MandateMind

PCI DSS 4.0.1

SURVIVAL GUIDE

Evidence Automation, Control Mapping,
and Cloud-Ready Compliance Intelligence

MandateMind Intelligence Briefing — August 2026

Strategic briefing • Tactical workbook • Audit-readiness roadmap

About This Guide

About MandateMind

MandateMind is a mandate-aware security intelligence platform built for CISOs, vCISOs, GRC teams, and security leaders who need more than checklist automation. The platform connects mandates, requirements, controls, evidence, intelligence, drift detection, and remediation so teams can understand what their evidence proves and where action is required.

What This Guide Provides

- A corrected view of the 64 new requirements introduced in PCI DSS v4.0, with the v4.0.1 revision clearly distinguished.
- A practical gap-analysis template.
- A control-mapping workbook for cloud and internal controls.
- An evidence-automation playbook with five repeatable patterns.
- AWS, Azure, and GCP evidence collection patterns.
- Customized Approach guidance and a working template.
- SAQ and QSA-readiness considerations.
- A 90-day audit-readiness roadmap.
- Drift detection, maturity scoring, glossary, and appendices.

Who This Guide Is For

- CISOs and security executives
- vCISOs and security consultants
- GRC and compliance directors
- PCI program owners and compliance managers
- Cloud security architects and engineers
- Security engineering and operations teams
- Organizations preparing for a QSA-led assessment

How to Use This Guide

Use this guide as both a strategic briefing and a tactical workbook. Start with the executive summary and 64-requirement inventory, then use the gap analysis and control mapping pages to identify ownership, evidence, and remediation.

Important versioning note

PCI DSS v4.0.1 is a limited revision. PCI SSC states that v4.0.1 added no new or deleted requirements; the 64 new requirements referenced in this guide were introduced in PCI DSS v4.0. All 51 future-dated requirements became effective on 31 March 2025. In 2026, organizations should assess against the current v4.0.1 standard.

Executive Summary

PCI DSS v4.0.1 is the current active PCI DSS version. It is a limited revision of v4.0 that clarifies intent, corrects errors, and adds applicability guidance. It did not create a new set of requirements. The major operational transition was the move to PCI DSS v4.x, which introduced 64 new requirements, 51 of them future-dated until 31 March 2025.

Key Themes

- More explicit validation and evidence expectations.
- Greater use of targeted risk analysis where the standard allows frequency or method flexibility.
- Expanded authentication and MFA expectations.
- New e-commerce payment-page protections for scripts and page-change detection.
- A formal Customized Approach for organizations that can demonstrate security objectives through alternative controls.
- Greater emphasis on scope governance, third-party relationships, and continuous operational awareness.
- A practical need for automation because evidence, configuration, logs, vulnerabilities, and cloud state change continuously.

MandateMind Perspective

MandateMind treats PCI DSS as a living mandate rather than an annual checklist. The operating model is:

Mandate → Evidence → Intelligence → Action → Verified Readiness

The objective is not simply to collect more artifacts. It is to understand whether each artifact actually supports a requirement, detect when the underlying condition changes, and create an auditable path from finding to remediation and verified closure.

What's New in PCI DSS 4.0.1

Overview

PCI DSS 4.0.1 was published in June 2024 as a limited revision. PCI SSC describes it as a release that addresses stakeholder feedback through corrections, clarifications, and additional guidance. There are no additional or deleted requirements in v4.0.1.

Examples of v4.0.1 Clarifications

- Requirement 3: clarified applicability notes and added a Customized Approach Objective for certain PAN-rendering methods.
- Requirement 6: clarified that the 30-day patch language applies to critical vulnerabilities and added applicability guidance for payment-page scripts.
- Requirement 8: added an applicability note concerning phishing-resistant authentication factors and MFA for non-administrative CDE access.
- Requirement 12: clarified several relationships and responsibilities involving third-party service providers.
- Appendix E: removed the Customized Approach sample templates from the standard and points users to PCI SSC templates.
- Appendix G: added definitions including Legal Exception, Phishing Resistant Authentication, and Visitor.

