

Building Continuous PCI DSS Compliance With AI

PCI SSC APAC Community Meeting, 2026

Amol Sawant

SVP, ControlCase



Agenda

1. Why Point-in-Time Compliance No Longer Works
2. Where AI Actually Helps — Use Cases
3. Where To Be Careful — Risk and Governance
4. The Auditor's View — What Changes for Assessors
5. Getting Started Without Getting Burned

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Why Point-in-Time Compliance No Longer Works

Part 1

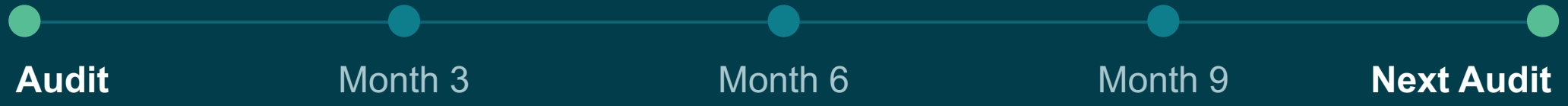




The Point-in-Time Compliance Paradox

A Passing ROC Proves One Moment — Not the 364 Days That Follow

CONTROL DRIFT ACCUMULATES HERE



Traditional Annual Audit

- Proves control status at a single moment during audit week
- Creates a false sense of security for the rest of the year
- Evidence is stale the day after the ROC is signed

The Compliance Latency Gap

- Infrastructure drift, firewall edits, IAM and cloud changes happen daily
- Latency is the time between a control failing and anyone noticing
- Closing that gap — not a faster report — is the real objective

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The PCI DSS v4.0.1 Paradigm Shift

The Standard Changed the Question an Assessor Asks

1 Early versions	2 v3.x	3 v3.2.1	4 v4.0.1
"Is the control implemented?"	"Implemented and operating effectively?"	"Critical controls validated often enough?"	"How often tested, based on risk?"



The assessment is a snapshot. Your controls don't have to be. PCI DSS sets the minimum cadence — targeted risk analysis and the Customized Approach let you go beyond it.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

What Standards Bodies and Surveys Say

Five Independent Sources, One Direction of Travel

PCI SSC	AI can assist assessments — but AI is a tool, not an assessor
NIST	IR 8011 identifies testable controls; OSCAL makes them machine-readable
PwC	82% plan more compliance-technology investment; 71% expect AI to help
IIA	Continuous auditing plus continuous monitoring equals continuous assurance
Gartner	Compliance automation is now a defined technology market

Machine-readable controls → automated tests → AI analysis → human assurance

Sources: PCI SSC AI Principles (2025); NIST IR 8011 / OSCAL; PwC Global Compliance Survey 2025 (1,802 executives); IIA GTAG; Gartner (2025)

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

From Periodic Audit to Continuous Assurance

Four Words We Use Interchangeably — And Should Not

Continuous Monitoring

Telemetry detects environment change.

›

Continuous Testing

Automated tests verify the control still works.

›

Continuous Compliance

Evidence is generated and mapped live.

›

Continuous Assurance

Management and the QSA hold confidence all year.

“The annual assessment should validate the compliance programme — not create it.”

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Where AI Actually Helps

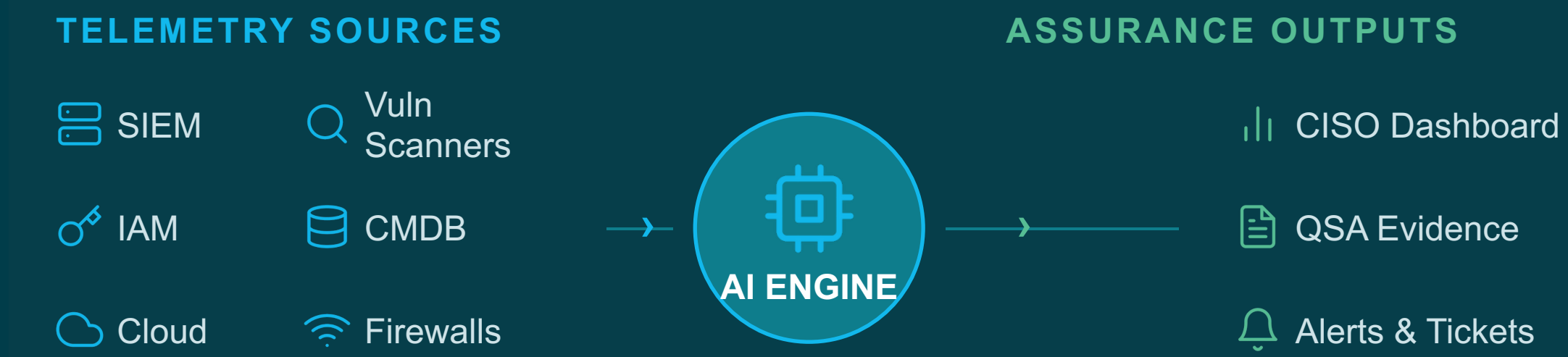
Part 2





AI and Continuous Compliance Architecture

Six Telemetry Sources, One Engine, One Assurance View



Compliance becomes telemetry-driven instead of paper-driven.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Use Case 1: Continuous Evidence Intelligence

