Apptega

GUIDE

NIST 800-53 Rev. 5 Compliance

Understanding and Implementing Security and Privacy Controls for Federal Information Systems and Organizations

Current as of August 19, 2025

Apptega

1. Introduction 3

2. Scope & Alignment (Who, What, and Relationship to RMF/FedRAMP/CMMC) 5

4. Key Terms & Concepts 6

5. Framework at a Glance (Rev. 5 • 53B • 53A • RMF) 6

6. Implementation Deep Dives (by Control Family, Rev. 5 order) 7

7. Authorization Boundary & Data-Flow Mapping 23

8. Baseline & Tailoring Record (Rev. 5 + 53B) 23

9. Control Parameter Table (Organization-Specific Settings) 24

10. Evidence Register (Artifacts & Retention) 25

11. Continuous Monitoring Plan (Frequencies & Automations) 25

12. POA&M Workflow & Risk Acceptance Criteria 26

13. Cloud & Hosting (Shared Responsibility & Inheritance) 26

14. Training & Awareness Program (Role-Based) 27

15. Supply Chain Coverage (TPRM overlays, SBOM, disclosure SLAs) 27

16. SDLC Gatekeeping & Pipeline Controls 28

17. Common Pitfalls 28

18. Quick Reference Summary (Family • Artifacts • Examples) 29

19. References & Resources 30

Apptega

1. Introduction

NIST SP 800-53 Rev. 5 provides a comprehensive catalog of security and privacy controls for information systems and organizations. This guide converts that catalog into an operational handbook: owners, workflows, technical guardrails, parameter settings, metrics, and audit evidence to sustain authorization and ongoing compliance within your boundary and interconnections.

Apptega

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

Days 1—15

- Assign Authorizing Official (AO), CISO, ISSO, System Owner, Privacy Officer.
- Define the authorization boundary; inventory components and draw a data-flow map.
- Select a Rev. 5 baseline (Low/Moderate/High) and draft tailoring rules (adds, scoping, parameters, compensations).
- Create a Control Implementation Statement (CIS) workbook and inheritance register (common/hybrid/system-specific).

Days 16—45

- Run family-by-family tailoring workshops; set parameter values.
- Draft the System Security Plan (SSP); place gaps into a POA&M with owners and due dates.
- Stand up logging architecture (AU/IR/SI), identity stack (IA), and change control (CM) integrated with SDLC/DevOps.

Days 46—90

- Launch continuous monitoring of priority controls; publish dashboards.
- Conduct a tabletop (IR) and a backup/restore drill (CP).
- Perform an internal assessment; finalize SSP, SAR inputs, and POA&M for authorization or renewal.

Apptega

2. Scope & Alignment (Who, What, and Relationship to RMF/FedRAMP/CMMC)

- **Who:** Federal agencies, contractors, and private organizations adopting Rev. 5.
- **What:** Organizational and system-level controls supporting confidentiality, integrity, availability, and privacy.
- **RMF lifecycle:** Categorize → Select (Rev. 5 + 53B) → Implement (inherit where possible) → Assess (53A) → Authorize → Monitor.
- **Crosswalks:** Maintain mappings to FedRAMP-style inheritance, CMMC, and ISO to maximize reuse.

3. Roles & Responsibilities (RACI)

Activity / Area	Executive Sponsor	AO	CISO	ISSO	System Owner	Privacy Officer	Engineering/ IT	Procurement	Legal/ Compliance
Boundary, Categorization, Baseline	A	**R**	**C**	**C**	**R**	C	C	I	I
SSP & Tailoring	A	**C**	**R**	**R**	**R**	C	C	I	I
Control Implementation & Evidence	A	I	**R**	**R**	**R**	C	**R**	I	C
Assessments & SAR	A	**C**	**R**	**R**	C	C	C	I	C
POA&M & Risk Acceptance	A	**R**	**R**	**R**	**R**	C	C	I	C
Authorization Decision	A	**R**	C	C	C	C	I	I	I
Continuous Monitoring	A	C	**R**	**R**	**R**	C	**R**	I	I

A = Accountable R = Responsible C = Consulted I = Info

4. Key Terms & Concepts

- **Family • Control • Enhancement:** Catalog hierarchy; enhancements extend core controls.
- **Baseline & Tailoring:** Pre-selected control sets with scoping, parameter values, overlays, and compensations.
- **Common / Hybrid / System-Specific:** Inherited from enterprise, shared responsibility, or local implementation.
- **SSP / SAR / POA&M:** Plan → assessment results → remediation.
- **Continuous Monitoring (ConMon):** Recurring assessments, metrics, risk decisions, and reporting.