Do not confuse v4.0.1 with the 64 new requirements

The 64 requirement count belongs to the v4.0 release compared with v3.2.1. v4.0.1 is the current limited revision and did not add another 64 requirements.

Current 2026 Position

PCI DSS v4.0 retired on 31 December 2024. The 51 future-dated v4.x requirements became effective on 31 March 2025. Organizations preparing for a 2026 assessment should therefore treat the full v4.0.1 requirement set as effective.

Summary of the 64 New Requirements Introduced in PCI DSS v4.0

All 64 are now effective. The list below is a transition inventory, not a statement that v4.0.1 itself added 64 requirements.

#	Requirement	Theme	#	Requirement	Theme
1	2.1.2	Secure configurations	33	8.6.3	Authentication / MFA
2	3.1.2	Stored account data	34	9.1.2	Physical security
3	3.2.1	Stored account data	35	9.5.1.2.1	Physical security
4	3.3.2	Stored account data	36	10.1.2	Logging / monitoring
5	3.3.3	Stored account data	37	10.4.1.1	Logging / monitoring
6	3.4.2	Stored account data	38	10.4.2.1	Logging / monitoring
7	3.5.1.1	Stored account data	39	10.7.2	Logging / monitoring
8	3.5.1.2	Stored account data	40	10.7.3	Logging / monitoring
9	3.6.1.1	Stored account data	41	11.1.2	Security testing / scanning
10	4.1.2	Transmission cryptography	42	11.3.1.1	Security testing / scanning
11	4.2.1	Transmission cryptography	43	11.3.1.2	Security testing / scanning
12	4.2.1.1	Transmission cryptography	44	11.4.7	Security testing / scanning
13	5.1.2	Malware protection	45	11.5.1.1	Security testing / scanning
14	5.2.3.1	Malware protection	46	11.6.1	Security testing / scanning
15	5.3.2.1	Malware protection	47	12.3.1	Governance / risk / incident response
16	5.3.3	Malware protection	48	12.3.2	Governance / risk / incident response
17	5.4.1	Malware protection	49	12.3.3	Governance / risk / incident response
18	6.1.2	Secure development / e-commerce	50	12.3.4	Governance / risk / incident response
19	6.3.2	Secure development / e-commerce	51	12.5.2	Governance / risk / incident response
20	6.4.2	Secure development / e-commerce	52	12.5.2.1	Governance / risk / incident response
21	6.4.3	Secure development / e-commerce	53	12.5.3	Governance / risk / incident response
22	7.1.2	Access control	54	12.6.2	Governance / risk / incident response
23	7.2.4	Access control	55	12.6.3.1	Governance / risk / incident response
24	7.2.5	Access control	56	12.6.3.2	Governance / risk / incident response
25	7.2.5.1	Access control	57	12.9.2	Governance / risk / incident response
26	8.1.2	Authentication / MFA	58	12.10.4.1	Governance / risk / incident response
27	8.3.6	Authentication / MFA	59	12.10.5	Governance / risk / incident response
28	8.3.10.1	Authentication / MFA	60	12.10.7	Governance / risk / incident response
29	8.4.2	Authentication / MFA	61	A1.1.1	Multi-tenant service providers
30	8.5.1	Authentication / MFA	62	A1.1.4	Multi-tenant service providers
31	8.6.1	Authentication / MFA	63	A1.2.3	Multi-tenant service providers
32	8.6.2	Authentication / MFA	64	A3.3.1	Designated entities validation

Source note: PCI SSC materials identify 64 new requirements in PCI DSS v4.0: 53 applicable to all entities and 11 applicable only to service providers. PCI DSS v4.0.1 did not add new requirements.

