Solving PCI DSS v4.0 Challenges with Confidence

A Focused Approach to Compliance Management

Loïc Bréat, CISA, CISM, PCI QSA, 3DS QSA
EMEA Payment Security Practice Regional Lead
Verizon Business Consulting Services – Cyber Security Consulting

verizon

PCI Security Standards Council

Agenda

Solving PCI DSS v4.0 challenges with confidence

- **What's the challenge?**

  The impact of Payment Card Industry Data Security Standard (PCI DSS) v4.0 and the scope of the challenge

- **What's the solution?**

  The approach for success and the scope of the solution

- **How should you implement the solution?**

  Key considerations for formulating your PCI DSS v4.0 transition strategy

PCI Security Standards Council®

Conclusions

Key learning points

- **You need a collection of methods** for simplifying the complexity of PCI DSS, to have confidence about leadership and management, and to make both the performance and the outcomes predictable
- **Perspective on the overall compliance system** is essential – a one-page canvas with all the important elements for perspective and rich contextual context
- **Avoid program mistakes** of vision (why), strategy (what), and architecture and design (how)
- **Apply systems thinking** – address problems at the “systems level” and at the “process level”
- **Use control design templates** for the design, implementation, and evaluation of controls

PCI Security Standards Council

The Problem

What is the scope of the challenge?

PCI DSS v4.0: Three Top Areas of Concern – A Management Perspective

PCI DSS v4.0 transition simplified

Milestone/Process	
1 Understanding the requirements	Control change classification: six classes New, updated, renumbered, removed, future-dated, and mandatory defined.
2 Continuous compliance	Stricter measurement and reporting of compliance, effectiveness and performance
3 Compliance validation (evidence)	Three options: 1. Defined approach only (recommended for 2022/2023) 2. Customized approach 3. Hybrid approach

PCI Security Standards Council

What Determines the Level of Effort?

Understanding the challenge with compliance

- The level of effort needed to secure an environment is ultimately determined by three major factors:

  (1) **complexity**, (2) **proficiency**, and (3) **focus.**

  - The level of complexity of the control environment
  - The level of proficiency to design, implement, maintain and evaluate (DIME) a control environment
  - The ability to focus (optimization of attention)

PCI Security Standards Council®

Global State of PCI DSS Compliance: Long-term Trends

Findings from the Verizon 2020 Payment Security Report

The long-term (5-year) trends in full compliance with PCI DSS by Key Requirement:

Cream of the crop:	**Best performing**
Requirement 7	- Restrict access
Requirement 4	- Protect data in transit
Requirement 5	- Protect against malicious software, and
Requirement 9	- Control physical access.

80%+ Over 80% of organizations keep these key requirements in place.

.

PCI Security Standards Council ®

Global State of PCI DSS Compliance: Long-term Trends

Findings from the Verizon 2020 Payment Security Report

So-so: Mediocre performance

Requirement 3	- Protect stored cardholder data
Requirement 8	- Authenticate access
Requirement 1	- Install and maintain a firewall configuration, and
Requirement 2	- Do not use vendor-supplied defaults

70%+ More than 70% of organizations maintain these requirements.

PCI Security Standards Council

Global State of PCI DSS Compliance: Long-term Trends

Findings from the Verizon 2020 Payment Security Report

Bad apples: **Worst performing**

Requirement 11	- Regularly test security systems and processes,
Requirement 6	- Develop and maintain secure systems, and
Requirement 12	- Security management

<70% Fewer than 70% of organizations maintain these requirements.

