Beyond Audit Season: How to Scale PCI DSS Evidence, Visibility, and Readiness

PCI North America Community Meeting

From Screenshot Evidence to Continuous Compliance Signals



Aaron Reynolds, CISSP, QSA
COALFIRE



David Cook
COMCAST

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Assessment-Led Compliance: The Old Model

Compliance was demonstrated periodically – not managed continuously

- Point-in-time Validation = Point-in-time Compliance
- Annual checkpoint instead of continuous visibility
- Reactive rather than operational
- Control weakness surfaces late, when remediation is most disruptive

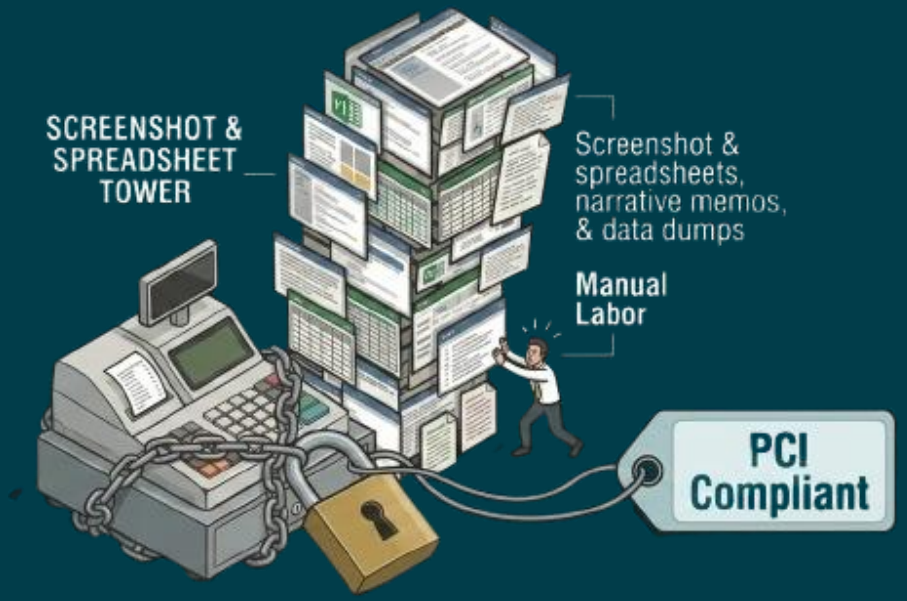


20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Challenges in Today's PCI DSS Assessments

The Problem Isn't Collecting Evidence – It's Operating Compliance at Scale

- Fire-drill behavior
- Spreadsheet chaos
- Evidence inconsistency and refresh
- Audit appeasement overhead
- Rework + compliance risk

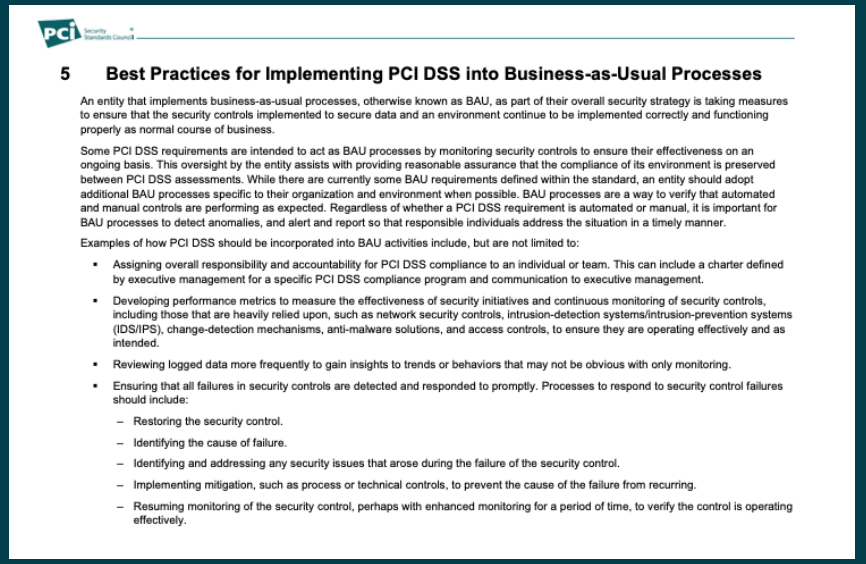


20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Industry Shift Is From Point-in-Time Compliance to Business-as-Usual Compliance

Readiness improves when compliance work follows normal operating rhythms.