5. Framework at a Glance (Rev. 5 • 53B • 53A • RMF)

- **SP 800-53 Rev. 5:** Unified security and privacy controls for organizations and systems.
- **SP 800-53B:** Baselines (Low/Moderate/High + privacy baseline) and tailoring guidance.
- **SP 800-53A:** Assessment procedures (examine, interview, test).
- **RMF:** Risk-managed selection, authorization, and operation over time.

Apptega

6. Implementation Deep Dives (by Control Family, Rev. 5 order)

Each family includes: Intent • Minimums • Implement — Procedural/Technical/ Contractual • Evidence • Metrics • Common Failure Modes • Internal Audit Plan

6.1 Access Control (AC)

Intent: Ensure only authorized identities access only what they need, when they need it.

Minimums: Role definitions; least privilege; session control; remote access safeguards; periodic access reviews.

Implement — Procedural: Role catalog with least-privilege profiles; joiner–mover–leaver ≤24h; quarterly recerts; privileged access request workflow.

Implement — Technical: SSO + MFA; PAM with just-in-time elevation and session recording; segmentation; API scopes for service accounts; IP allowlists for admin consoles.

Implement — Contractual: Providers enforce MFA/RBAC and retain access logs; right to review privileged access.

- **Evidence:** RBAC matrix; recert attestations; elevation logs; VPN/SSO configs.
- **Metrics:** ≥95% recerts on time; 100% MFA on interactive/admin; orphaned accounts = 0.
- **Common Failure Modes:** Shared admin credentials; stale service accounts; weak session timeouts.
- **Internal Audit Plan:** Sample 25 users and 10 admins; verify least privilege, MFA, JIT, and session controls.

6.2 Awareness & Training (AT)

Intent: Build role-appropriate security and privacy competence.

Minimums: Onboarding ≤30 days; annual refresh; targeted training for admins/developers; privacy topics for PT family.

Implement — Procedural: Training matrix by role; phishing program; remediation coaching ≤10 days; micro-modules quarterly.

Implement — Technical: LMS tracking; secure-coding labs tied to SDLC; phishing simulations; role-targeted labs for IR/Forensics.

Implement — Contractual: Vendors attest workforce training equivalency for personnel with access.

- **Evidence:** Rosters; scores; phishing metrics; developer course completions.
- **Metrics:** Completion ≥98%; phishing failure trending down; developer coverage ≥95%.
- **Common Failure Modes:** One-size-fits-all courses; no developer or IR content; training not tied to access.
- **Internal Audit Plan:** Trace 10 new hires and 10 role changes to training evidence.

6.3 Audit & Accountability (AU)

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

Minimums: Time sync; required event set; privileged activity capture; retention; alerting.

Implement — Procedural: Logging standard; event taxonomy; review cadence; escalation runbook; evidence preservation SOP.

Implement — Technical: Central SIEM; immutable storage; endpoint/cloud audit sources; UEBA rules; clock synchronization.

Implement — Contractual: CSP/API log export and retention SLAs; admin events included.

- **Evidence:** Log configs; time-sync proofs; sample admin events; alert tickets; retention settings.
- **Metrics:** 100% logging on critical systems; MTTD/MTTR; log integrity check pass rate.
- **Common Failure Modes:** Missing admin events; clock drift; unmonitored logs; retention gaps.
- **Internal Audit Plan:** Select 5 critical systems; verify events, retention, and alert handling.

6.4 Assessment, Authorization, and Monitoring (CA)

Intent: Independently assess controls, decide on authorization, and monitor continuously.