Change Categories & Impact Levels

The 64-Requirement Transition Model

Category	Count	Meaning	2026 treatment
New requirements in v4.0	64	Net-new requirements introduced versus v3.2.1.	All effective
Applicable to all entities	53	Requirements broadly applicable across PCI DSS entities.	Assess where in scope
Service-provider-only	11	Requirements specific to service providers.	Assess where applicable
Future-dated	51	New requirements that were initially deferred during the transition period.	Mandatory since 31 Mar 2025
Immediately effective	13	New requirements effective for v4.0 assessments from the start.	Mandatory

Impact Levels for a 2026 Program

Impact	Typical examples	What to do
High	Payment-page script controls; MFA; targeted risk analysis; evidence validation; scope governance.	Assign executive owner, validate evidence, test operating effectiveness.
Moderate	Configuration standards; access governance; logging and monitoring; vulnerability workflows.	Map to technical controls and recurring evidence sources.
Lower	Terminology, applicability, documentation, and process refinements.	Update policies, procedures, templates, and assessment narratives.

MandateMind impact lens

Prioritize by operational exposure rather than requirement numbering alone: CDE access, payment-page integrity, vulnerability exposure, logging, scope, third-party dependencies, and evidence freshness are natural automation candidates.

Gap Analysis Template — Overview

How to Use

- Identify the requirement or sub-requirement and confirm whether it is in scope.
- Document the current operating state, not merely the existence of a policy.
- Identify the actual evidence source and test whether it proves the control objective.
- Rate the gap based on risk, audit impact, and operational exposure.
- Assign a named owner and target date.
- Track remediation through closure and retain evidence of the fix.
- Revalidate the evidence after material changes to systems, cloud services, vendors, or payment flows.

Gap Analysis Questions

- What PCI DSS requirement applies?
- What system, process, people, or third party are responsible?
- What is the defined control?
- What is the actual operating state?
- What evidence proves the control is operating?
- Is the evidence current and complete?
- What changed since the last validation?
- What remediation is required?
- How will closure be verified?

Gap Analysis Worksheet

Requirement	Control Area	Current State	Evidence Status / Gap	Severity	Owner	Target
2.1.2	Secure configurations	Partially documented	Configuration standard exists; cloud exceptions not consistently tracked.	Moderate	Cloud Security	30 days
3.4.2	Protect stored account data	Gap	Remote access control requires technical validation.	High	Security Engineering	30 days
6.4.3	Payment-page script controls	Partial	Script inventory and authorization workflow need formalization.	High	Application Security	21 days
8.4.2	MFA into CDE	Implemented	MFA enforced for identified access paths; evidence refresh required.	High	IAM	14 days
10.4.1.1	Log review	Partial	Automated review exists; exception handling needs documented workflow.	Moderate	SOC	30 days
11.3.1.1	Internal vulnerability scans	Partial	Scanning exists but coverage evidence is incomplete.	High	Vulnerability Mgmt	21 days
11.6.1	Payment-page change detection	Gap	No validated change-detection evidence for all payment pages.	High	AppSec	21 days
12.3.1	Targeted risk analysis	Gap	Frequency decisions are not consistently documented.	High	GRC	14 days
12.5.2	Scope confirmation	Partial	Annual scope review exists; cloud dependency inventory needs expansion.	Moderate	PCI Owner	30 days
12.10.5	Incident response testing	Implemented	Testing completed; next exercise and evidence package scheduled.	Moderate	IR Lead	60 days

Status key: Implemented = operating and evidenced; Partial = operating with evidence or scope weakness; Gap = requirement objective not yet demonstrated.

Control Mapping Workbook — Overview

Purpose

Map PCI DSS requirements to the actual technical and organizational controls that satisfy them. For cloud environments, mapping should identify the cloud-native service, configuration state, evidence source, automation opportunity, and accountable owner.

Recommended Mapping Layers

- PCI DSS requirement → security objective
- Security objective → internal control
- Internal control → cloud or operational mechanism
- Mechanism → evidence source
- Evidence source → automated collection method
- Control → owner and remediation workflow
- Evidence → validation date and freshness expectation

Avoid one-to-one mapping traps

One control can support multiple PCI DSS requirements, and one requirement may require multiple technical and procedural controls. The workbook should preserve those many-to-many relationships.