- BAU Compliance introduced in PCI DSS v3.0 (Nov 2013)
- PCI DSS v4.0 operationalizes BAU Compliance
- Improved compliance visibility
- Longer remediation windows
- Less Deadline-driven chaos



PCI Security Standards Council

5 Best Practices for Implementing PCI DSS into Business-as-Usual Processes

An entity that implements business-as-usual processes, otherwise known as BAU, as part of their overall security strategy is taking measures to ensure that the security controls implemented to secure data and an environment continue to be implemented correctly and functioning properly as normal course of business.

Some PCI DSS requirements are intended to act as BAU processes by monitoring security controls to ensure their effectiveness on an ongoing basis. This oversight by the entity assists with providing reasonable assurance that the compliance of its environment is preserved between PCI DSS assessments. While there are currently some BAU requirements defined within the standard, an entity should adopt additional BAU processes specific to their organization and environment when possible. BAU processes are a way to verify that automated and manual controls are performing as expected. Regardless of whether a PCI DSS requirement is automated or manual, it is important for BAU processes to detect anomalies, and alert and report so that responsible individuals address the situation in a timely manner.

Examples of how PCI DSS should be incorporated into BAU activities include, but are not limited to:

- Assigning overall responsibility and accountability for PCI DSS compliance to an individual or team. This can include a charter defined by executive management for a specific PCI DSS compliance program and communication to executive management.
- Developing performance metrics to measure the effectiveness of security initiatives and continuous monitoring of security controls, including those that are heavily relied upon, such as network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), change-detection mechanisms, anti-malware solutions, and access controls, to ensure they are operating effectively and as intended.
- Reviewing logged data more frequently to gain insights to trends or behaviors that may not be obvious with only monitoring.
- Ensuring that all failures in security controls are detected and responded to promptly. Processes to respond to security control failures should include:
  - Restoring the security control.
  - Identifying the cause of failure.
  - Identifying and addressing any security issues that arose during the failure of the security control.
  - Implementing mitigation, such as process or technical controls, to prevent the cause of the failure from recurring.
  - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Pre-Assessment Activities

- Validate in-scope assets and scoping tags on a defined cadence
- Verify application owners and key contacts
- Create interview invite templates
- Standardized data flow template for each application
- Come to meeting prepared with data elements
- Last 5 minutes of an interview is important

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Start Identifying Data Elements

- Cleaning and Rationalizing Historical Evidence
- Build a PCI Knowledge Base
- Identify Quick Wins across all Assessments via read-only access and API access
  - Inventory
  - Change Management Tickets
  - Anti-Malware Solution
  - FIM Solution
  - Code Scanning for Bespoke and Custom Software
  - Hardening Standards

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Criteria for a PCI Readiness Assessment

GUI Access w/RBAC and MFA	**Update knowledge base for specific interviews**	**Company guidance to knowledge base**	Evidence Control Templates
Ability to export Controls per individual Readiness Assessment	Support All SAQ types	**API Integrations for quick wins**	Scoring overall and per application
Inventory and Evidence Refresh Rate	Control Exception Capability	**Ability to generate a clear report that's actionable**	

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Screenshots to Signals

From manual evidence to continuous signals with context



Annual Assessment Still Happens, but It Starts From a Better Place

Year-round readiness makes for a smoother and more predictable assessment.

- The annual assessment still matters
- Evidence is captured continuously throughout the year
- Evidence quality improves
- Teams focus on exceptions and remediation

QSA Experience: Annual assessment evidence packaging

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Assessor Partnership Works Best When Expectations Are Aligned Early

Shared expectations make the assessment more predictable.

- Align control and evidence expectations early
- Reduce friction and rework
- Build repeatable evidence practices that scale
- Align on defensible evidence – not artifact volume



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

What Other Organizations Can Reuse

Most organizations can borrow the model before they borrow the tooling.

- Adopt the model before the tooling.
- Establish clear ownership before automating.
- Prioritize readiness and pre-assessment activities.
- Define standard evidence outputs before building collection workflows.
- Connect scope, assets, owners, and signals with shared context.
- Embed compliance into daily operations, not just reporting.
- Engage assessors early to ensure audit-ready evidence.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council