PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Beyond PCI

Leveraging PCI DSS to Drive Multistandards Compliance Success

PCI Security Standards Council

Loïc BREAT

Associate Director
Head of Cyber Security South EMEA
Verizon Security Consulting Services

20+ years in InfoSec | Payment Security & Compliance Expert

PCI QSA, 3DS QSA, CISA, CISM

verizon business

PCI Security Standards Council

Security Consulting Services | Highlights

450+ **Consultants** speaking more than **20 languages** covering 100+ countries (#118 in EMEA).

18 **years** of the Data Breach Investigations Report

+12K Forensic **breach investigations** in 2025.

60 B **Security events** processed annually from 500k monitored devices.

~900 Network security **engagements** annually.

20K **Compliance assessments** completed since 2012.

#1 **Rating for Incident Response and Payment Security**.

Customer Outcomes

Identify and respond to threats

Provide defense and assurance services

Assist with defensive postures and compliance

Industry Eminence

Thought Leadership

C-suites conversations

Industry best practices

IDC

The Multi-Compliance Maze

Navigating Regulatory Overload

How many **distinct compliance standards** or **audit cycles** do you manage annually?

AUDIENCE POLL, SHOW OF HANDS

1	1-3	1-5	5+
			
Easy Peasy	**Tricky?**	**Meltdown imminent!**	**Send Help**

PCI Security Standards Council

Navigating the Compliance Maze

From Silos to Synergy

The Challenge: A Familiar Labyrinth

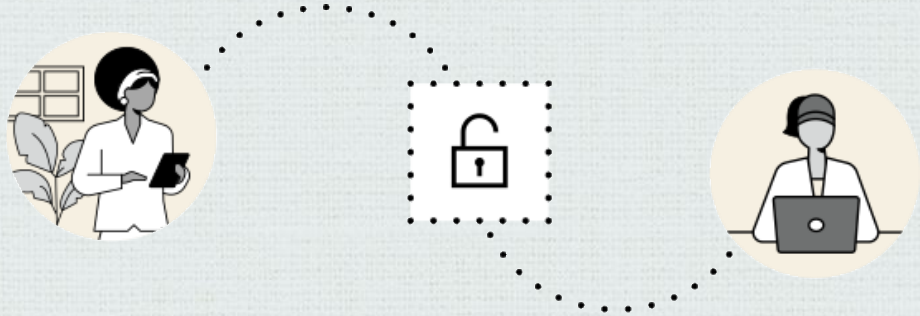
- Fragmented efforts.
- New standards or versions.
- Compliance issues.
- Audit fatigue.

The Solution: A Unified Compliance Hub

- Leveraging **PCI DSS** as your foundation.
- Building **efficiency** and **trust**.
- Improving your overall compliance posture.

PCI Security Standards Council

It’s Been a Busy Year for Cybercriminals (still)



34% Exploitation of vulnerabilities as an initial access step for a data breach grew by 34%, now accounting for 20% of breaches.

54% Only about 54% of perimeter device vulnerabilities were fully remediated, and it took a median of 32 days to do so.

60% Human involvement in security breaches remained about the same as last year—60%.

15% 15% of employees routinely accessed generative AI platforms on their corporate devices—increasing the potential risk for data leaks.

Are you vendor vulnerable?

15% → **30%**

The percentage of breaches where a third party was involved doubled in the past year, from 15% to 30%.

Developing a unified cybersecurity posture with partners can help reduce vulnerability.

Who are the culprits?

Organized crime is the leading source of cyberattacks.

60% of all breaches include the human element, through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

What are the motives?

#1 The number 1 motive was Financial gain, which was the driver for 89% of attacks.

