Apptega

GUIDE

PCI DSS

Self-Assessment Questionnaire (SAQ) v4.0.1 Compliance Guide

For SAQ-eligible merchants and service providers handling payment cards

Apptega

Apptega

1. Introduction

This guide provides practical, implementation-focused direction to complete a PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ) and become compliant. It aligns people, processes, technology, and third-party arrangements to the 12 PCI DSS requirement areas with clear owners, parameters, measurable acceptance criteria, evidence locations, and SAQ mappings. Use it to prepare accurate SAQ responses and a credible Attestation of Compliance (AOC).

Apptega

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

Days 1-5 — Program stand-up

- Appoint: PCI Program Lead; CDE Owner(s); Network/Cloud Owner; AppSec Lead; Helpdesk Lead; E-commerce Lead; Vendor Risk Lead.
- Establish the **CDE authorization boundary**; draft **CHD/SAD data-flow** diagrams (ingress, storage, transmission, egress, disposal).
- Build the D**ocumentation Set** skeleton: policy index; boundary narrative; SAQ type hypothesis; role responsibilities; risk methodology; requirement summaries.

Days 16-45 — Tailor & implement

- Confirm **SAQ eligibility** and segmentation approach; set control parameters (MFA, logging, encryption, password/lockout).
- Stand up change control, vulnerability scanning, EDR/anti-malware, and log monitoring baselines.
- Draft full narratives for **R1–R12**; map to SAQ questions; identify evidence locations.

Days 46—90 — Evidence & readiness

- Populate the **Evidence Register**; complete an external **ASV scan** cycle (if applicable); perform an internal **self-assessment** and one **tabletop** (e.g., e-commerce defacement).
- Record gaps with owners and due dates in the **Remediation Log**; prepare draft SAQ and AOC.

2. SAQ Eligibility & Scope Determination

Scope. Include all people, processes, systems, and third parties that **store, process, or transmit** cardholder data (CHD) or sensitive authentication data (SAD), plus any system that could impact CDE security (jump hosts, logging/monitoring, domain controllers, web tiers affecting payment pages, etc.

SAQ type quick guidance (choose one primary type with written rationale):

- **SAQ A:** Card-not-present merchants fully outsourcing processing; merchant pages do not receive CHD (hosted iFrame/redirect).
- **SAQ A-EP:** E-commerce site can affect security of a hosted payment page; site does not receive CHD but is in scope due to influence.
- **SAQ B:** Imprint machines or **standalone dial-out** (PSTN) terminals; no electronic CHD storage.
- **SAQ B-IP:** Only **standalone PTS** devices with IP connectivity; no electronic CHD storage.
- **SAQ C-VT:** Only **web-based virtual terminals** on isolated workstations; no electronic CHD storage.
- **SAQ C:** Payment application systems connected to the Internet; no electronic CHD storage.
- **SAQ P2PE:** Using a **PCI-validated P2PE** solution; merchant does not store/process/transmit CHD electronically.
- **SAQ SPoC:** Using a **Software-based PIN entry on COTS** solution as designed; no CHD/SAD storage by merchant.
- **SAQ D (Merchant) / SAQ D (Service Provider):** All other eligible entities not fitting the above.

Eligibility acceptance criteria: Boundary diagram; segmentation description; third-party inventory with PCI status and responsibility matrix; confirmation that **SAD is never stored** post-authorization; executive acknowledgement of SAQ selection.

3. PCI DSS Requirement Narratives (R1—R12)

Each section includes: Intent • Minimums • Implement (Procedural/Technical/ Contractual) • Evidence • Acceptance Criteria • Common Failures • Internal QA Plan • Documentation tie-in.

R1 — Network Security Controls

Intent: Restrict inbound/outbound traffic to only what is required; ensure segmentation where used.

Minimums: Documented rules; deny-by-default; change control; segmentation tested.