Minimums: Assessment plan; assessor independence; SAR; authorization decision; monitoring strategy and cadence.

Implement — Procedural: Rolling assessments; POA&M governance; risk acceptance workflow; change-driven reassessment triggers.

Implement — Technical: Evidence automation; machine-readable catalogs; scripted tests; dashboards for KPIs and exceptions.

Implement — Contractual: Assessor access and independence; evidence-sharing protocols with providers.

- **Evidence:** SAP/SAR; POA&M; authorization letter; ConMon reports; risk acceptance memos.
- **Metrics:** POA&M burn-down; % controls tested per quarter; time from finding → fix; % accepted risks with expiry dates.
- **Common Failure Modes:** Paper-only ATO; stale POA&M; unmanaged exceptions; no change triggers.
- **Internal Audit Plan**: Confirm last SAR, authorization decision, monitoring outputs, and risk acceptances.

6.5 Configuration Management (CM)

Intent: Establish hardened baselines and control change.

Minimums: Baseline configs; change approvals; code/config review; drift detection; inventory accuracy.

Implement — Procedural: CR process with risk rating; emergency path; SoD; rollback/testing; CMDB governance.

Implement — Technical: IaC with PR reviews; CIS-aligned baselines; config scanning; drift alerts; SBOM management.

Implement — Contractual: Providers disclose change windows and maintain baselines; notify of impactful changes.

- **Evidence:** Approved CRs; hardened images; drift reports; PR trails; inventory reports.
- **Metrics:** % assets compliant; change success rate; drift MTTR; CMDB–reality match rate.
- **Common Failure Modes:** Manual tweaks; no rollback; ignored drift; stale inventory.
- **Internal Audit Plan:** Sample 10 changes; compare running configs to baseline; verify CMDB accuracy.

6.6 Contingency Planning (CP)

Intent: Recover operations within defined objectives.

Minimums: BIA; RTO/RPO; backups; alternate processing; tests.

Implement — Procedural: Annual BCP/DR exercises; tabletop plus live restores; prioritized runbooks; lessons-learned tracking.

Implement — Technical: Encrypted/immutable backups; replication; tested restores; automated recovery scripts; cross-region failover.

Implement — Contractual: Recovery SLAs; test participation; evidence sharing with providers.

- **Evidence:** BIA; test reports; backup job logs; restoration screenshots; failover records.
- **Metrics:** Backup success ≥99%; restore success ≥95%; findings closed ≤60 days; RTO/RPO met in drills.
- **Common Failure Modes:** Untested backups; co-located copies; unclear priorities; no runbooks.
- **Internal Audit Plan:** Perform a sample restore; review last DR test evidence and closures.

6.7 Identification & Authentication (IA)

Intent: Strongly identify and authenticate users, devices, and services.

Minimums: MFA for remote/admin; credential policy; service account control; device identity.

Implement — Procedural: Credential issuance/revocation; secrets management; rotation SLAs and exception handling.

Implement — Technical: SSO; phishing-resistant MFA where feasible; PAM; certificate-based device auth; crypto aligned to policy; passwordless options where appropriate.

Implement — Contractual: Admin consoles require MFA and automated deprovision (e.g., SCIM).

- **Evidence:** MFA coverage; password/secret policies; PAM logs; device cert inventories.
- **Metrics:** 100% MFA on applicable paths; zero shared accounts; secrets within age SLAs; device trust coverage.
- **Common Failure Modes:** API keys in code; shared creds; unmanaged service accounts; weak MFA exceptions.
- **Internal Audit Plan:** Pull 20 identities and 10 service accounts; check MFA, groups, last login, secret age.

6.8 Incident Response (IR)

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

Minimums: IR plan; roles; communications; reporting timelines; lessons learned.

Implement — Procedural: Playbooks (phishing, ransomware, exfiltration, insider, vendor breach); evidence handling; post-incident reviews feeding fixes.

Implement — Technical: EDR, email security, SOAR, threat intel; sandboxing; forensics-ready logging; case management.

Implement — Contractual: Vendor incident notice SLAs; forensics cooperation and data-sharing.