#2 The number 2 motive was Espionage—but a very distant second place (17%)

Source: 2025 Verizon Data Breach Investigation Report

PCI Security Standards Council

The Compliance Avalanche

Navigating an ever-growing landscape of rules

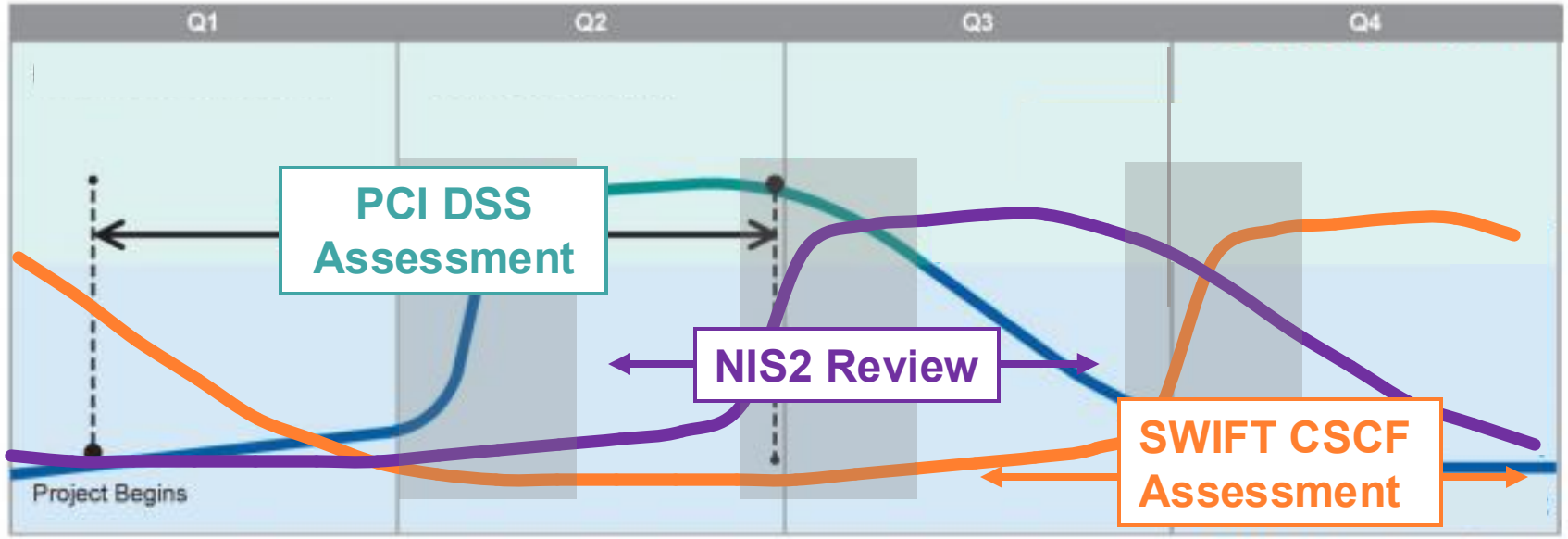
Laws and Directives

Contractual Rules

Industry Standards and Best Practices


PCI Security Standards Council®

A Familiar Pattern: The "Peak & Valley" Compliance Curve



This graph illustrates the race against compliance over time.

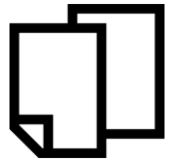
Reality Check

PCI Security Standards Council

Fragmented Compliance

The hidden costs

- **Siloed teams**
- **Lack of continuous monitoring**
- **Problems not caught early**
- **Reactive posture**



Duplicates
(Policies / procedures / tasks)

Overload &
availability challenges

Immediate Remediation
Tasks

Higher risk of
breaches / outages

PCI Security Standards Council

70%

of consumers would stop shopping with a brand that suffered a security incident.

Vercana 2024 Consumer Trust & Risk Report

Continuous Compliance as a Trust Enabler for the Business

- **Beyond checkboxes**: Compliance builds the security posture that earns customer trust and loyalty.
- **Strategic advantage**: It fosters reliable partnerships and a secure market for growth.
- **Trust is the ultimate currency**: In the digital economy, confidence fuels commerce.