Implement:

- **Procedural:** NSC standard; request/approval workflow; quarterly ruleset reviews.
- **Technical:** Layered NSCs (firewalls/WAF/IPS); allow-lists for CDE; egress controls; anti-spoofing; configuration backups.
- **Contractual:** For managed NSC providers—SLAs, change approvals, evidence delivery.
- **Evidence:** Rulesets; change tickets; config backups; segmentation test reports.
- **Acceptance Criteria:** Only required ports/services open; proof of segmentation efficacy; rules reviewed quarterly; no shadow rules.
- **Common Failures:** Any-any rules; stale temporary rules; weak egress.
- **Internal QA Plan:** Sample 10 rules; verify approvals, last-used timestamps, documentation.
- **Documentation tie-in:** Network Security Control Standard; Change Management SOP.

R2 — Secure Configurations

Intent: Harden all system components to reduce attack surface.

Minimums: Baseline configs; change control; unauthorized change detection.

Implement:

- **Procedural:** Baseline standards by platform; image management; exception handling via Targeted Risk Analysis (TRA).
- **Technical:** CIS-aligned baselines; endpoint config mgmt; file integrity monitoring (FIM); removal of default accounts/services.
- **Evidence:** Baselines; drift reports; FIM alerts; exception register.
- **Acceptance Criteria:** 100% in-scope systems on approved baselines; drift remediated or time-bound exceptions.
- **Common Failures:** “Gold image” not maintained; default services left enabled.
- **Internal QA Plan:** Monthly drift sample of 20 endpoints/servers.
- **Documentation tie-in:** Hardening Standards; FIM Procedure.

R3 — Protect Stored Account Data

Intent: Minimize and secure storage of CHD; never store SAD post-authorization.

Minimums: Data minimization; truncation, hashing, or encryption of PAN; key management controls; prohibition on SAD storage.

Implement:

- **Procedural:** Data retention schedule; PAN rendering policies (trunc/mask); key management roles; rotation; backup protection.
- **Technical:** Strong cryptography; tokenization where feasible; masked displays; HSM/KMS; least-privilege access to keys.
- **Evidence:** Data inventory; storage locations; key logs; tokenization architecture; sample displays.
- **Acceptance Criteria:** No SAD anywhere; PAN unreadable at rest; keys protected/rotated; access least privilege.
- **Common Failures:** Logs/backups with clear PAN; unmasked dashboards; orphan keys.
- **Internal QA Plan:** Quarterly search for PAN/SAD; review 3 key lifecycle events.
- **Documentation tie-in:** Data Retention Policy; Cryptographic Key Management SOP.

R4 — Strong Cryptography in Transit

Intent: Protect CHD during transmission over open, public networks.

Minimums: Approved protocols/ciphers; certificate management; secure email/file transfer.

Implement:

- **Procedural:** Standards for in-scope protocols; change approval; certificate lifecycle management.
- **Technical:** TLS 1.2+; HSTS/WAF for web; VPN/private connectivity; secure APIs; disable legacy protocols; mailbox/FTP alternatives.
- **Evidence:** Cipher scans; config snippets; cert inventory; WAF policies.
- **Acceptance Criteria:** 100% public flows encrypted with approved ciphers; no plaintext PAN in transit.
- **Common Failures:** Legacy TLS; email/file share leaks.
- **Internal QA Plan:** Monthly external cipher scan; sample 5 interfaces for packet validation.
- **Documentation tie-in:** Transmission Security Standard.

R5 — Malware Protection

Intent: Protect systems and networks against malware.

Minimums: Malware detection/prevention across endpoints/servers; alert review.

Implement:

- **Procedural:** EDR standard; response playbooks; update cadence.
- **Technical:** Next-gen AV/EDR with behavioral detection; real-time protection; automated quarantine; logging to SIEM.
- **Evidence:** Coverage reports; alert queues; response tickets.
- **Acceptance Criteria:** 100% in-scope endpoints/servers enrolled; critical alerts triaged within SLA.
- **Common Failures:** Exceptions without expiry; offline endpoints.
- **Internal QA Plan:** Monthly coverage audit; sample alert response times.
- **Documentation tie-in:** Endpoint Protection Standard; IR Playbook.

R6 — Secure Systems & Software (SDLC/Change)

Intent: Keep systems/software secure through patching, secure development, and controlled change.

Minimums: Patch management; SAST/SCA/DAST as applicable; change approvals/testing; public-facing app protections.

