binders collapse into one.

Duplicate policies that drift.
A separate policy binder per framework produces two or three slightly different password policies, two or three slightly different backup policies, and a guaranteed finding the first time an assessor compares them side by side.

Duplicate evidence.
A screenshot of MFA coverage lives in the CMMC evidence folder, a different version lives in the SOC 2 folder, and neither is dated. Same control, three copies, all stale within a quarter.

Conflicting remediation backlogs.
The CMMC POA&M;, the HIPAA risk analysis action log, and the SOC 2 exception list all contain the same three overdue items. Nobody is accountable for any of them because ownership sits in three places.

Auditor fatigue.
Each framework's assessor walks the same environment and asks the same questions. Your engineers context-switch through four audits a year and lose a quarter of their delivery capacity to audit support.

Brittle to change.
When one framework revises (Rev 4 to Rev 5, HIPAA security rule amendments, SOC 2 points of focus), the change breaks only the binder that tracked it. The rest of the program silently falls out of sync.

SECTION 05

One control set, five audits.

Six moves that turn five programs into one. Every subsequent section of this document is a practical application of these moves.

STEP 01	**Pick the most-demanding framework as the master.** For federal civilian and DoD-adjacent buyers, that is almost always NIST SP 800-53 Rev 5 at the Moderate baseline. For a commercial SaaS with some regulated customers, SOC 2 plus the HIPAA Security Rule typically sits underneath. One master, not five.
STEP 02	**Build a single control catalog against that master.** Policies, procedures, and runbooks are authored once, in one repository, with a single version history. Every control carries a list of the frameworks it satisfies as metadata.
STEP 03	**Map every control to every framework, once.** The crosswalk in this document is the starting point. Keep it in a single spreadsheet or GRC tool; do not let framework-specific binders re-emerge. If a new framework enters scope, add a column, not a program.
STEP 04	**Store evidence once, tag it to every control it satisfies.** One access-review memo, one backup-restore report, one signed SSP. Each artifact is tagged with every control ID it evidences across every framework. Assessors pull directly from the same repo.
STEP 05	**Operate one cadence, not five.** Monthly risk reviews, quarterly access reviews, semi-annual training, annual tabletop. Frameworks consume the cadence; the cadence does not change for them.
STEP 06	**Retire the parallel POA&Ms.;** One remediation list with one owner per item. Every POA&M; entry carries the framework-specific references it closes so that you can still answer each assessor's line of questioning without duplicating the work.

SECTION 06

The crosswalk

Twenty-eight controls, ten domains, five frameworks. Each card is self-contained so it can be routed to a specific owner.

CMMC 2.0 L2 | FedRAMP Mod | NIST 800-53 | HIPAA | SOC 2

DOMAIN G Governance, policy, and risk

The program's constitution. Accountable ownership, a current system security plan, and a live POA&M; are scored against in every framework.

G.1 Security policy and procedures

Published, signed, and reviewed annually. One set, authored against the master framework, with per-framework references as metadata.

CMMC 2.0 L2	`CA.L2-3.12.4 · policy family lead-ins`
FedRAMP Mod	`PL-1 · AC-1 · all family '-1' controls`
NIST 800-53	`PL-1, AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PS-1, RA-1, SA-1, SC-1, SI-1, SR-1`
HIPAA	`§164.316(a) Policies and procedures`
SOC 2	`CC1.4, CC2.2`

EVIDENCE One policy binder, version-controlled, with a quarterly review log signed by the accountable owner.

G.2 System security plan (SSP)

Current-dated, signed by a senior accountable official, describing the boundary, the control baseline, and the implementation status of every in-scope control.

CMMC 2.0 L2	CA.L2-3.12.4
FedRAMP Mod	PL-2
NIST 800-53	PL-2
HIPAA	§164.316(b)(1) Documentation
SOC 2	CC3.1, CC3.4

EVIDENCE Signed SSP v{N} with date on the cover page; linked to the evidence repository for every control.

G.3 Risk assessment and POA&M;

Documented risk register reviewed quarterly. One POA&M; for the whole program, with framework-specific references on each row.