“One Framework to rule them all,
One Framework to find them,
One Framework to bring them all,
and in a Compliance Hub bind them”

Credit : Peter J. Yost

One Framework to Rule Them all …

PCI DSS as the Strategic Foundation

	PCI DSS 4.0.1	NIS2 directive	TISAX 5.1	PSD2	SWIFT CSCF
Identity and Access Management	**7.x:** Restrict Access to System Components and Cardholder Data by Business Need to Know	**21.2.j:** Use of Multi-Factor authentication or continuous authentication solutions	**4.1:** Identity Management **4.2:** Access Management	**Article 97**: Authentication	**5.1:** Logical Access Control
Patch Management	**6.3.3**: All system components are protected from known vulnerabilities by installing applicable security patches/updates	**21.2.e:** Security in network and information systems (…) maintenance including vulnerability handling	**5.2.5:** An adequate patch management is defined and implemented (e.g. patch testing and installation).	No match	**2.2:** All hardware and software inside the secure zone (..) have had security updates promptly applied.
Incident Management	**12.10.x:** Suspected and confirmed security incidents that could impact the CDE are responded to immediately	**21.2.b:** Incident Handling	**1.6:** Incident Management	**Article 95**: Management of operational and security risks	**7.1:** Cyber Incident Response Planning

PCI Security Standards Council

PCI DSS: The Core of Your Unified Compliance Hub

Why PCI DSS as a baseline?

- **Prescriptive**: Not just principles, but detailed controls.
- **Universal**: Ability to cover security requirements for any sensitive data, not just CHD (PII, confidential business data ..)
- **Battle-Tested**: A long-standing framework, continuously refined against real-world threats.
- **Gold standard security**: Adhering to PCI controls improves the entire security landscape.
- **Built for verification**: Designed for annual assessment, promoting audit readiness across the board.

PCI Security Standards Council

Building Your Unified Compliance Hub

1. Define

Strategic Compliance & Standards Management
Maintaining knowledge on your scopes and the framework mapping matrix. Strategic implementation and maintenance roadmap.

Risk Intelligence
Monitoring and anticipating future regulatory changes and leveraging threat intelligence to improve controls.

2. Execute

Governance & Control Oversight
Defining control activities planned throughout the year. Establishing policies / procedures / R&R. Catching compliance topics for new projects.

Remediation & Operational Support
Managing non-compliance incidents and corrective actions. Providing guidance and support to operational teams. Continuous improvement based on findings. Automation opportunities.

3. Assess and Report

Assessment Management
Streamlining external audit processes. Consolidating evidence requests and facilitating assessor interactions.

Continuous Monitoring & Reporting
Ongoing assessment of unified security controls effectiveness through consolidated metrics. Identification and assessment of compliance risks. Reporting and dashboards to stakeholders.

PCI Security Standards Council

Building your Unified Compliance Hub

A practical approach

1. Assess

Identify all relevant standards and map our PCI baseline against other standards to identify overlaps and unique requirements.

2. Design

Develop unified security policies, procedures, and technical controls that satisfy multiple standards simultaneously. Prioritize controls that address common requirements first, maximizing efficiency.

3. Centralize

Implement a single platform for managing compliance documentation, evidence, and evidences. Standardize reporting formats to streamline audit preparation across all frameworks.

4. Operationalize

Embed compliance activities into daily security operations. Leverage existing PCI processes (vulnerability scans, pen tests) for broader, ongoing assurance across all standards.

5. Collaborate

Break down silos between compliance, security, IT, and business teams. Foster shared responsibility and provide cross-functional training to empower your people.

6. Improve

Take lessons learned from the field and improve effectiveness, performance, coverage compliance and security levels.