Implement:

- **Procedural:** Patch SLAs; SDLC checkpoints; CAB; emergency change process; code review policy.
- **Technical:** Automated patching; secrets scanning; dependency mgmt; WAF/virtual patching; signed artifacts; deployment approvals.
- **Evidence:** Patch dashboards; change tickets; code review records; scan results; WAF logs.
- **Acceptance Criteria:** Patching within SLA (e.g., Critical ≤15 biz days); no critical unresolved vulns on public apps; changes approved/tested.
- **Common Failures:** Untracked hotfixes; stale libraries; missing code reviews.
- **Internal QA Plan:** Sample 10 changes; reconcile patch SLA exceptions.
- **Documentation tie-in:** Patch Management Policy; SDLC Standard.

R7 — Access Control by Business Need

Intent: Restrict access to system components and CHD to least privilege.

Minimums: Role-based access; approval workflow; periodic recertifications; restriction for PAN displays.

Implement:

- **Procedural:** JML (joiner/mover/leaver) ≤24h; role catalog; quarterly recerts for privileged roles.
- **Technical:** Centralized IAM/SSO; groups/roles; separation of duties; just-in-time elevation; masking controls.
- **Evidence:** Access requests; role matrices; recertification results.
- **Acceptance Criteria:** 100% users mapped to roles; access recerts ≥95% on time; privileged access time-bound.
- **Common Failures:** Shared admin accounts; orphaned access.
- **Internal QA Plan:** Sample 25 users and 10 admin accounts.
- **Documentation tie-in:** Access Control Policy; JML SOP.

R8 — User Identification & Authentication

Intent: Identify users and authenticate access to system components.

Minimums: Unique IDs; MFA for remote/admin and access to CDE; strong auth parameters.

Implement:

- **Procedural:** Authentication standard; password/lockout parameters; service account governance; MFA coverage targets.
- **Technical:** MFA for remote network access and administrative access; password vaulting; PAM; disable shared/anonymous.
- **Evidence:** MFA coverage reports; PAM logs; password policy configs.
- **Acceptance Criteria:** 100% MFA for remote/admin; unique IDs everywhere; service accounts documented/rotated.
- **Common Failures:** VPN without MFA; shared accounts.
- **Internal QA Plan:** Audit 10 services; verify MFA enforcement.
- **Documentation tie-in:** Authentication Standard; PAM Procedure.

R9 — Physical Security

Intent: Restrict physical access to CDE facilities/devices.

Minimums: Access control mechanisms; visitor management; media handling; video/door logs.

Implement:

- **Procedural:** Facility access policy; visitor escort; media inventory; destruction procedures.
- **Technical:** Badging with logs; CCTV retention; locked racks; secure media destruction and chain-of-custody.
- **Evidence:** Access lists; visitor logs; destruction certificates.
- **Acceptance Criteria:** Physical access limited to authorized; media tracked to destruction.
- **Common Failures:** Shared badges; unlogged visitors.
- **Internal QA Plan:** Quarterly sample of visitor logs and media chain-of-custody.
- **Documentation tie-in:** Physical Security Plan; Media Handling SOP.

R10 — Logging & Monitoring

Intent: Log and monitor access to system components and CHD.

Minimums: Time-synced logs; capture security-relevant events; protect logs; review/alerting.

Implement:

- **Procedural:** Logging standard; use-cases/alert SLAs; retention policy.
- **Technical:** Centralized SIEM; admin/auth events; integrity controls on logs; time sync (NTP).
- **Evidence:** SIEM configs; sample events; retention settings; alert tickets.
- **Acceptance Criteria:** Required events from 100% in-scope systems; alerts triaged within SLA; clock drift within policy.
- **Common Failures:** Logging on but unused; missing admin events.
- **Internal QA Plan:** Validate 5 representative systems end-to-end.
- **Documentation tie-in:** Logging & Monitoring Standard; Alert Runbooks.

R11 — Regular Security Testing

Intent: Validate effectiveness of controls.

Minimums: Quarterly external ASV scans for Internet-facing systems; internal vulnerability scans; penetration testing at least annually and after significant changes; segmentation testing where used.