Requirement 3 and Requirement 8 — Finding Real Evidence in Unstructured Noise

TRADITIONAL EVIDENCE COLLECTION

Request › Manual search › Screenshot › Review › Finding

AI-ASSISTED INTELLIGENCE

Continuous pull › AI ingestion › NL parsing › Control mapping

Contextual PAN discovery

Tells a real PAN from a tracking number or SKU.

Config-to-requirement mapping

Maps SSH, RDP and IAM settings to Requirement 8.

Scope creep prevention

Surfaces cardholder data outside the CDE.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Use Case 2: Configuration and Change Testing

Catching Drift the Day It Happens

SCENARIO

Yesterday: port 443 exposed

Today: port 22 open to the internet

Ticket raised in minutes, not months

Configuration Drift Alerting

Baselines firewall rules, cloud security groups and exposed management ports

Instant PCI DSS Impact Analysis

Names the requirement the change breaks and checks for a change ticket

Payment Page Script Integrity (6.4.3)

Baselines payment-page JavaScript — direct Magecart and formjacking defence

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Use Case 3: Cross-Domain Correlation and TPSP Oversight

Context Based Correlation Is The Key

Siloed Data Synthesis

One context graph from CMDB, firewall logs and scans.

- Single correlated view, not five consoles
- Asset classification travels with the log
- Removes manual cross-referencing

TPSP Oversight

Tracks AOC expiries and shared responsibility.

- Flags AOCs before they lapse
- Maps vendor scope to your requirements
- Keeps Req 12.8 / 12.9 evidence current

Scope Leak Detection

Flags unauthorised paths into the CDE.

- Detects silent scope expansion
- Surfaces undocumented CDE routes
- Protects segmentation assumptions

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Use Case 4: Predictive PCI DSS Compliance

The Most Exciting Use Case — and by Far the Least Mature

THE SHIFT From “Are we compliant today?” › **to “Which controls are likely to fail next?”**

Telemetry Inputs

- Repeat audit findings and exceptions
- Vulnerability patch latency trends
- Configuration drift frequency
- Turnover in administrator teams

Intended Output

- Ranked forecast of likely failures
- Weeks of warning before the audit
- Remediation before sampling begins
- Fewer pre-audit fire drills

Most tools today detect and correlate compliance issues; AI-driven monitoring enables a shift toward predictive compliance.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Where To Be Careful

Part 3





AI Is Not the Control

AI Advises — the Assessor Decides

Control › **Telemetry** › **Deterministic Engine** › **AI Analysis** › **Human Judgement**

What AI Should Never Do

- Independently declare “Requirement X = compliant”
- Replace human risk ownership or executive accountability
- Override QSA or ISA professional judgement

Where AI Delivers Real Value

- Collect and classify — turn messy logs into evidence
- Correlate and detect — spot anomalies humans miss
- Recommend — prioritise remediation for security teams

Source: PCI SSC, “AI Principles: Securing the Use of AI in Payment Environments” — AI use does not remove the need to meet any applicable PCI DSS requirement.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The New Risk Surface: AI Is Also an Exposure

Your AI System Is Now in Scope

Cardholder data pasted into public AI tools

Platforms now ship browser-layer DLP to block this in real time — a productised risk, not a theory.

Your audit evidence holds personal data

Access reviews carry names, logs carry user IDs. Feeding that to AI needs a lawful basis.

The AI system is now in your scope

Touch CDE telemetry and it inherits Requirement 10 logging and access control.

Scope your AI system before you scope your AI use case.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Public Versus Private AI

Residency Is a Compliance Decision

Enterprise Public AI (SaaS)

PROS

- Rapid deployment, no infrastructure build
- Frontier model reasoning

CONSIDERATIONS

- Cardholder-data exposure risk
- Residency and sovereignty constraints

Private Local AI (On-Prem / Enclave)

PROS

- CDE evidence never leaves your control
- Full data sovereignty

CONSIDERATIONS

- Higher infrastructure investment
- Slower to stand up than SaaS

In APAC and MEA, residency rules make private or enclave the realistic start.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

What Do Regulators Actually Require?