CMMC 2.0 L2	RA.L2-3.11.1 · CA.L2-3.12.2
FedRAMP Mod	RA-3 · CA-5
NIST 800-53	RA-3, RA-3(1), CA-5
HIPAA	§164.308(a)(1)(ii)(A) Risk analysis · (B) Risk management
SOC 2	CC3.2, CC3.3, CC3.4

EVIDENCE Dated risk register; POA&M; export with owner, due date, and multi-framework references on every open item.

DOMAIN I Identity and access

The single largest source of findings across all five frameworks. If these are tight, assessments get short.

I.1 Account management

Provisioning and deprovisioning with documented approvals; same-day removal on termination; quarterly review of all privileged accounts.

CMMC 2.0 L2	AC.L2-3.1.1 · AC.L2-3.1.2
FedRAMP Mod	AC-2, AC-2(1), AC-2(3)
NIST 800-53	AC-2, AC-2(1), AC-2(3), AC-2(13)
HIPAA	§164.308(a)(4)(ii)(B) Access authorization · (C) Access establishment and modification
SOC 2	CC6.2, CC6.3

EVIDENCE Identity-provider account inventory; quarterly access review minutes with removals listed; three recent termination tickets showing same-day deprovisioning.

I.2 Least privilege

Roles are scoped; privileged access is time-boxed; separation of duties is documented for sensitive operations.

CMMC 2.0 L2	AC.L2-3.1.5 · AC.L2-3.1.4
FedRAMP Mod	AC-6, AC-6(1), AC-6(5), AC-6(7)
NIST 800-53	AC-6, AC-6(1), AC-6(5), AC-6(7), AC-6(9), AC-6(10)
HIPAA	§164.308(a)(3)(ii)(B) Workforce clearance · §164.308(a)(4)(ii)(A) Isolating health-care functions
SOC 2	CC6.1, CC6.3

EVIDENCE Role matrix with separation-of-duties map; privileged-access justification records; quarterly review of role membership.

I.3 Multi-factor authentication

Enforced for every privileged account, every remote access path, and every cloud admin console. Exception list is written, owned, and calendared for removal.

CMMC 2.0 L2	IA.L2-3.5.3
FedRAMP Mod	IA-2(1), IA-2(2), IA-2(8), IA-2(11), IA-2(12)
NIST 800-53	IA-2(1), IA-2(2), IA-2(8), IA-2(11), IA-2(12)
HIPAA	§164.312(d) Person or entity authentication
SOC 2	CC6.1, CC6.6

EVIDENCE MFA coverage export from the identity provider; exception list with expiration dates; PIV/CAC integration memo where applicable.

I.4 Authenticator management

Strength, rotation, storage, and recovery for passwords and certificates. FIPS-validated where required.

CMMC 2.0 L2	IA.L2-3.5.7 · IA.L2-3.5.8 · IA.L2-3.5.9
FedRAMP Mod	IA-5, IA-5(1), IA-5(2), IA-5(6)
NIST 800-53	IA-5, IA-5(1), IA-5(2), IA-5(6), IA-5(7)
HIPAA	§164.308(a)(5)(ii)(D) Password management
SOC 2	CC6.1

EVIDENCE Password policy; NIST 800-63B mapping memo; FIPS CMVP certificate numbers for any hardware or software authenticator modules.

DOMAIN D Data protection and cryptography

FIPS-validated encryption in transit, at rest, and on retired media. This is where 'TLS is not enough' becomes a finding.

D.1 Cryptography in transit

TLS 1.2 or higher between every in-scope component and every external user, backed by a FIPS 140-2 or 140-3 validated module.

CMMC 2.0 L2	SC.L2-3.13.8
FedRAMP Mod	SC-8, SC-8(1)
NIST 800-53	SC-8, SC-8(1), SC-8(2)
HIPAA	§164.312(e)(1) Transmission security · (e)(2)(ii) Encryption
SOC 2	CC6.7

EVIDENCE CMVP certificate numbers for every crypto module; testssl.sh or ssllabs scan output for every external endpoint; HSTS preload submission.

D.2 Cryptography at rest

Encryption of regulated data on disk with FIPS-validated modules; KMS-managed keys with documented rotation.