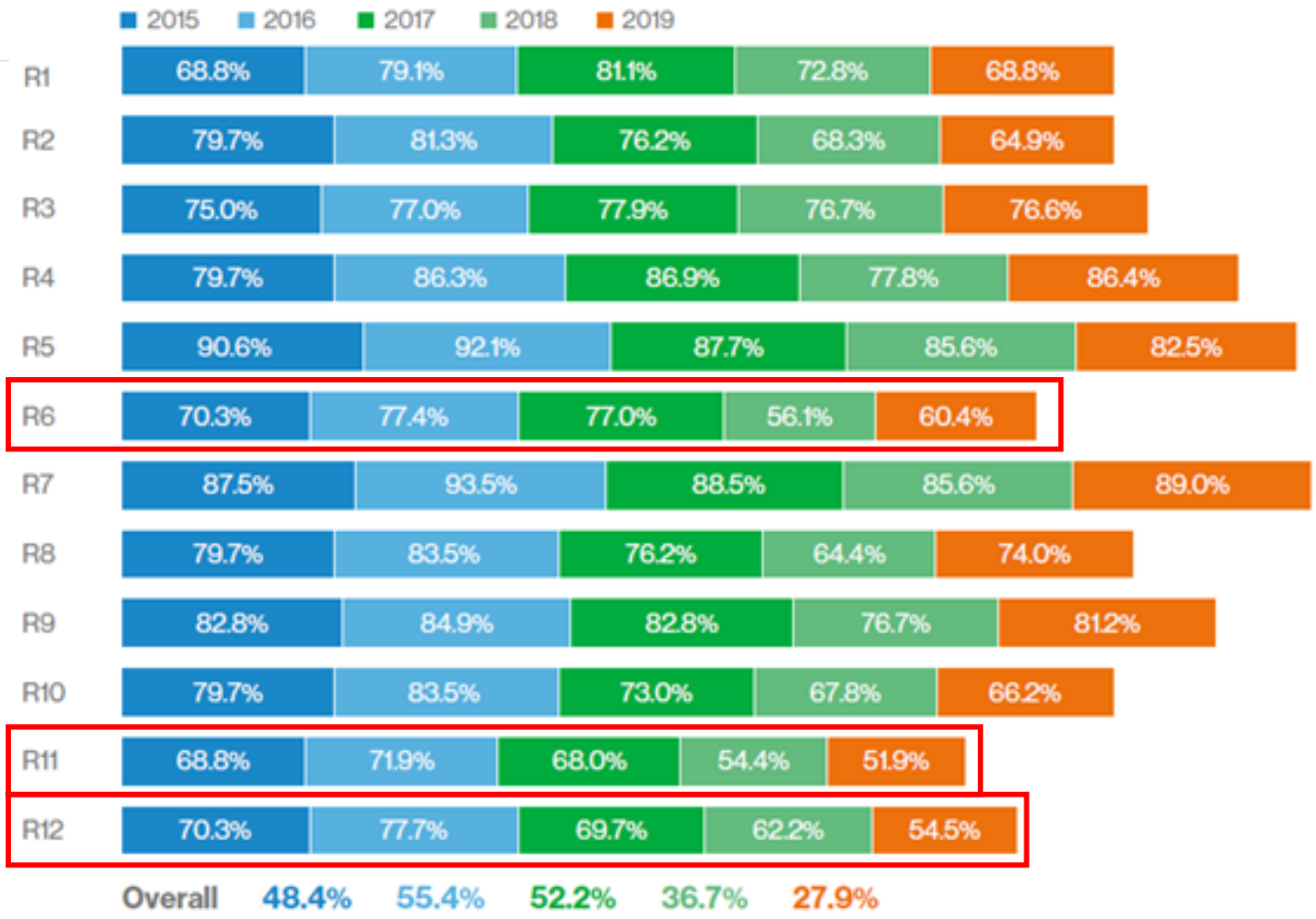
Note: Requirement 11 remains the worst-performing requirement for sustainable compliance for more than 10 years running - but did improve significantly.

PCI Security Standards Council

Five-year Trends in PCI DSS Compliance

Full Compliance (sustainability):

- Poor performance on compliance assessments isn't a spontaneous act; rather, it's the outcome of a sequence of activities and events based on strategic planning—or lack thereof
- Unless the security and compliance strategy, business models and operating models are improved, it's mostly symptoms that are addressed
- A control environment's system output depends on past and current inputs. It's a causal system.
- Data security is a process that requires long-term attention to strategic initiatives



PCI Security Standards Council

Reasons for Lack of Sustainable Control Effectiveness

The ability to rapidly detect and correct controls that fall out of place

- **To achieve it, you need to aim for it!**

  Include sustainable control effectiveness as an expressed objective and articulated PCI DSS goal statement.

- **Three stages of PCI Security program failure:**

  1. Vision (Why) → 2. Strategy (What) → 3. Architecture and design (How)

- **Can organizations achieve sustainable control effectiveness?** Yes!

  Almost half of organizations demonstrate this capability. The solution exists.

PCI Security Standards Council®

The Three Stages of Compliance Management Failure

Mistakes that occur during planning and execution of PCI Security compliance programs

Stage 1: Failure of vision – these are “why” mistakes.

Failure to understand, define and communicate the purpose - why you are engaged in PCI security compliance and the overall goals and outcomes.

Stage 2: Failure of strategy – these are “what” mistakes.

Failure to design and execute a strategy in a manner that delivers the desired results.

Choosing the wrong “what” to make the strategy happen (i.e., wrong priorities and objectives).

Stage 3: Failure of architecture and design – these are “how” mistakes.

Taking the wrong execution and implementation approach. Inadequate methods.

Using inappropriate strategy development, management methods, and framework implementation.

PCI Security Standards Council®

The Six Phases of a Project

"Six Phases of a Big Project," Wikipedia, https://en.wikipedia.org/wiki/Six_phases_of_a_big_project

1. Enthusiasm,
2. Disillusionment,
3. Panic,
4. Search for the guilty,
5. Punishment of the innocent, and
6. Praise and honor for the nonparticipants

PCI Security Standards Council

The Solution

What is the scope of the solution?

Requirements for Effective Security and Compliance Management

Avoid all 7 strategic data security management traps

1. Inadequate leadership and strategy
2. Failure to secure strategic support
3. Lack of resourcing capabilities
4. Falling short on strategic design
5. Deficient strategy execution
6. Low capability and process maturity with lack of continuous improvement
7. Communication and culture constraint

PCI Security Standards Council

The Goal of PCI Data Security

"The organization goal of a PCI Data Security compliance program is to develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing protection of payment card data in a consistent, predictable and sustainable manner.

To achieve this goal, the PCI security compliance program is integrated with and supported by additional security, risk management, and governance frameworks, a security operating model, a strategy and a security business model."

—Verizon Payment Security Report

PCI Security Standards Council

Goals vs. Objectives

All stakeholders must agree up front on the goals, objectives and success criteria

Goals:

- An overarching idea expressed clearly, concisely, and descriptively of the end result,
- aligned with your organization's vision, mission, and ideals,
- with long-term and time-sensitive indicators of what should be accomplished.

Goals are a measure of progress. Goals support the strategy.

Objectives:

- More specific, clear, and actionable statements of smaller, specific targets within the general goal,
- that articulate how the goal is attained, with specific actions and steps to take, time-bound and shorter deadlines,
- and with measurable performance factors, clearly stated costs and quantities.

PCI Security Standards Council®

The Constraints of Organizational Proficiency - “the 7 C’s”

A categorization of common limitations that restricts or prevents performance improvement

1. Capacity

Limitations on the amount of resources that can be allocated to security and compliance

2. Competence

The level of experience and skill at an individual level to support security and compliance

3. Capability

The level of proficiency at team and organization levels – what people can achieve collectively

4. Commitment

The pledge from stakeholders to undertake the actions needed to achieve the security goals

5. Communication

The frequency and quality with which stakeholders exchange information

6. Culture

The sum of an organization’s attitudes, actions and behaviors toward security and compliance

7. Cost

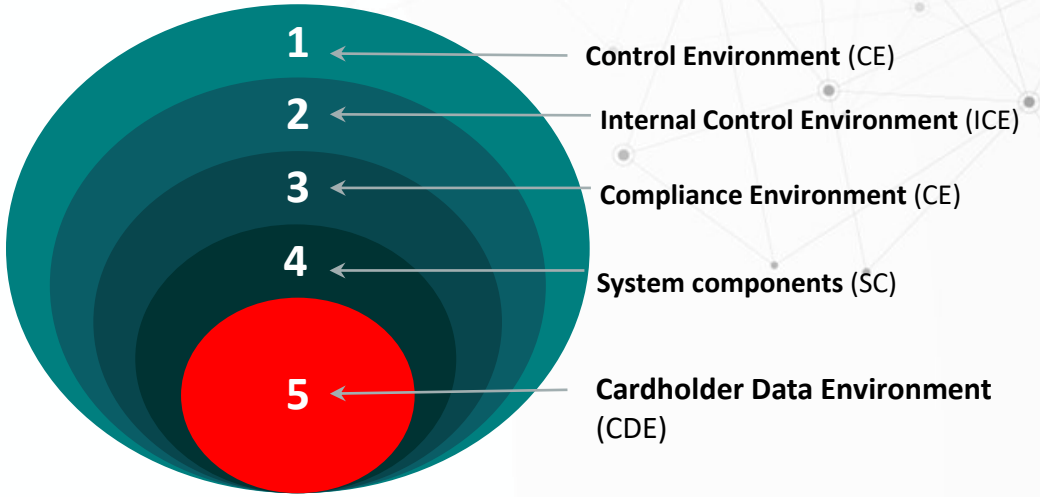
The amount of time and money allocated and required to achieve objectives and goals

PCI Security Standards Council

Requirements for Effective Security and Compliance Management

Control environment – understanding the complete scope

- A control environment is a **continuous managerial process** with structures and standards that provide the basis for carrying out internal control across the organization. It should be clearly defined, documented, communicated, evaluated, and maintained.



- **It is comprehensive** – includes all the actions taken by management to manage the environment; strategic governance and operational day-to-day management of activities; all participants, all policies, standards and procedures, tools, processes, and documents.
- Within an **effective control environment**, competent people understand their responsibilities and the limits of their authority. They are knowledgeable, mindful, and committed to doing what is right and doing it the right way.
  - An effective control system rapidly detects and discloses where failures are occurring and what/who is responsible for the failures. It ensures that corrective action is taken, and performance is measured, reported, and continuously improved.

PCI Security Standards Council

The Security Management Canvas

Security business model and security strategy

1 **Security business model:** ties all the elements together, obtaining business support for the security strategy

2 **Security strategy:** careful selection of data security compliance objectives, methods of execution and allocation of resources

Security operating model and security framework

3 **Operating model:** aligns the resources and core processes with the security business model and strategy

The model can help diagnose performance problems and identify solutions

4 **Framework:** a conceptual structure intended to serve as a support guide for the data security and compliance management system

Security programs and projects

5 **Security program:** a structured organizational process for the ongoing direction and application of internal and external resources (people, time, budget, processes and technology)

Its purpose is to meet defined objectives by integrating the management of related projects in a coordinated manner to obtain benefits and control that is not available when managing them individually

PCI Security Standards Council®

(See 2020 PSR page 16 for an explanation)

Visibility and Perspective on the Overall Approach: The Security Management Canvas

Security business model

1. Value proposition
2. Stakeholders
3. Goals and objectives
4. Core process architecture
5. Resources
6. Culture
7. Regulations
8. Risk management
9. Governance

Security strategy

1. Stakeholders
2. Priorities
   a. Goals
   b. Objectives
3. Focus
   - Exclusion of activities
4. Application of resources
   a. In-house
   b. Third-party
5. The Top 7 Strategic Management Traps

Security operating model

Visual presentation of the operations (value chains)

a. Stakeholders and relationships

b. Organizational chart

c. Geographical map

d. Org processes map (Core / Supporting)

e. Security processes map

f. Network architecture

g. Functional responsibilities

h. Capability map

i. Constraints map

Security frameworks

1. Integration of security frameworks & standards

a. PCI DSS

b. IS0 27000

c. NIST CSF

d. CoBiT

2. Coverage / Scope of implementation –

a. Partial vs full implementation of frameworks

b. Coverage of framework elements

Security Program

1. Program management

a. Charter

b. PM Office

2. Program scope

a. 9 Fs

b. 7 Cs

c. 4 Ls

3. Project management

a. Maturity models
   - Process
   - Capability

b. Performance
   - Metrics
   - Reporting

PCI Security Standards Council®

An Effective Management approach

A logical approach with solving complex challenges

1. **Purpose** before planning (start with “why”, then formulate goals)

2. Clarity on **objectives** (intermediate steps to achieve the goals)

3. **Requirements** for achieving objectives (necessary and sufficient conditions)

4. **Constraints** analysis of requirements (focus on removing the most significant limiting factor)

And now that you actually know what you are dealing with (scope and impact):

5. **Strategy** development & communication (focused allocation of resources)

6. **Program** design and implementation (program- and project-level execution of the strategy)

7. Continuous re-evaluation and **improvement** (performance management)

PCI Security Standards Council

Suggested Control Design Templates

Twelve essential components to include in every control design document

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

PCI Security Standards Council ®

Summary of Takeaways

Key learning points

1. **Most security and compliance programs can do a lot better. Where should you focus your efforts?**
   Use The Security Management Canvas (TSMC) to know which important elements are deficient or missing within your control environment and how to structure all of your activities.
2. **Begin by establishing clear goals.** Know which objectives to prioritize, and their conditions for success.
3. **Follow a logical process.** Use effective methods to identify and eliminate core conflicts and constraints.

verizon

Visit the Verizon booth for more information.

email us: paymentsecurity@verizon.com

PCI Security Standards Council