Regulated, Not Required

No regulator mandates AI in testing or auditing.

India — RBI FREE-AI

Advisory (Aug 2025). AI inventory, board policy, risk-based audits.

Singapore — MAS AIRG

Consultation (Nov 2025). Board accountability, lifecycle controls.

UAE — CBUAE

Bias testing, continuous monitoring, audit rights over providers.

The only automation mandate is PCI DSS 10.4.1.1 — and automation is not AI.

Sources: RBI FREE-AI (Aug 2025); MAS consultation (Nov 2025); CBUAE AI/ML guidance. Positions evolve — verify before citing.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Auditor's View

Part 4



The QSA Audit Transformation

Most Assessment Effort Today Is Administrative, Not Analytical

~60% of engagement effort sits in fieldwork

150 - 200 internal person-hours per assessment cycle

Traditional Assessment Model

- Assessor time spent chasing and organising paperwork
- Testing restricted to small samples by manual time limits
- Findings surface late, when remediation is most expensive

AI-Assisted Assessment Model

- Evidence pre-organised and correlated before kickoff
- Population testing replaces small-sample extrapolation
- Professional judgement elevated, paperwork reduced

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The AI-Assisted QSA Workflow

The Assessor Sees Only What Needs Judgement

1. Continuous evidence repository
Evidence streams in all year.

2. AI pre-analysis
Scans for completeness and gaps.

3. Exception highlighting
Points straight to the outliers.

4. Targeted QSA testing
Judgement where humans add most value.

EVIDENCE REVIEW QUEUE

Auto Validated by AI 4

- Firewall rulesets
- IAM access reviews
- Patch records
- Script integrity

Needs QSA judgement 2

- ⚠ Port 22 exposure
- ⚠ TPSP AOC expired

AI is the assessor's second pair of eyes — never the second signature.

20 YEARS OF SECURING PAYMENT DATA

Governance: Trust and Auditability

The AI System Itself Becomes an Audit Object

Traceability

Every AI conclusion cites the raw source telemetry it came from.

Reproducibility

Deterministic engines, not the model, enforce pass or fail.

Complete Audit Log

Every prompt, model version and override is permanently logged.

Named Human Owner

An accountable assessor reviewed and accepted it.

PCI SSC is explicit that AI outputs are non-deterministic and can drift.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Getting Started Without Getting Burned

Part 5



The Continuous Compliance Maturity Curve

Where Does Your Organisation Sit — and Where Does the Value Start?

1 Manual

Periodic evidence gathering and manual sampling.

2 Automated

Script-based evidence extraction.

3 Continuous

Control monitoring and drift detection.

4 AI-Assisted

AI correlates evidence and flags anomalies.

5 Predictive

AI forecasts control degradation.

Most enterprises sit between Level 2 and Level 3 today.

Staging mapped to the NIST ISCM scale (SP 800-137 / 800-137A), as operationalized in the IG FISMA maturity model. No PCI DSS-specific maturity model exists.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Practical Implementation Roadmap

Do Not Buy an “AI Compliance Tool” on Day One — Build the Foundation First

PHASE 1
Telemetry

- Identify monitorable controls
- Connect evidence APIs
- Asset inventory

PHASE 2
Automation

- Deterministic test scripts
- Automate evidence ingestion
- Standardise formats

PHASE 3
AI Layer

- Cross-domain correlation
- Anomaly detection
- Automate TRA tracking

PHASE 4
Assurance

- Continuous CISO dashboards
- QSA-ready evidence
- Human-in-the-loop sign-off

⚠ **Skipping straight to Phase 3 is the most common reason pilots fail.**

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Business Case for Adopting AI

Build It on Latency and Reclaimed Effort, Not Headline Savings

Compliance latency

Req 10.4.1.1 turns evidence from an annual snapshot into live telemetry.

Cost avoidance

Evidence gathering is the most automatable line in the budget.

Engineering time returned

No more screenshot-chasing blitzes before every audit window.

Reduced breach exposure

Shorter drift discovery shrinks the attacker's window.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Key Takeaways

Five Things To Carry Out of This Room

1. Continuous compliance is an operating model — PCI DSS does not mandate it
2. AI is a tool, not an assessor — the signature never moves
3. Scope your AI system before you scope your AI use case
4. No regulator mandates AI; all of them regulate how you use it
5. Build telemetry first — the AI layer is Phase 3, never Phase 1

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Your Next Assessment - AI Will Sit on Both Sides of the Table

Thank You