CMMC 2.0 L2	SC.L2-3.13.11 · SC.L2-3.13.16
FedRAMP Mod	SC-28, SC-28(1)
NIST 800-53	SC-28, SC-28(1), SC-28(2)
HIPAA	§164.312(a)(2)(iv) Encryption and decryption
SOC 2	CC6.7, CC6.1

EVIDENCE CMVP certificates; KMS inventory; key-rotation logs; sample storage service configuration showing encryption enabled.

D.3 Media protection and sanitization

Media inventory, handling, and end-of-life sanitization documented per NIST SP 800-88 Rev 1.

CMMC 2.0 L2	MP.L2-3.8.1 through 3.8.9
FedRAMP Mod	MP-1, MP-3, MP-4, MP-5, MP-6, MP-7
NIST 800-53	MP-1, MP-3, MP-4, MP-5, MP-6, MP-7
HIPAA	§164.310(d)(1) Device and media controls · (d)(2)(i) Disposal · (d)(2)(ii) Media re-use
SOC 2	CC6.5

EVIDENCE Media inventory; sanitization certificates from the disposal vendor; internal wipe logs with tool and method recorded.

DOMAIN M Audit, logging, and monitoring

Logs without review are a storage bill. Every framework asks implicitly or explicitly for ticketed evidence that logs are read.

M.1 Event logging

Every in-scope system emits security-relevant events to a centralized log store; retention matches the authoritative framework for the environment.

CMMC 2.0 L2	AU.L2-3.3.1 · AU.L2-3.3.2
FedRAMP Mod	AU-2, AU-3, AU-11, AU-12
NIST 800-53	AU-2, AU-3, AU-3(1), AU-11, AU-12
HIPAA	§164.312(b) Audit controls
SOC 2	CC7.2

EVIDENCE SIEM coverage map showing every in-scope system; log source inventory; retention configuration export.

M.2 Log review and alerting

A named analyst reviews alerts on a documented cadence; alert-to-ticket-to-closure path is auditable.

CMMC 2.0 L2	AU.L2-3.3.3 · AU.L2-3.3.5
FedRAMP Mod	AU-6, AU-6(1), AU-6(3)
NIST 800-53	AU-6, AU-6(1), AU-6(3), AU-6(5)
HIPAA	§164.308(a)(1)(ii)(D) Information system activity review
SOC 2	CC7.2

EVIDENCE Three alert dispositions from the last 30 days (alert, analyst, action, closure timestamp); on-call rotation schedule.

M.3 Continuous monitoring

Authoritative baseline for what 'healthy' looks like; drift is detected, ticketed, and closed against the baseline.

CMMC 2.0 L2	CA.L2-3.12.3 · SI.L2-3.14.6
FedRAMP Mod	CA-7, CA-7(1), SI-4, SI-4(2)
NIST 800-53	CA-7, CA-7(1), SI-4, SI-4(2), SI-4(4)
HIPAA	§164.308(a)(8) Evaluation
SOC 2	CC7.1, CC7.2

EVIDENCE Continuous monitoring strategy document; dashboard screenshots with dates; drift tickets with closure timestamps.

M.4 Vulnerability scanning

Authenticated scans on every in-scope asset at least monthly; findings routed into the same POA&M; that carries audit items.

CMMC 2.0 L2	RA.L2-3.11.2 · RA.L2-3.11.3
FedRAMP Mod	RA-5, RA-5(2), RA-5(5)
NIST 800-53	RA-5, RA-5(2), RA-5(4), RA-5(5), RA-5(11)
HIPAA	§164.308(a)(8) Evaluation
SOC 2	CC4.1, CC7.1

EVIDENCE Scanner configuration showing authenticated mode; 30-day scan history; POA&M; rows referencing scanner IDs.

DOMAIN R Incident response

A paper plan that has never survived a tabletop is a red flag in every debrief we have ever read.

R.1 Incident response plan

Written IR plan with named roles, notification chains, and framework-specific reporting obligations baked in (CISA, HHS, customer contractual, auditor notification).

CMMC 2.0 L2	IR.L2-3.6.1
FedRAMP Mod	IR-8
NIST 800-53	IR-8, IR-8(1)
HIPAA	§164.308(a)(6)(i) Security incident procedures
SOC 2	CC7.4

EVIDENCE Signed IR plan with version history; reporting-chain diagram covering each framework's notification obligation.