- **Evidence:** IR plan; incident tickets; artifacts; AARs with corrective actions; comms records.
- **Metrics:** MTTD/MTTR; tabletop cadence; % corrective actions closed on time; containment time.
- **Common Failure Modes:** Unclear decision rights; no forensics retainer; comms delays; evidence gaps.
- **Internal Audit Plan:** Review 3 incidents end-to-end including chain of custody and corrective action closure.

6.9 Maintenance (MA)

Intent: Perform authorized, controlled maintenance.

Minimums: Scheduled/unscheduled procedures; tool control; sanitized devices post-maintenance.

Implement — Procedural: Maintenance windows; approvals; escorted visitors; maintenance logs; spare parts control.

Implement — Technical: Secure remote maintenance; session recording; deny-by-default outside windows; break-glass with approvals.

Implement — Contractual: Technician backgrounding where required; confidentiality/NDAs.

- **Evidence:** Maintenance logs; approvals; session recordings; visitor logs.
- **Metrics:** Unauthorized maintenance = 0; logs present for 100% events; remote session coverage.
- **Common Failure Modes:** Ad-hoc fixes; insecure remote sessions; missing logs.
- **Internal Audit Plan:** Sample 5 maintenance events; verify approvals, recordings, and device sanitation.

6.10 Media Protection (MP)

Intent: Protect media throughout its lifecycle.

Minimums: Labeling; encryption; transport controls; sanitization/disposal standards.

Implement — Procedural: Media tracking; chain of custody; approved destruction vendors; export approvals.

Implement — Technical: Full-disk encryption; restricted removable media; TLS for transfers; DLP for exports; vaulting for secrets.

Implement — Contractual: Certificates of destruction; right to audit; secure shipping.

- **Evidence:** Media logs; encryption configs; destruction certificates; transport records.
- **Metrics:** 100% encrypted portable media; disposal within SLA; export approval adherence.
- **Common Failure Modes:** Lost removable drives; untracked exports; weak disposal.
- **Internal Audit Plan:** Trace 10 items from issuance to disposal; review export logs.

6.11 Physical & Environmental Protection (PE)

Intent: Control physical access and ensure environmental resilience.

Minimums: Facility controls; visitor logs; monitoring; environmental specs.

Implement — Procedural: Badge policy; escort rules; periodic access reviews; incident drills.

Implement — Technical: Badging, CCTV, alarms; redundant power/cooling; leak/smoke detection; tamper-evident seals.

Implement — Contractual: DC attestations; right to review; SLA for environmental incidents.

- **Evidence:** Access lists; visitor logs; camera retention; environmental test results; badge reviews.
- **Metrics:** Badge review completion; tailgating incidents; environmental test pass rate; CCTV uptime.
- **Common Failure Modes:** Shared badges; blind spots; poor retention; uncontrolled deliveries.
- **Internal Audit Plan:** Walkthrough and sample visitor/badge records; spot-check camera coverage.

6.12 Planning (PL)

Intent: Establish and maintain a coherent security and privacy plan.

Minimums: SSP; policies/standards; resource assignment; strategy and objectives.

Implement — Procedural: Security strategy; risk appetite; governance cadence; exception process; periodic plan updates.

Implement — Technical: Policy-as-code checks in CI/CD; document management with versioning.

Implement — Contractual: Governance/reporting clauses with key providers.

- **Evidence:** Policies; SSP; meeting minutes; exception register; plan versions.
- **Metrics:** Policy review ≤12 months; exception aging; SSP updates on change.
- **Common Failure Modes:** Stale SSP; exception sprawl; unclear ownership.
- **Internal Audit Plan:** Verify policy currency and SSP completeness vs boundary and interconnections.

6.13 Program Management (PM)

Intent: Run security and privacy as an organization-wide program.

Minimums: Governance structure; roles; enterprise risk management; budgeting; enterprise metrics.

Implement — Procedural: Charter boards; define KPIs; portfolio POA&M oversight; communication plan.

Implement — Technical: Enterprise dashboards; asset/identity baselines; automated control checks.