Implement:

- **Procedural:** VM cycle; remediation SLAs; scope and frequency defined (TRA if customized).
- **Technical:** Authenticated scans; ASV scanning; segmentation tests; pen tests including app/API as applicable.
- **Evidence:** Scan reports (pass/fail and remediation); pen test reports; segmentation test results.
- **Acceptance Criteria:** No high/critical findings unremediated past SLA; passing ASV scans or timely rescan; segmentation efficacy demonstrated.
- **Common Failures:** ASV findings left open; pen test scope too narrow.
- **Internal QA Plan:** Monthly review of open vulns; verify last pen test covered all in-scope components.
- **Documentation tie-in:** Vulnerability Mgmt SOP; Pen Test Methodology.

R12 — Security Policy & Program

Intent: Maintain policies, roles, awareness, risk processes, and incident response supporting the DSS.

Minimums: Documented policies; role training; risk assessments; IR procedures; annual program review.

Implement:

- **Procedural:** Policy lifecycle; training cadence; risk register; IR with payment-brand contact paths.
- **Technical:** Awareness LMS; IR tooling; ticketing for risks and incidents.
- **Evidence:** Policies with revision history; training rosters; risk register; IR exercises and post-mortems.
- **Acceptance Criteria:** Policies current and accessible; 100% in-scope staff trained; two IR exercises/year; risks tracked to closure.
- **Common Failures:** Policies not followed in practice; training gaps.
- **Internal QA Plan:** Audit last two policy updates and the last IR exercise.
- **Documentation tie-in:** Information Security Policy; IR Plan.

4. Cardholder Data Environment (CDE) Boundary & Data-Flow Mapping

Define CDE components, trust zones, interfaces, and all CHD/SAD flows (collection, processing, storage, transmission, archival, disposal). Include payment channels (POS, e-commerce, mail/phone order, virtual terminal), tokenization boundaries, and connections to service providers. Keep diagrams current with change management.

5. Documentation Set — Canonical Narratives (SAQ-Ready)

Write cohesive narratives proving how your program satisfies each applicable PCI requirement and SAQ question for the defined boundary: overview/mission; boundary & inventory; CHD categories and lifecycle; roles/governance; shared responsibility with providers; control implementations (R1–R12); logging/monitoring; vulnerability/patch mgmt; training; incident response; evidence pointers. Maintain versioned releases for assessments.

6. SAQ Selection & Applicability Guidance

Maintain a definitive record: SAQ type and rationale; scoping decisions; segmentation use; third-party matrix; list of inapplicable questions with scope justification; customized approach usage with validation method; evidence links.

Apptega

6A. SAQ Coverage Matrix (All SAQ Types)

Use this matrix to pick the correct SAQ, confirm eligibility, and understand the control focus and evidence needed. Covers 10 SAQ types, including SPoC and P2PE.

SAQ	Who It's For / Eligibility (Summary)	Typical Channels	CHD Stored by Merchant?	SAD Post-Auth Stored?	Merchant Web/App Receives CHD?	CDE Internet-Connected?	Key Control Focus Areas (high level)	Scanning / Testing Expectations	Top Evidence to Prep
A	Card-not-present merchants that fully outsource processing; merchant web pages **do not** receive CHD (hosted iFrame/ redirect).	E-com-merce (hosted pay page), mail/ phone via provider	**No**	**No**	**No**	Often **Yes** (business site), but not CDE	Provider governance, change control, script governance, incident response, policy/awareness	**ASV** only if in-scope public IPs; internal scans typically N/A for CDE	Provider attestations; contracts/ responsibility matrix; evidence merchant site can't capture CHD; script inventory/controls
A-EP	E-commerce merchants whose site affects security of hosted payment page; site does **not** receive CHD.	E-com-merce	**No**	**No**	**No**	**Yes**	Secure SDLC, script mgmt (SRI/ allow-lists), WAF/ monitoring, VM	**ASV** quarterly; internal scans; annual pen test; segmentation tests if used	Web/app inventories; code reviews; WAF logs; ASV & pen test reports
B	Only **imprint** machines or **standalone dial-out** (PSTN) terminals; no electronic CHD storage.	Card-present (PSTN)	**No**	**No**	N/A	**No**	Device control/ inspection, physical security, receipts handling, training	No ASV; targeted device checks	Device inventory; deployment logs; procedures; training & inspection records
B-IP	Only **standalone PTS** devices with IP; no electronic CHD storage; no other systems that could impact devices.	Card-present (IP)	**No**	**No**	N/A	**Yes** (device IP)	Allow-listing, tamper checks, physical security, provider governance	**ASV** if public IPs; internal scans of supporting comps if applicable	Device inventory & tamper logs; network rules; provider attestations
C-VT	**Web-based virtual terminals** only, on isolated, locked-down workstations; no electronic CHD storage.	MOTO via browser VT	**No**	**No**	**Yes** on provider VT page	**Yes** (work-stations)	Endpoint hardening, browser lockdown, EDR, egress controls to VT only, training	**ASV** only if in-scope public IPs; internal scans for VT hosts if applicable	Build standard; EDR coverage; URL allow-lists; training; access reviews
C	Payment application systems **connected to the Internet**; no electronic CHD storage.	POS/app servers	**No**	**No**	Possibly	**Yes**	NSCs/segmentation, hardening/FIM, TLS, logging/SIEM, patching	**ASV** for public IPs; internal scans; pen tests; segmentation tests	NSC rules; baselines; SIEM/ retention; patch/ scan dashboards

Apptega

SAQ	Who It's For / Eligibility (Summary)	Typical Channels	CHD Stored by Merchant?	SAD Post-Auth Stored?	Merchant Web/App Receives CHD?	CDE Internet-Connected?	Key Control Focus Areas (high level)	Scanning / Testing Expectations	Top Evidence to Prep
P2PE	Merchants using a **PCI-validated P2PE** solution; encryption at point of interaction; no electronic CHD storage.	Card-present	**No**	**No**	No (typically)	Often **Yes** (business network), not CDE	Solution listing validation, device/tamper, component mgmt, vendor oversight	**ASV** only if in-scope public IPs; solution-defined testing	Solution listing & implementation evidence; device inventories; provider agreements
SPoC	**Software-based PIN on COTS** solution with approved readers + vendor platform; no CHD/SAD storage by merchant.	Mobile/COTS	**No**	**No**	App per solution (not generic)	**Yes**	Follow solution guide; MDM controls; reader pairing; vendor oversight	Testing per solution; **ASV** if public IPs; fleet/MDM checks	Solution implementation guide; device/MDM inventories; pairing logs; training
D (Merchant)	All other merchants not covered by A/A-EP/B/B-IP/C-VT/C/P2PE/SPoC.	Any	Possibly (minimize)	**No**	Possibly	**Yes**	Full DSS (R1–R12): segmentation, crypto, access/MFA, logging/SIEM, scanning/pen test, key mgmt, IR, policy/training	**ASV** quarterly; internal scans; annual pen test; segmentation tests	Complete Documentation Set; full evidence register across R1–R12
D (Service Provider)	Service providers storing/processing/transmitting CHD for clients or impacting client CDE.	Any	Possibly (minimize)	**No**	Possibly	**Yes**	Full DSS plus provider duties: customer segmentation, logging/retention SLAs, incident notice, crypto/key mgmt at scale	**ASV** quarterly; internal scans; annual pen test; segmentation tests	Responsibility matrices; tenant isolation evidence; IR comms runbooks; attestation package

Notes: No SAD storage post-authorization is universal. ASV applies to public-facing in-scope IPs. Penetration testing applies where in-scope public applications/infrastructure exist. Segmentation testing is required when relying on segmentation.

7. Control Parameter Defaults (Organization-Specific Settings)

- **Authentication:** MFA required for remote network access and all admin access to CDE; password min length 12; lockout 10 attempts/30 min; session idle 15 min.
- **Cryptography:** TLS 1.2+; approved cipher suites; cert rotation ≤13 months; PAN masked by default; PAN at rest encrypted with keys in KMS/HSM; key rotation ≤12 months or per risk.
- **Logging:** Required events (auth, admin, PAN access, config changes); retention ≥12 months; time sync drift ≤5 minutes.
- **Patching:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90; exceptions require TRA with expiry.
- **Scanning/Testing:** Internal scans monthly; **ASV** quarterly (public IPs); pen test annually and after significant change; segmentation tests semiannual.
- **Network:** Deny-by-default; egress allow-listing; WAF on public web apps; DDoS protections for e-commerce.
- **Data Handling:** Prohibit SAD storage; truncate/mask PAN; approved export channels; secure deletion on disposal.
- **Vendors:** Provider PCI status on file; incident notice ≤24–72 hours; responsibility matrix; right-to-audit for material services.