R.2 Incident handling and reporting

Exercised at least annually with leadership at the table; post-incident after-action reports drive corrective actions that land in the POA&M.;

CMMC 2.0 L2	IR.L2-3.6.2 · IR.L2-3.6.3
FedRAMP Mod	IR-4, IR-4(1), IR-6, IR-6(1)
NIST 800-53	IR-4, IR-4(1), IR-4(3), IR-6, IR-6(1)
HIPAA	§164.308(a)(6)(ii) Response and reporting
SOC 2	CC7.3, CC7.4, CC7.5

EVIDENCE Tabletop scenario + attendees + AAR from the last 12 months; tickets showing closure of the corrective actions.

DOMAIN C Configuration and change management

A dated asset inventory and a signed baseline are the two artifacts that shorten every assessment.

C.1 Baseline configuration

Per-platform hardened baselines (CIS or vendor equivalent) with drift reporting.

CMMC 2.0 L2	CM.L2-3.4.1 · CM.L2-3.4.2
FedRAMP Mod	CM-2, CM-2(2), CM-2(3), CM-6
NIST 800-53	CM-2, CM-2(2), CM-2(3), CM-6, CM-6(1)
HIPAA	§164.308(a)(5)(ii)(B) Protection from malicious software · §164.312(a)(1) Access control
SOC 2	CC8.1

EVIDENCE Approved baseline documents per platform; last drift report per baseline; exceptions with expiration.

C.2 System and asset inventory

One inventory covering every in-scope asset, classification, owner, and data class; refreshed at least monthly.

CMMC 2.0 L2	CM.L2-3.4.1
FedRAMP Mod	CM-8, CM-8(1), CM-8(3)
NIST 800-53	CM-8, CM-8(1), CM-8(2), CM-8(3), PM-5
HIPAA	§164.310(d)(1) Device and media controls
SOC 2	CC6.1

EVIDENCE Dated inventory export; reconciliation log showing monthly refresh; data-flow diagram.

C.3 Flaw remediation

Documented patch cadence with SLAs per severity; vulnerability records feed into the unified POA&M.;

CMMC 2.0 L2	SI.L2-3.14.1
FedRAMP Mod	SI-2, SI-2(2)
NIST 800-53	SI-2, SI-2(2), SI-2(3), SI-2(5)
HIPAA	§164.308(a)(5)(ii)(B) Protection from malicious software
SOC 2	CC7.1

EVIDENCE Patch policy; patch compliance dashboard; 90-day aging report showing SLA adherence.

C.4 Change management

Every production change goes through a reviewed, approved, and logged workflow; emergency changes reconcile back within one business day.

CMMC 2.0 L2	CM.L2-3.4.3 · CM.L2-3.4.5
FedRAMP Mod	CM-3, CM-3(2), CM-5
NIST 800-53	CM-3, CM-3(2), CM-3(4), CM-5, CM-5(1)
HIPAA	§164.312(a)(1) Access control
SOC 2	CC8.1

EVIDENCE Change records with approvals from the last quarter; emergency-change post-mortems; segregation of development and production access.

DOMAIN B Contingency, backup, and resilience

Backups you have not restored are wishes. Recovery tests are the difference between passing and failing CP controls.

B.1 System backup

Regular, encrypted, and tested. Immutable or offsite copies for anything that would hurt to lose.

CMMC 2.0 L2	MP.L2-3.8.9
FedRAMP Mod	CP-9, CP-9(1), CP-9(8)
NIST 800-53	CP-9, CP-9(1), CP-9(5), CP-9(8)
HIPAA	§164.308(a)(7)(ii)(A) Data backup plan · (D) Testing and revision
SOC 2	A1.2

EVIDENCE Backup policy; most recent restore-test report; offsite or immutable storage evidence; RTO/RPO matrix.

B.2 Contingency planning

Plans for disruption, from a single-service outage to a full site-loss scenario. Tested at least annually.

CMMC 2.0 L2	RE.L2-3.8.9 (implied)
FedRAMP Mod	CP-2, CP-2(1), CP-2(3), CP-3, CP-4
NIST 800-53	CP-2, CP-2(1), CP-2(3), CP-3, CP-4, CP-4(1)
HIPAA	§164.308(a)(7)(i) Contingency plan · (ii)(C) Emergency mode operation
SOC 2	A1.3

EVIDENCE Contingency plan document; most recent exercise AAR; named contingency roles in the IR plan.

DOMAIN T Third-party and supply chain

Every assessor now pulls on the supply chain. The POA&M; that covers your vendors is the POA&M; they read first.

T.1 External system services

Vendor inventory covering every system that stores, processes, or transmits regulated data. Signed agreements matching your control rigor.

CMMC 2.0 L2	SA.L2-3.16.1 (flow-down portion)
FedRAMP Mod	SA-9, SA-9(1), SA-9(2)
NIST 800-53	SA-9, SA-9(1), SA-9(2), SA-9(4), SA-9(5)
HIPAA	§164.308(b)(1) Business associate contracts · §164.314(a) Organizational requirements
SOC 2	CC9.2

EVIDENCE Vendor inventory with data-class per vendor; signed DPAs, BAAs, or flow-down clauses; last risk review date per vendor.

T.2 Supply chain risk management

Program covering acquisition, component integrity, and supplier tiering. Formal SCRM plan where applicable.

CMMC 2.0 L2	SA.L2-3.16.1
FedRAMP Mod	SR-3, SR-5, SR-6, SR-11
NIST 800-53	SR-1 through SR-12 as applicable
HIPAA	Implied through §164.308(a)(1) and §164.308(b)
SOC 2	CC9.2

EVIDENCE SCRM plan; supplier tiering list; acquisition-stage security review template; counterfeit-prevention attestation where applicable.

DOMAIN P Personnel security

Screening and lifecycle controls. Small teams make these skippable; every framework asks anyway.

P.1 Personnel screening

Documented screening criteria per role, with records retained and reviewed at reassignment.

CMMC 2.0 L2	PS.L2-3.9.1
FedRAMP Mod	PS-3, PS-3(1), PS-3(3)
NIST 800-53	PS-3, PS-3(1), PS-3(3)
HIPAA	§164.308(a)(3)(ii)(B) Workforce clearance procedure
SOC 2	CC1.4, CC1.5

EVIDENCE Per-role screening matrix; redacted screening records; reassignment review log.

P.2 Termination and role change

Same-day deprovisioning for terminations; documented role-change reviews that recheck access scope.

CMMC 2.0 L2	PS.L2-3.9.2
FedRAMP Mod	PS-4, PS-5, AC-2(6)
NIST 800-53	PS-4, PS-4(1), PS-5, AC-2(6)
HIPAA	§164.308(a)(3)(ii)(C) Termination procedures
SOC 2	CC6.3, CC1.4

EVIDENCE Termination tickets with same-day deprovisioning evidence; role-change review records; asset-return checklists.

DOMAIN A Awareness and training

Common cause of a finding in every framework. Records are what make it auditable.

A.1 Security awareness training

Annual general training for every workforce member, with records retained and reminders scheduled for role changes.

CMMC 2.0 L2	AT.L2-3.2.1
FedRAMP Mod	AT-2, AT-2(2), AT-2(3)
NIST 800-53	AT-2, AT-2(2), AT-2(3)
HIPAA	§164.308(a)(5)(i) Security awareness and training
SOC 2	CC1.4, CC2.2

EVIDENCE LMS completion records; curriculum outline; reminder-email template; role-change triggered re-training log.

A.2 Role-based training

Elevated training for privileged roles (admins, developers, responders, executives), with content tailored to the role's threat model.

CMMC 2.0 L2	AT.L2-3.2.2 · AT.L2-3.2.3
FedRAMP Mod	AT-3, AT-3(2), AT-3(4)
NIST 800-53	AT-3, AT-3(2), AT-3(3), AT-3(4)
HIPAA	§164.308(a)(5)(ii)(A-D) Security reminders · Protection · Log-in monitoring · Password management
SOC 2	CC1.4

EVIDENCE Role-based curriculum per function; completion records; content review log.

SECTION 07

Evidence reuse patterns

Six artifacts that, produced once, satisfy every framework in scope. Build the evidence habit around these and the audits get shorter.