Control Mapping Matrix

PCI Requirement	Cloud Mapping	Internal Control	Evidence Source	Automated?	Owner
1.2	AWS VPC / Azure NSG / GCP VPC controls	Network Security Standard	Cloud configuration export	Yes	Cloud Security
2.1.2	CIS-aligned cloud baselines	Secure Configuration Standard	CSPM / configuration snapshots	Yes	Cloud Engineering
3.5.1.1	KMS / HSM / encryption services	Cryptographic Key Management	KMS configuration and key reports	Yes	Data Security
4.2.1	TLS configuration	Transport Encryption Standard	Load balancer / endpoint config	Yes	Platform
6.4.3	Payment-page script inventory	E-commerce Script Control	Script inventory / CSP evidence	Partial	AppSec
8.4.2	Identity provider MFA	Authentication Standard	IdP policy export / auth logs	Yes	IAM
10.4	SIEM / log analytics	Logging & Monitoring Standard	SIEM dashboards / review records	Yes	SOC
11.3	Vulnerability scanner	Vulnerability Management	Scan reports / tickets	Yes	Vuln Mgmt
11.6.1	Payment-page integrity monitor	Web Integrity Control	Change alerts / baselines	Yes	AppSec
12.3.1	Targeted Risk Analysis process	Risk Management Policy	TRA register / approvals	Partial	GRC
12.5.2	CDE inventory and data-flow map	PCI Scope Management	CMDB / cloud inventory	Yes	PCI Owner

Evidence Automation Playbook — Overview

Why Automation Matters

PCI DSS evidence is not a static folder. Cloud configurations change, identities change, vulnerabilities are remediated, scripts change, logs move, vendors change, and payment flows evolve. Automation creates repeatability and reduces the risk of presenting stale evidence.

Automation Design Principles

- Collect from authoritative sources whenever possible.
- Preserve timestamps and source metadata.
- Map evidence to controls and requirements automatically.
- Detect changes from a known-good baseline.
- Create exceptions when evidence is missing or stale.
- Route gaps to owners rather than leaving them in a report.
- Capture remediation and revalidation evidence.
- Retain human approval where judgment is required.

Five Evidence Automation Patterns

1. Continuous Configuration Evidence

Pull configuration state from cloud APIs, identity providers, firewalls, endpoint platforms, and security tools on a scheduled basis. Normalize the output and map it to the controls it supports.

2. Evidence-to-Control Mapping

Use a control library to associate artifacts with PCI DSS requirements, control objectives, owners, and evidence freshness. Flag artifacts that do not sufficiently support the expected objective.

3. Drift Detection

Compare current state against approved baselines and prior evidence. Trigger an exception when a material configuration, access, script, policy, or security-control change occurs.

4. Finding-to-Remediation Automation

Create a ticket or workflow when a gap is identified. Assign ownership, target date, severity, and required evidence for closure.

5. Verified Audit Package Generation

Assemble the latest validated evidence, control narratives, exceptions, remediation history, and approvals into an assessor-ready package.

Cloud Evidence Collection Patterns

AWS

- AWS Config snapshots and compliance evaluations
- CloudTrail configuration and event evidence
- IAM users, roles, policies, MFA, and access-key state
- KMS key configuration and rotation evidence
- Security groups, NACLs, VPC routing, and network controls
- GuardDuty, Security Hub, Inspector, WAF, and related security findings
- S3 bucket policies, encryption, public-access state, and logging
- CloudWatch logs, alarms, and retention configuration

Microsoft Azure

- Azure Policy compliance state
- Microsoft Entra ID authentication and MFA configuration
- RBAC assignments and privileged access
- Key Vault configuration and key lifecycle evidence
- NSGs, Azure Firewall, WAF, and network configuration
- Defender for Cloud recommendations and findings
- Storage account security and encryption settings
- Activity Logs and diagnostic settings

Google Cloud

- Security Command Center findings
- Cloud Asset Inventory
- IAM policies and service-account configuration
- Cloud KMS configuration
- VPC firewall rules and network configuration
- Cloud Audit Logs
- Cloud Storage IAM, encryption, and public-access settings
- Organization Policy and Security Health Analytics evidence

Evidence Automation Workflow — Preview

MANDATE	CONTROL	EVIDENCE	INTELLIGENCE	DRIFT	AUTOMATION	READINESS
Requirement identified	Control mapped	Artifact collected	Evidence interpreted	Change or gap detected	Remediation triggered	Closure verified

The operational difference

Traditional compliance workflows often stop at collection and reporting. A mandate-intelligence workflow continues into interpretation, drift detection, remediation, and verified closure.