Implement — Contractual: Enterprise obligations into supplier contracts; reporting and audit rights.

- **Evidence:** Charters; program KPIs; portfolio POA&M; budget plans.
- **Metrics:** KPI attainment; portfolio risk trend; audit closure timeliness.
- **Common Failure Modes:** Fragmented ownership; no enterprise view; reactive resourcing.
- **Internal Audit Plan:** Review program charters, KPIs, funding alignment, and portfolio closures.

6.14 Personnel Security (PS)

Intent: Ensure trustworthy personnel and clean separations.

Minimums: Screening by role; NDAs; re-checks for elevated access; timely terminations.

Implement — Procedural: Tiered background checks; offboarding checklist; periodic re-screening; insider risk awareness.

Implement — Technical: Automated deprovision; badge disable sync; device wipe; residual access scans.

Implement — Contractual: Vendor screening equivalency; attestations.

- **Evidence:** Screening records; offboarding tickets; badge logs; access removal proofs.
- **Metrics:** Deprovision ≤24h; lingering access = 0; screening completeness by role.
- **Common Failure Modes:** Manual offboarding; stale accounts; inconsistent screening.
- **Internal Audit Plan:** Sample 10 exits and 10 elevated-role changes.

6.15 PII Processing & Transparency (PT)

Intent: Process personally identifiable information lawfully, minimally, and transparently.

Minimums: Purpose specification; data minimization; transparency notices; consent where required; individual participation where applicable.

Implement — Procedural: Records of processing; privacy impact assessments; DPIA triggers; notice and choice governance; complaint handling.

Implement — Technical: Data tagging/classification; access controls; retention and deletion automation; consent signals integration; de-identification where appropriate.

Implement — Contractual: Privacy obligations and flow-down; subprocessor transparency; breach/privacy notice SLAs.

- **Evidence:** Processing records; privacy notices; DPIAs; consent logs; deletion reports.
- **Metrics:** DPIA completion rate; deletion SLA adherence; minimization exceptions; requests handled on time.
- **Common Failure Modes:** Over-collection; opaque notices; stale data; unmanaged trackers.
- **Internal Audit Plan:** Review processing records for a sample of systems; verify notices, consent handling, and deletion proofs.

6.16 Risk Assessment (RA)

Intent: Identify and treat security and privacy risk systematically.

Minimums: Periodic assessments; threat/vulnerability intel; business context; documented treatment.

Implement — Procedural: Enterprise risk register; system risk logs; treatment plans feeding POA&M; risk acceptance criteria.

Implement — Technical: Vulnerability scanning; threat modeling; external attack surface monitoring; scenario analyses.

Implement — Contractual: Vendor risk due diligence and monitoring cadence.

- **Evidence:** Risk reports; scan results; decisions and dates; treatment closure proofs.
- **Metrics:** Critical/high findings mitigated within SLA; residual risk trend; acceptance expirations.
- **Common Failure Modes:** Snapshot-only reviews; no linkage to remediation; stale acceptances.
- **Internal Audit Plan:** Trace 5 high-risk items from discovery to closure or time-bound acceptance.

6.17 System & Services Acquisition (SA)

Intent: Procure and build securely from the outset.

Minimums: Security requirements in sourcing; SDLC gates; supplier assurance and vulnerability disclosure.

Implement — Procedural: Security non-functional requirements; threat modeling; security acceptance criteria; release gating.

Implement — Technical: IaC pipelines with SAST/DAST/SCA; artifact signing; reproducible builds; secrets scanning.

Implement — Contractual: Breach SLAs; vulnerability disclosure; SBOM delivery; pen-test rights; right to remediate.

- **Evidence:** RFP/SOW security terms; pipeline logs; pen-test summaries; supplier attestations; SBOMs.
- **Metrics:** % releases passing security gates; third-party issues closed on schedule; SBOM coverage.
- **Common Failure Modes:** Late security in SDLC; weak supplier terms; missing SBOMs.
- **Internal Audit Plan:** Sample 3 acquisitions and 3 releases for artifacts and gates.

6.18 System & Communications Protection (SC)

Intent: Protect data and system boundaries.

Minimums: Strong cryptographic protocols; encryption at rest; boundary defenses; segmentation; egress control.

Implement — Procedural: Key management SOP; network zoning; secure API rules; data egress policy; hardening standards.

Implement — Technical: WAF; IDS/IPS; micro-segmentation; KMS with rotation; DNS security; email protections; DLP where appropriate.

Implement — Contractual: CSP/KMS responsibilities; egress controls; logging and alerting commitments.

- **Evidence:** Cipher configs; key rotation logs; segmentation diagrams; WAF/IDS rules; egress/ACL records.
- **Metrics:** % strong cipher usage; boundary incidents; key rotation SLA; segmentation exceptions.
- **Common Failure Modes:** Legacy ciphers; flat networks; unmanaged keys; open egress.
- **Internal Audit Plan:** Validate cipher suites; inspect segmentation against inventory; review egress rules and exceptions.

6.19 System & Information Integrity (SI)

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

Minimums: Patch management; anti-malware; integrity checks; alerts; exception handling.

Implement — Procedural: Patch SLAs by severity; exception register; integrity baselines; vulnerability management process.

Implement — Technical: EDR/AV; file integrity monitoring; vulnerability scanning; anomaly detection; memory protection.

Implement — Contractual: Vendor patch timelines; supported software only; vulnerability notifications.

- **Evidence:** Patch dashboards; EDR/FIM coverage; exceptions; scan results; remediation tickets.
- **Metrics:** Patch SLA adherence; EDR/FIM coverage ≥99%; mean time to patch critical; exception aging.
- **Common Failure Modes:** Shadow IT; unsupported OS; stale exceptions; scanning blind spots.
- **Internal Audit Plan:** Sample 20 hosts for patch level and coverage; verify exception justifications and expiry.

6.20 Supply Chain Risk Management (SR)

Intent: Control third-party and sub-tier risks across the lifecycle.

Minimums: Supplier tiering; security clauses; monitoring; incident/breach data-sharing; exit plans.

Implement — Procedural: TPRM intake; periodic reviews; sub-tier visibility; country-of-origin/sovereignty considerations; offboarding controls.

Implement — Technical: External attack surface monitoring; software integrity verification; code provenance; package/pipeline verification.

Implement — Contractual: Flow-down requirements; right to audit; SBOM and vulnerability disclosure; incident SLAs; continuity/escrow where appropriate.

- **Evidence:** Assessments; contract exhibits; monitoring reports; SBOMs; incident correspondence.
- **Metrics:** % critical vendors reviewed on schedule; high-risk issues >60 days; SBOM coverage; incident notice timeliness.
- **Common Failure Modes:** One-time vetting; no sub-tier visibility; unclear offboarding; weak disclosure SLAs.
- **Internal Audit Plan:** Review 5 critical vendors; verify attestations, SBOMs, incidents, and remediation.

7. Authorization Boundary & Data-Flow Mapping

Describe components, interfaces, trust zones, external services, and data classifications. Maintain records of processing showing sources, stores, transmissions, and recipients. Update on material change; validate quarterly.

8. Baseline & Tailoring Record (Rev. 5 + 53B)

- **Purpose:** A single source of truth for what controls apply and why.
- **Content:**
  - Final baseline (Low/Moderate/High) and any overlays.
  - Row per control: Keep / Add / Withdraw / Compensate, parameter values, rationale, inheritance type (common/hybrid/system).
  - Link to CIS entry and evidence location.
- **Governance:** Reviewed at least annually and on boundary/technology changes; version-controlled.

Example (excerpt):

Control	Baseline	Decision	Parameter(s)	Rationale	Inheritance
AC-2	Moderate	Keep	Inactive lockout 12h; review quarterly	Risk-based session mgmt	System
SC-13	Moderate	Keep	AES-256 at rest; TLS 1.2+	Crypto policy	Common (CSP)
CP-9	Moderate	Keep+Enh	Daily incr; weekly full; immutability 30d	Ransomware resilience	Hybrid

9. Control Parameter Table (Organization-Specific Settings)

Purpose: The “dials” that make controls operational and testable.

Recommended parameters (fill in values):

- **Access & Sessions:** interactive MFA required; admin MFA; session idle timeout; max failed attempts; lockout duration; privileged JIT lifetime.
- **Crypto:** approved ciphers/protocols; key lengths; rotation intervals; HSM/KMS usage.
- **Logging:** required event set; retention period by system tier; clock sync tolerance; alert severities and SLAs.
- **Backups & DR:** RTO/RPO by system tier; backup frequency; immutability window; test cadence.
- **Patching:** critical/high/medium SLAs; reboot windows; exception expiry.
- **Identity:** deprovision ≤24h; service account ownership; secret rotation SLA; device trust requirements.
- **Privacy (PT):** retention schedule; DPIA triggers; consent handling; deletion SLA; transparency notice update cadence.
- **Vendors:** incident notice SLA; SBOM requirement; vulnerability disclosure SLA; right to audit cadence.

10. Evidence Register (Artifacts & Retention)

- **Purpose:** Show, don't tell—know exactly where the proof lives.
- **Structure:** Artifact name, control(s) covered, where stored (repo path, system, dashboard), owner, format, retention period, last updated.

Example (excerpt):

Artifact	Controls	Location	Owner	Format	Retention
Access Recert Q2	AC-2, AC-6	GRC/Recerts/2025Q2	IAM Lead	CSV + sign-off PDF	6 years
SIEM Rule Pack v5	AU-x, IR-5	SecOps/SIEM/rules	SecOps	JSON	Current+1 year
DR Test Report 2025-05	CP-2/4/9	Resilience/Tests/2025-05	DR Lead	PDF	6 years

11. Continuous Monitoring Plan (Frequencies & Automations)

- **Scope:** Controls and artifacts monitored continuously or on a cadence.
- **Frequencies & Examples:**
  - **Daily:** log pipeline health; critical alerts triage; EDR coverage check.
  - **Weekly:** vulnerability scans; failed backups; admin activity review samples.
  - **Monthly:** access recert roll-up; config drift review; patch SLA dashboard.
  - **Quarterly:** DR tabletop; restore drill; segmentation review; vendor attestations check.
  - **Annually:** full internal assessment; risk register refresh; authorization review.
- **Automations:** Health checks for SIEM ingestion, backup success, EDR coverage, encryption states, MFA coverage, and drift—open tickets automatically for failures.
- **Reporting:** Dashboard to AO/CISO; exceptions escalated with owners and dates.

12. POA&M Workflow & Risk Acceptance Criteria

Workflow:

1. Identify weakness or gap (from tests, incidents, or monitoring).
2. Record in POA&M with severity, root cause, owner, due date, milestones.
3. Treat (remediate, compensate, or accept with time bound).
4. Verify closure with evidence.
5. Report status to governance.

Severity & Targets (example):

- **Critical:** fix ≤15 business days; High: ≤30; Medium: ≤60; Low: ≤90 (adjust to your risk tolerance).

Risk Acceptance:

- Allowed only with compensating controls, explicit expiry date, and AO/CISO sign-off.
- Track in register; auto-remind 14 days before expiry.

13. Cloud & Hosting (Shared Responsibility & Inheritance)

- **Decide:** Which controls are inherited, shared, or system-specific.
- **Capture:** Provider authorizations/attestations, service list, data location, KMS/encryption model, logging/egress controls, incident notice SLAs, subprocessor transparency.
- **Verify:** Service-level settings (MFA, logging, encryption, public object access).
- **Integrate:** SSO/MFA; native logging exports; egress restrictions; object ACL governance.

14. Training & Awareness Program (Role-Based)

- **Cadence:** Onboarding ≤30 days; annual refresh; quarterly micro-modules; change-driven updates.
- **Tracks:** Workforce baseline; Admin/IT; Developers (secure coding/SDLC); Security Ops; Executives; Vendors.
- **Measures:** Completion ≥98%; phishing failure trend; remediation ≤10 days; retraining after incidents.