Quarterly access review memo

What it is. A single dated memo, signed by the accountable owner, listing every privileged account reviewed in the quarter, the action taken (retained, removed, scoped down), and the next review date.

Cadence. Quarterly, dated, signed, linked to the evidence repository.

Identity and access I.1 · I.2 · I.4 · P.2	Governance G.3 (feeds the risk register)
CMMC 2.0 L2	AC.L2-3.1.1, 3.1.2, 3.1.5; IA.L2-3.5.7
FedRAMP Mod	AC-2, AC-2(3), AC-6, IA-5
NIST 800-53	AC-2, AC-2(3), AC-2(13), AC-6, IA-5
HIPAA	§164.308(a)(4)(ii)(B)(C); §164.308(a)(3)(ii)(C)
SOC 2	CC6.2, CC6.3

FIPS CMVP certificate inventory

What it is. One spreadsheet listing every cryptographic module in use (TLS, KMS, disk encryption, VPN, HSM) with CMVP certificate numbers, validation version, and the system that depends on the module.

Cadence. Refreshed monthly; keyed off the CMVP catalog export.

	Data protection D.1 · D.2	**Identity and access** I.4 (where authenticators rely on validated modules)
CMMC 2.0 L2	`SC.L2-3.13.8, 3.13.11, 3.13.16`	
FedRAMP Mod	`SC-8, SC-8(1), SC-13, SC-28`	
NIST 800-53	`SC-8, SC-13, SC-28`	
HIPAA	`§164.312(a)(2)(iv), §164.312(e)(2)(ii)`	
SOC 2	`CC6.7, CC6.1`	

SIEM coverage map and 30-day alert sample

What it is. A diagram showing every in-scope system mapped to its log source in the SIEM, plus three alert dispositions pulled from the last 30 days (alert payload, analyst, action, closure timestamp).

Cadence. Coverage map reviewed monthly; alert samples rotated every month.

Audit and monitoring M.1 · M.2 · M.3	Incident response R.2 (feeds the handling workflow)
CMMC 2.0 L2	AU.L2-3.3.1, 3.3.3, 3.3.5; CA.L2-3.12.3
FedRAMP Mod	AU-2, AU-6, AU-6(3), CA-7, SI-4
NIST 800-53	AU-2, AU-6, AU-6(3), CA-7, SI-4, SI-4(4)
HIPAA	§164.308(a)(1)(ii)(D); §164.312(b)
SOC 2	CC7.1, CC7.2

Tabletop AAR and incident response runbook version history

What it is. A two-page after-action report from a tabletop in the last 12 months (scenario, attendees, timeline, corrective actions, due dates, closure evidence), paired with the runbook's change history.

Cadence. At least annual exercise; runbook version history on every change.

	Incident response R.1 · R.2	Contingency planning B.2	Awareness and training A.2
CMMC 2.0 L2	IR.L2-3.6.1, 3.6.2, 3.6.3		
FedRAMP Mod	IR-3, IR-4, IR-6, IR-8		
NIST 800-53	IR-3, IR-4, IR-4(1), IR-6, IR-8		
HIPAA	§164.308(a)(6)(i)(ii); §164.308(a)(7)(ii)(D)		
SOC 2	CC7.3, CC7.4, CC7.5		

SSP and POA&M; with quarterly-signed cover

What it is. One System Security Plan and one Plan of Action & Milestones, version-controlled, with a quarterly review memo signed by a senior accountable official on the cover. Every POA&M; row carries multi-framework references.

Cadence. Quarterly review and re-sign; version-bump on every material change.

Governance G.1 · G.2 · G.3	**Every other domain (these are the authoritative records)** all
CMMC 2.0 L2	CA.L2-3.12.4; RA.L2-3.11.1; CA.L2-3.12.2
FedRAMP Mod	PL-2, CA-5, RA-3
NIST 800-53	PL-2, CA-5, RA-3, RA-3(1)
HIPAA	§164.308(a)(1)(ii)(A)(B); §164.316(b)(1)
SOC 2	CC3.1, CC3.2, CC3.4

Vendor inventory with signed agreements

What it is. One vendor list covering every service that stores, processes, or transmits regulated data; one signed agreement per vendor (DPA, BAA, or flow-down clause); one risk-review date per vendor.

Cadence. Inventory refreshed monthly; risk review at least annually per vendor.

	Third-party and supply chain T.1 · T.2	**Data protection** D.1 · D.2 (where vendors hold keys or custodial data)
CMMC 2.0 L2	SA.L2-3.16.1	
FedRAMP Mod	SA-9, SA-9(1), SA-9(2), SR-3, SR-5	
NIST 800-53	SA-9, SA-9(2), SA-9(5), SR-3, SR-5, SR-6	
HIPAA	§164.308(b)(1); §164.314(a)(1)(2)	
SOC 2	CC9.2	

SECTION 08

Operating cadence

The unified program runs on one calendar. Frameworks consume the cadence; the cadence does not flex for them.

Frequency	Activities
Monthly	Risk register review · vendor inventory reconciliation · patch compliance review · drift report per baseline · open POA&M; items aging report.
Quarterly	Privileged access review · SSP + POA&M; quarterly sign-off · backup restore test · training reminders for lapsed roles · vendor attestation refresh.
Semi-annually	Policy review and re-publish · role-based training refresh for privileged roles · tabletop on a non-primary scenario.
Annually	Program-level tabletop with leadership · external penetration test · third-party attestation renewal (SOC 2, ISO 27001) · control-baseline re-scoping against the authoritative framework.

Anything that does not fit this cadence is usually theater. If a framework insists on a bespoke schedule, that is worth pushing back on in your first assessor conversation; in our experience every assessor we have worked with accepts the unified cadence once they can see the evidence trail it produces.

SECTION 09

Migration from parallel tracks

If you already run a multi-framework program in parallel, this is the fifteen-week sequence to collapse it into one.

Weeks 1-2. Pick the master.
Choose the most-demanding framework in your scope as the master control baseline. For federal or DoD-adjacent scope, that is NIST SP 800-53 Moderate or High. Put the choice in writing; this becomes the program's constitution.

Weeks 3-4. Build the crosswalk.
Adopt this document's crosswalk or import it into your GRC tool. Add columns for any additional frameworks in your scope. Do not build a separate workbook per framework; there is one workbook.

Weeks 5-8. Rewrite policies against the master.
One policy binder, versioned once. Every clause carries metadata tagging the frameworks it satisfies. Retire the per-framework binders the week the master binder is published.

Weeks 9-12. Consolidate the evidence repository.
Stand up one repo (SharePoint site, Box folder, Git repo, GRC tool record — the platform is less important than the one). Move every existing evidence artifact into it, tagging each with every control ID it satisfies.

Weeks 13-14. Merge the POA&Ms.;
Take every per-framework POA&M; row and collapse duplicates into a single list. Each row keeps the per-framework references it closes. One owner, one due date, one status.

Week 15 onward. Operate one cadence.
Run the monthly / quarterly / semi-annual / annual cadence described earlier in this document. Assessors consume the cadence; the cadence does not flex for them.

SECTION 10

Next step

About Connvertex.

WANT THIS CROSSWALK TAILORED TO YOUR ENVIRONMENT?

Book a 30-minute readiness call.

Book a 30-minute readiness call with a senior Connvertex practitioner. The person on the call is the person who would do the work. We will review your current framework footprint, pick the right master baseline, and send you a written migration plan within 48 hours. No proposal, no qualification call, no BDR loop.

connvertex.com/contact · hello@connvertex.com

About Connvertex

Connvertex is a practitioner-led cybersecurity and digital services firm serving U.S. federal, state, and local government and the regulated enterprises that support them. Our GRC and compliance service line builds unified compliance programs against the five frameworks covered in this document, plus ISO/IEC 27001 and CJIS where the scope calls for them.

Minority-owned. Woman-owned. NMSDC MBE certified. Pursuing SBA 8(a), WOSB / EDWOSB, and CMMC 2.0 Level 2 certification in 2026.

Connvertex Unified Compliance Crosswalk, version 1.0. Released April 2026. Informational; not a substitute for assessor-grade advice. Consult the primary-source publications for authoritative interpretation.