Customized Approach — Overview

What It Is

The Customized Approach allows an entity to meet the security objective of a PCI DSS requirement through a different method than the Defined Approach, subject to the PCI DSS requirements and applicable validation procedures. It is not a shortcut and does not remove the need to demonstrate that the security objective is achieved.

When It May Make Sense

- Cloud-native architectures that do not map neatly to traditional infrastructure controls.
- Modern identity and access patterns that use phishing-resistant authentication.
- Highly automated environments where a control objective is continuously enforced by software.
- Architectures where the defined approach is technically awkward but the security objective can be demonstrably achieved.

What Good Evidence Looks Like

- Clearly stated security objective.
- Documented method and rationale.
- Risk analysis and threat consideration.
- Defined control design and operating evidence.
- Testing procedures and results.
- Evidence that the customized control is maintained over time.
- Traceable ownership and approval.

Customized Approach Template

Requirement	PCI DSS objective	Customized method	Threat addressed	Evidence	Test method	Owner
6.4.3	Prevent unauthorized payment-page script changes	Automated script inventory + authorization + CSP controls	E-commerce skimming	Script inventory, CSP policy, change logs	Quarterly + event-driven validation	AppSec
8.4.2	Protect CDE access with MFA	Phishing-resistant authentication for supported access paths	Credential theft	IdP policy, auth logs	Access-path validation	IAM
10.4	Detect anomalies in logs	Risk-based automated analytics and alerting	Delayed detection	SIEM analytics, alert history	Use-case test and review	SOC

Template

- Requirement / objective:
- Why the Defined Approach does not fit the architecture:
- Customized security objective:
- Threats and failure modes:
- Control design:
- Implementation evidence:
- Testing method and frequency:
- Responsible owner:
- Approval and review date:
- Ongoing monitoring / drift trigger:

Example principle

Do not describe a customized control as 'better' merely because it is automated. Demonstrate how the method achieves the same security objective and how its effectiveness is tested and maintained.

SAQ Changes

PCI SSC updated the Self-Assessment Questionnaires to align with PCI DSS v4.0.1. Eligibility criteria and completion guidance were refined, and specific SAQs changed in response to requirement applicability.

SAQ	Practical focus	Key consideration
SAQ A	Card-not-present merchants using compliant payment providers	Confirm eligibility and understand the revised eligibility criteria.
SAQ A-EP	E-commerce merchants whose site can affect payment security	Review payment-page security and script-related responsibilities.
SAQ D	Broad merchant or service-provider scope	Expect the largest evidence and control population.
SAQ P2PE	Merchants using validated P2PE solutions	Confirm solution eligibility and responsibilities outside the P2PE scope.
SAQ C-VT	Virtual terminal environments	Validate the actual environment and current SAQ eligibility criteria.

Always verify eligibility

The correct SAQ depends on the entity's actual payment architecture, scope, and eligibility criteria. This guide is not a substitute for the current PCI SSC SAQ instructions or the entity to which the validation is submitted.

QSA Expectations

What Assessors Need to See

- Evidence that is relevant to the requirement being tested.
- Evidence that is sufficiently complete to support the assessment conclusion.
- Evidence that represents the current operating state.
- Clear ownership and responsibility.
- Documented risk analyses where the standard calls for them.
- Testing procedures and test results.
- Traceability between policies, procedures, configurations, evidence, and remediation.
- A credible explanation of scope and third-party dependencies.
- Evidence that exceptions are controlled rather than hidden.

What Creates Friction

- Screenshots without context or timestamps.
- Policies that do not match actual configurations.
- Evidence collected from the wrong environment.
- Stale reports presented as current state.
- Controls marked 'implemented' without operating evidence.
- Unclear responsibility between merchant and third-party service provider.
- Cloud inventories that omit dependencies or ephemeral resources.