Apptega

8. Evidence Register

Artifact	Requirement(s)	Location/Path	Owner	Forma	Retention
CDE Boundary Diagram & Data Flows	R1–R4	PCI/Boundary/	PCI Lead	PDF/PNG	Current + 1 yr
NSC Rulesets & Reviews	R1	NetSec/NSC/	NetSec	YAML/PDF	1 yr
Hardening Baselines & Drift Reports	R2	Build/Hardening/	Platform	PDF/CSV	1 yr
Data Retention & PAN Rendering Policy	R3	Policy/Data/	Governance	PDF	3 yrs
Key Mgmt Logs & KMS Exports	R3	Crypto/KMS/	Crypto Owner	CSV/PDF	1 yr
TLS Config & Cert Inventory	R4	Net/Web/TLS/	WebSec	CSV/PNG	1 yr
wEDR Coverage & Alerts	R5	SecOps/EDR/	SecOps	CSV/PNG	1 yr
Patch Dashboards & Exceptions	R6	VM/Patch/	SecOps	CSV/PDF	1 yr
Access Requests & Recerts	R7	IAM/Access/	IAM Lead	CSV/PDF	1 yr
MFA Coverage & PAM Logs	R8	IAM/MFA/	IAM Lead	CSV/PNG	1 yr
Visitor Logs & Media Destruction Certs	R9	Facilities/PCI/	Facilities	PDF	1 yr
SIEM Config, Alerts & Retention	R10	SecOps/SIEM/	SecOps	JSON/PDF	1 yr
Vulnerability & ASV Scan Reports	R11	VM/Reports/	SecOps	PDF/CSV	3 yrs
Pen Test & Segmentation Test Reports	R11	Testing/Pen/	AppSec	PDF	3 yrs
Policies, Training Rosters, IR AARs	R12	GRC/Policy/	Governance	PDF/CSV	3 yrs

9. Continuous Monitoring Plan

- **Daily:** SIEM ingestion health; high/critical alerts triage; EDR coverage exceptions; cert expiry <30 days.
- **Weekly:** Vulnerability scan review; NSC change review; MFA/PAM anomalies; website content integrity for e-commerce.
- **Monthly:** Access recert roll-up; baseline drift review; patch SLA dashboard; vendor incident notifications; ASV status (if in quarter).
- **Quarterly:** Ruleset review; ASV scan; segmentation sampling; management review of KPIs.
- **Automations:** Open tickets for ingestion failures, missing EDR/MFA, crypto drift, expired exceptions, failed scans, or untested segmentation.

10. Remediation, Targeted Risk Analyses & Compensating Controls

- **Workflow:** Identify → Log in Remediation Register (severity, owner, due date, milestones) → Treat (remediate/compensate/TRAs) → Verify with evidence → Report.
- **Targeted Risk Analysis (TRA):** Use to justify alternative frequencies or control approaches permitted by PCI DSS; include scope, risk, compensations, validation method, expiration, and management approval.
- **Compensating Controls:** When a stated control cannot be met, document objective, constraints, risk, control design, and evidence demonstrating equivalent protection.

11. E-commerce & Third-Party Service Providers

Define who hosts payment pages, scripts, and SDKs; maintain inventory of all externally loaded scripts; implement subresource integrity or script management; monitor content changes; ensure provider PCI compliance and incident notice timelines; document responsibility matrices; enforce TLS and WAF protections.

12. Training & Awareness (Role-Based)

Covers all in-scope roles including general workforce, helpdesk, network/ infrastructure teams, developers, e-commerce staff, SOC personnel, and executive sponsors. Training is required prior to system access, followed by annual refreshers and targeted sessions after security incidents. Specialized modules address phishing awareness and secure coding where relevant. Success is measured through ≥98% completion rates and a demonstrated reduction in repeat findings.

13. Vulnerability Management & Penetration Testing Program

Scanning cadence (internal monthly; ASV quarterly for public IPs), authenticated scanning for servers/workstations, web app scans for public and key internal sites, and remediation SLAs. Pen tests: annual and after significant changes; include segmentation validation where used; cover app/API as relevant.

14. Network Segmentation & Scoping Practices

Segmentation reduces scope but must be effective and validated: ACLs, firewalls, routing rules, jump hosts, and monitoring. Prove that non-CDE networks cannot impact CDE (no inbound admin, no uncontrolled trust). Document tests and results; retest after changes.

15. Evidence Sampling Plans (Internal QA)

- **Access (R7–R8):** Sample 25 users and 10 admins; verify least privilege, MFA, timely deprovisioning.
- **Changes (R2/R6/R1):** Sample 10 changes; confirm approvals, testing, rollback, and deployed state vs baseline.
- **Logging (R10):** Sample 5 CDE systems; verify required events, retention, and alert handling.
- **Vulnerabilities (R11):** Sample 20 hosts; verify patch SLA adherence and exception expiry; confirm passing ASV where applicable.
- **Cryptography (R3/R4):** Inspect 3 key lifecycle events and 3 TLS endpoints; validate PAN rendering and cert currency.
- **Physical (R9):** Review one month of visitor logs and two media destruction events.

16. Common Pitfalls

- Selecting SAQ A when site code can modify payment page content, instead of properly declaring SAQ A-EP.
- Assuming a service provider's PCI compliance automatically covers inherited controls without validation.
- Storing sensitive authentication data (SAD) in logs, cache, or transient system folders.
- Failing to enforce multi-factor authentication (MFA) for remote access or administrative accounts.
- Implementing logging but neglecting timely alerting, correlation, or active review.
- Leaving Approved Scanning Vendor (ASV) scan failures unaddressed or unresolved.
- Limiting penetration test scope by excluding APIs, third-party integrations, or segmentation validation.
- Allowing unrestricted outbound traffic (egress), increasing risk of cardholder data exfiltration.

17. Quick Reference Summary

Area	Core Artifacts	Examples
R1	NSC rulesets; segmentation tests	Allow-list; deny-by-default; WAF
R2	Baselines; FIM/drift reports	CIS alignment; exception register
R3	Data inventory; key logs	Tokenization; masked displays
R4	TLS configs; cert inventory	HSTS; strong ciphers
R5	EDR coverage; alerts	Quarantine; triage SLAs
R6	Patch dashboards; code reviews	SAST/SCA/DAST; signed builds
R7–R8	Role matrix; MFA/PAM logs	JML ≤24h; JIT elevation
R9	Visitor/media logs	Locked racks; destruction certs
R10	SIEM configs; alerts; retention	Admin/auth events; NTP
R11	ASV/pen/segmentation reports	Authenticated scans; retests
R12	Policies; training; IR AARs	Risk register; program review

18. Self-Assessment & Executive Attestation

Use status: **In Place / In Place with CCW / Not Applicable / Not Tested / Not in Place** (aligned with SAQ scoping).

Tracker (illustrative):

Requirement/ Control	Status	Rationale (for N/A or gaps	Evidence Link	Owner	Action ID
R4 – TLS for Public Endpoints	In Place	—	Net/TLS/Scan_2025Q3.pdf	WebSec Lead	—
R7 – Least Privilege	In Place with CCW	Excessive group membership	IAM/Recerts_Q3.csv	IAM Lead	ACT-2025-017
R11 – ASV Scan	In Place	—	VM/ASV_Q3_Pass.pdf	SecOps	—

Leadership attests that scope is complete, evidence exists for each “In Place,” and all “In Place with CCW” or “Not in Place” items are tracked with assigned owners and remediation timelines in the Remediation Log. **Controls designated as “Not Applicable” are supported by documented scoping rationale and evidence demonstrating that the requirement does not apply to the assessed environment.**

19. References & Resources

PCI SSC Document Library
https://www.pcisecuritystandards.org/document_library

SAQ Forms & Instructions
https://www.pcisecuritystandards.org/saq

Approved Scanning Vendors (ASVs)
https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

P2PE Solutions & Listings
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

SPoC Program Information
https://www.pcisecuritystandards.org/programs/software-based-pin-entry-on-cots

Secure Coding & OWASP Top 10
https://owasp.org/www-project-top-ten/

NVD Vulnerability Database
https://nvd.nist.gov/

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