PCI Security Standards Council

Building your Unified Compliance Hub

Suggested Unified Control Design Templates

1. Control objective	Defines the applicable objective(s) of the control system and its contribution toward the overall goal	**7. Control testing**	Describes or references all applicable, related control test procedures and standards for the control and control system
2. Control owner	Assigns ownership of, accountability and responsibilities over the control or control systems	**8. Implementation**	Specifies implementation scope, control, procedure and dependencies—lists primary control and all dependent PCI DSS controls
3. Control function	Describes the control function, such as management, procedural or technical and functional boundaries	**9. Operation**	Documents control operation specifications and define scope, processes, operational dependencies, supporting processes and control support requirements, and component impacts on people, systems, processes and third parties
4. Control type(s)	Shows the applicable control types, such as preventative, detective, corrective or directive, or a combination thereof	**10. Maintenance**	Defines control maintenance specifications, scope and maintenance standards and processes
5. Architecture	Establishes the control architecture — such as system-specific, common or hybrid — and its contextual application	**11. Performance metrics**	Provides a list of PCI DSS key performance indicators (KPIs) and other metrics to measure control performance
6. Control risk	Details key risks that the control mitigates —such as using control-to-risk matrix or mapping	**12. Governance**	References related policies, standards, frameworks and regulations

Source: 2024 Verizon Payment Security Report

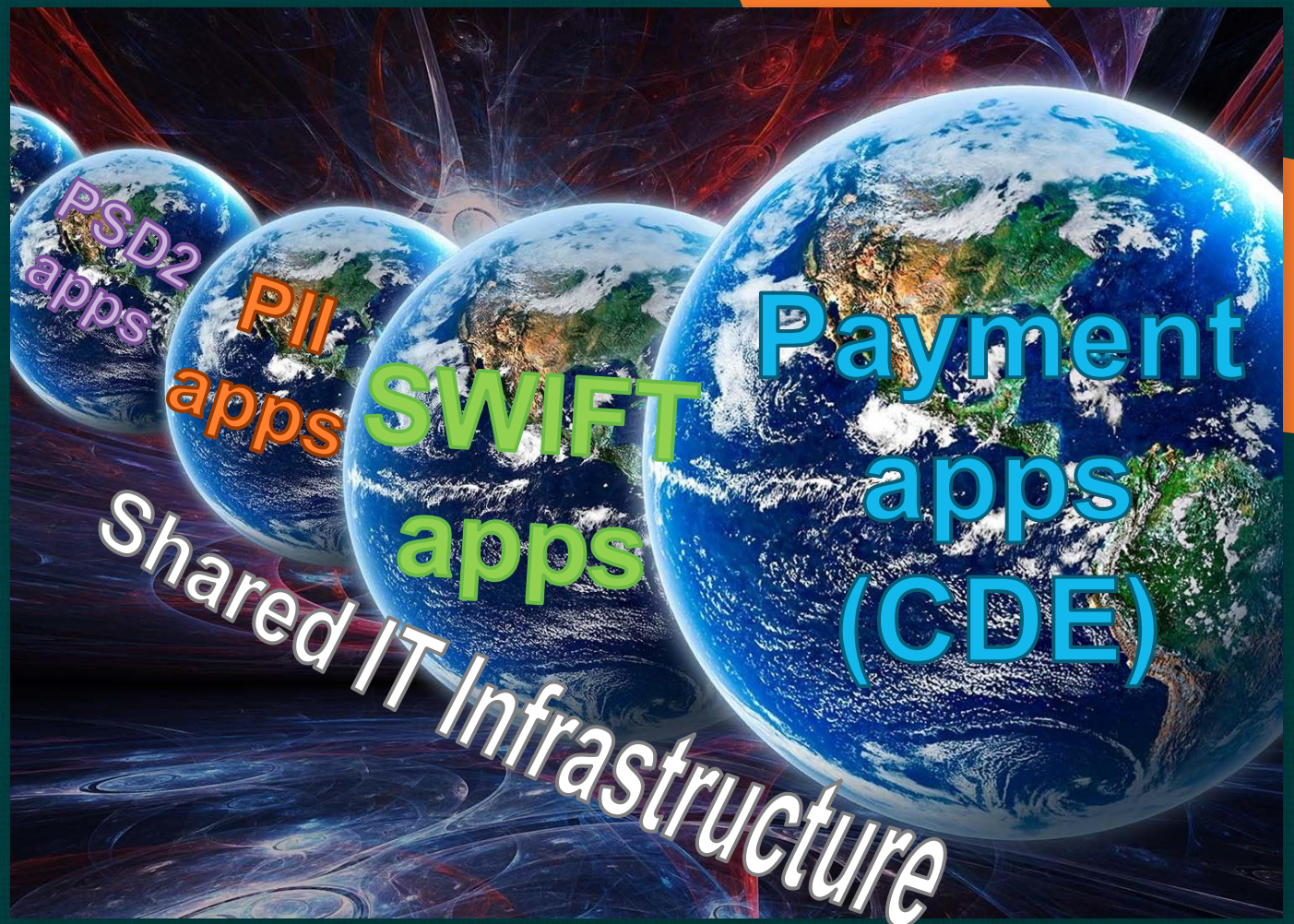
PCI Security Standards Council

The Scopes Multiverse

… because not everything lives in the CDE

A Top-Down approach:

- **Start with the service/business Function:** Define scopes & requirements from the business perspective.
- **Map to the technical layer:** Drill down to identify applicable applications, systems/network components and people.
- **Determine control applicability:** Decide which standards and controls apply to each specific scope.
- **Identify specifics:** Pinpoint unique requirements not covered by the PCI DSS baseline.



Your Unified Hub Toolkit: Start Simple

… even if you're not a Compliance Guru (Yet!)

Scope Definition Document

A clear inventory of *which* applications, system/network components, data and people are subject to *which* regulations along with the security frameworks to comply with (PCI DSS, SWIFT CSCF, NIS2…).

Recurring Control Calendar

Visualize and schedule all your compliance activities (scans, audits, reviews) on a single monthly timeline.

Control Mapping Matrix