90-Day Roadmap — Overview

Three Phases

Phase	Days	Objective	Primary outputs
Discovery	1–30	Understand scope, requirements, evidence, ownership, and gaps.	CDE map, requirement inventory, evidence inventory, gap register
Validation	31–60	Test controls, automate evidence, remediate high-risk gaps.	Validated controls, automation coverage, remediation evidence
QSA Readiness	61–90	Stabilize evidence and run a mock assessment.	Assessor package, narratives, exceptions, final gap closure

Roadmap principle

Do not wait until Day 75 to discover that evidence is unavailable. Build the evidence model in the first 30 days, then improve automation and validation throughout the remaining phases.

Roadmap — Days 1–30: Discovery

Week	Tasks	Deliverables
Week 1	Confirm PCI scope; identify payment flows; inventory CDE and connected systems; identify TPSPs.	Scope statement; payment-flow diagram; initial system inventory
Week 2	Map requirements; identify control owners; collect existing policies and evidence.	Requirement-to-control map; owner matrix
Week 3	Assess evidence quality; identify stale or missing artifacts; baseline cloud configurations.	Evidence register; gap register; baseline evidence
Week 4	Prioritize high-risk gaps; define automation candidates; approve remediation plan.	90-day backlog; automation plan; executive status

Roadmap — Days 31–60: Validation

Week	Tasks	Deliverables
Week 5	Remediate high-risk authentication, scope, payment-page, and vulnerability gaps.	Verified fixes; updated evidence
Week 6	Implement automated evidence collection for cloud, IAM, logging, and vulnerability controls.	Automation connectors; scheduled collection
Week 7	Test control operating effectiveness; validate evidence-to-control mappings.	Test records; evidence mapping validation
Week 8	Review exceptions; validate third-party responsibilities; update narratives.	Exception register; responsibility matrix; draft assessment package

Roadmap — Days 61–90: QSA Readiness

Week	Tasks	Deliverables
Week 9	Run mock assessment; challenge evidence; sample high-risk requirements.	Mock assessment findings
Week 10	Close remaining gaps; refresh evidence; resolve evidence-quality issues.	Closure evidence; refreshed evidence set
Week 11	Prepare narratives, scope documentation, exception rationale, and testing records.	Assessment-ready package
Week 12	Executive review; QSA pre-read; final readiness score; establish continuous process.	Readiness sign-off; recurring evidence plan

End-state

The target is not a static '100%' dashboard. The target is a defensible operating process in which changes create evidence, evidence maps to requirements, gaps create action, and remediation creates new evidence.

Common Pitfalls

1. Treating v4.0.1 as a brand-new standard

v4.0.1 is a limited revision. The 64 new requirements were introduced in v4.0.

2. Collecting evidence without interpreting it

A screenshot or report is not automatically proof. Validate what the artifact demonstrates.

3. Ignoring payment-page script controls

For applicable e-commerce environments, Requirements 6.4.3 and 11.6.1 deserve explicit engineering attention.

4. Treating cloud scope as static

Cloud services, identities, integrations, and data paths change. Scope needs recurring validation.

5. Marking controls implemented without operating evidence

A policy can describe an intended state while the environment operates differently. Test the actual state.

Drift Detection

Types of Drift

Drift type	Example	Evidence trigger
Configuration	Security group opens an unexpected port.	Cloud configuration diff
Identity	Privileged role gains a new assignment.	IAM event / policy diff
Application	Payment page loads an unapproved script.	Script inventory / integrity alert
Vulnerability	Critical vulnerability appears on an in-scope asset.	Scanner / asset telemetry
Logging	Audit logging disabled or retention changed.	Cloud/SIEM configuration diff
Scope	New cloud service enters a payment-data flow.	Asset discovery / data-flow change
Third party	TPSP changes a service or responsibility boundary.	Contract / service review

Why It Matters

A control can be compliant at the time it is tested and non-compliant later because the environment changed. Drift detection closes the gap between assessment evidence and current operational truth.

MandateMind insight

Treat material drift as an evidence event. A meaningful change should trigger reassessment of the affected control, not merely a new ticket.

MandateMind 5-Level Maturity Model

Level	Name	Characteristics	Evidence state
1	Ad Hoc	Manual, inconsistent, reactive.	Evidence is fragmented or missing.
2	Documented	Policies and procedures exist; execution varies.	Evidence exists but is largely manual.
3	Managed	Owners, recurring reviews, and repeatable processes are established.	Evidence is structured and traceable.
4	Measured	Controls are monitored, scored, and tested continuously.	Evidence is refreshed and mapped automatically where possible.
5	Intelligent	Mandates, evidence, drift, remediation, and readiness are connected.	Operational truth drives continuous readiness.

Scoring Guidance

- Score the operating process, not the quality of the policy document.
- Use evidence freshness and completeness as part of the score.
- Downgrade maturity when ownership is unclear.
- Downgrade maturity when drift is discovered but not automatically detected.
- Use remediation closure and revalidation as indicators of operational maturity.

Cloud Control Validation Workflows

AWS Workflow

- Discover in-scope accounts, regions, resources, identities, and payment flows.
- Pull configuration evidence from AWS Config, CloudTrail, IAM, KMS, security services, and network controls.
- Normalize evidence against the PCI control library.
- Flag deviations and create remediation workflows.
- Re-collect evidence after remediation and retain the before/after record.

Azure Workflow

- Inventory subscriptions, resource groups, identities, and CDE-connected services.
- Collect Azure Policy, Entra ID, RBAC, Key Vault, network, Defender, and Activity Log evidence.
- Map configuration state to PCI controls.
- Route deviations to responsible owners.
- Revalidate and preserve closure evidence.

GCP Workflow

- Inventory projects, folders, organization policies, service accounts, and CDE-connected resources.
- Collect IAM, Cloud KMS, VPC, Audit Logs, SCC, Asset Inventory, and storage evidence.
- Normalize and map to PCI control objectives.
- Detect drift and trigger remediation.
- Revalidate after changes and retain evidence history.

Glossary

Term	Definition
CDE	Cardholder Data Environment; the systems and components subject to PCI DSS scope.
CSP	Cloud Service Provider.
Customized Approach	A PCI DSS validation method that uses an alternative method to achieve the security objective of a requirement.
Defined Approach	The standard PCI DSS method of meeting a requirement using the defined requirements and testing procedures.
Evidence	An artifact or record used to demonstrate that a requirement or control is operating as expected.
Future-dated requirement	A v4.0 requirement that was initially designated as a best practice during the transition period and became effective on 31 March 2025.
MFA	Multi-factor authentication.
PAN	Primary Account Number.
QSA	Qualified Security Assessor.
ROC	Report on Compliance.
SAQ	Self-Assessment Questionnaire.
Scope	The people, processes, technology, locations, and third parties included in the PCI DSS assessment.
TPSP	Third-Party Service Provider.
TRA	Targeted Risk Analysis.
Drift	A material change between an approved or previously validated state and the current operating state.
Evidence Intelligence	The process of interpreting evidence to determine what it proves, what it supports, what is missing, and whether it remains current.

Appendix A — Suggested Evidence Register Fields

- Evidence ID
- PCI requirement / control
- Evidence type
- Source system
- Collection timestamp
- Owner
- Coverage period
- Freshness status
- Validation status
- Exception / remediation link

Appendix B — Recommended Assessment Package

- Current PCI DSS scope statement and data-flow diagrams
- Requirement-to-control mapping
- Evidence register
- Policies and procedures
- Configuration and technical evidence
- Vulnerability and penetration-testing evidence
- Logging and monitoring evidence
- Risk analyses
- Third-party responsibility matrix
- Remediation and closure evidence

Appendix C — Primary References

- PCI Security Standards Council — PCI DSS v4.0.1, June 2024.
- PCI Security Standards Council — Summary of Changes from PCI DSS v4.0 to v4.0.1, August 2024.
- PCI Security Standards Council — PCI DSS v4.0.1 SAQs and SAQ Instructions and Guidelines.
- PCI Security Standards Council — Guidance for Compensating Controls and the Customized Approach, June 2026.