15. Supply Chain Coverage (TPRM overlays, SBOM, disclosure SLAs)

- **TPRM Intake:** Tier suppliers; define required artifacts (attestations, reports).
- **Contracts:** Security/privacy clauses, breach and vulnerability notice SLAs, SBOM delivery, right to audit, sub-tier transparency.
- **Monitoring:** Renewal cadence; external attack surface; incident sharing; change notifications.
- **Offboarding:** Data return/destruction; credential revocation; certificate revocation; logs preserved.
- **Evidence:** Assessments, contracts, SBOMs, incident correspondence, remediation proofs.

16. SDLC Gatekeeping & Pipeline Controls

Where controls live in delivery:

- **Planning:** threat modeling; security NFRs; acceptance criteria.
- **Build:** SAST/SCA; secrets scanning; artifact signing.
- **Test:** DAST; dependency checks; container scans.
- **Release:** change approval; environment drift checks; rollout/backout plans.
- **Operate:** observability, runtime policies, WAF/IDS rules, IaC drift monitors.
- **Gates:** Failing checks block merges/releases unless exception with expiry.
- **Evidence:** Pipeline logs; gate results; exceptions; artifact signatures.

17. Common Pitfalls

- Assuming CSP inheritance without verifying service-level settings.
- Missing parameter values in the SSP (e.g., lockout thresholds, session lifetimes).
- Logging enabled but unused (no alerts/use cases or review cadence).
- Weak joiner–mover–leaver processes; shared credentials; stale service accounts.
- DR plans untested; backups not restorable or co-located.
- Supplier contracts lacking breach/vulnerability/SBOM obligations or sub-tier visibility.
- Overreliance on manual configuration; no drift detection or rollback plans.
- Privileged access not just-in-time or unrecorded; insufficient session controls.
- Patch SLAs undefined or unenforced; unsupported OS/software lingering.
- Incident communications unclear; no forensics readiness or evidence retention plan.

Apptega

18. Quick Reference Summary (Family • Artifacts • Examples)

Area	Core Artifacts	Examples
AC	RBAC matrix; access reviews; PAM/JIT logs	MFA; least privilege; session mgmt
AT	Training matrix; rosters; phishing results	Role-based training; dev secure coding
AU	Log standard; SIEM rules; retention configs	Immutable logs; admin event capture
CA	SAP/SAR; POA&M; auth letter	Continuous monitoring dashboards
CM	Baseline configs; CRs; drift reports	IaC; CIS baselines; SBOM
CP	BIA; DR tests; backup logs	Immutable backups; restore drills
IA	MFA policy; credential rotation; device certs	SSO; PAM; service account controls
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
PE	Badge/CCTV logs; env tests	Visitor mgmt; redundancy
PL	Policies; SSP; charters; exceptions	Strategy; risk appetite
PM	Program KPIs; portfolio POA&M	Governance cadence
PS	Screening; offboarding tickets	JML; badge disable; device wipe
PT	Processing records; DPIAs; notices	Minimization; deletion; consent logs
RA	Risk reports; scans; treatment	Threat modeling; vuln mgmt
SA	RFP security reqs; build evidence	SAST/DAST/SCA; artifact signing
SC	Crypto/KMS records; segmentation	WAF; IDS/IPS; TLS configs
SI	Patch dashboards; EDR/FIM coverage	Integrity checks; anti-malware
SR	TPRM files; contracts; SBOMs	Disclosure SLAs; monitoring

19. References & Resources

NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST SP 800-53B – Control Baselines for Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53b/final

NIST SP 800-53A Rev. 5 – Assessing Security and Privacy Controls in Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

NIST SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST OSCAL (Open Security Controls Assessment Language)
https://csrc.nist.gov/projects/oscal

NIST Privacy Framework
https://www.nist.gov/privacy-framework

NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

NIST SP 800-63-3 – Digital Identity Guidelines
https://pages.nist.gov/800-63-3/

National Vulnerability Database (NVD)
https://nvd.nist.gov/

National Checklist Program (baseline configuration checklists)
https://nvd.nist.gov/ncp/repository

FedRAMP Documents & Templates
https://www.fedramp.gov/documents/

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