Define your baseline framework (PCI DSS or a simplified version) then map *which* controls address *which* requirements from other standards. Identify what needs to be covered separately.

Unified Control Cards

Document *how* to control *each* requirement, *per scope*, including frequency and expected results. Start small, expand gradually.

Examples: Vuln scans, penetration tests, security patches …

PCI Security Standards Council

The Security Management Canvas

An all-in-one canvas to rule your Unified Compliance Hub

Security business model	Security Strategy	Security operating model	Frameworks and standards	Security Program
Business model • Value proposition • Stakeholders • Goals and objectives • Core process architecture • Resources • Culture • Regulations • Risk management • Governance	**Strategy** • Stakeholders • Priorities – Goals – Objectives • Scope – Focus – In-scope – Excluded • Resources – In-house – Third party • The Top 7 Strategic Management Traps	**Operations (value chains, visual representation)** • Stakeholder relationships • Organizational charts • Geographic maps – Facilities and operations • Organizational processes – Core processes – Supporting processes • Security processes • Network architecture • Functional responsibilities • Capabilities map • Constraints map	**Integration of security frameworks and standards** • PCI DSS • PCI PIN • PCI P2PE • PCI 3DS • CIS CSC • NIST CSF • SWIFT CSP **Coverage of standards and framework elements** • Partial implementation • Full implementation **Scope of implementation across the environment** • Partial implementation • Full implementation	**Program management** • Program office • Program charter **Program design** • Life-cycle management **Program scope** • Resources (4 Ls) • Constraints (7 Cs) • Sustainability (9 Fs) **Project management** • Maturity – Process – Capability • Performance – Metrics – Reporting

Source: 2024 Verizon Payment Security Report

PCI Security Standards Council

Summary of Takeaways

Beyond Compliance, Building Trust

1. **The "Avalanche" is a response, not a random act**. Regulations are driven by escalating cyber threats and the imperative to build and maintain trust in the digital economy.

2. **Fragmented compliance is unsustainable:** Siloed efforts lead to audit fatigue, wasted resources, and higher risk. The "peak and valley" delivers an illusion of security.

3. **PCI DSS is your strategic hub**: Leverage its robust, prescriptive controls as a foundational baseline to efficiently map, integrate, and manage multiple compliance standards.

4. **Shift to integrated, continuous compliance**: Move beyond checklists to a proactive, top-down approach. This drives operational efficiency, enhances your security posture, and creates sustainable, verifiable trust for your business.

verizon business

For more information
email us: paymentsecurity@verizon.com

PCI Security Standards Council

PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING