White paper

PSR

2023 Payment Security Report insights

Advanced PCI security program management design

Verizon Cyber Security Consulting

verizon✓

About the cover

The 5x5 cube on the cover depicts the complexity of security program management. Designing a security program can be like trying to solve a mechanical three-dimensional (3D) combination puzzle. Each move affects the rest of the design and overall system. While some people struggle to solve the puzzle's quintillions of options, others solve it within a few seconds. The difference has to do with their methodology.

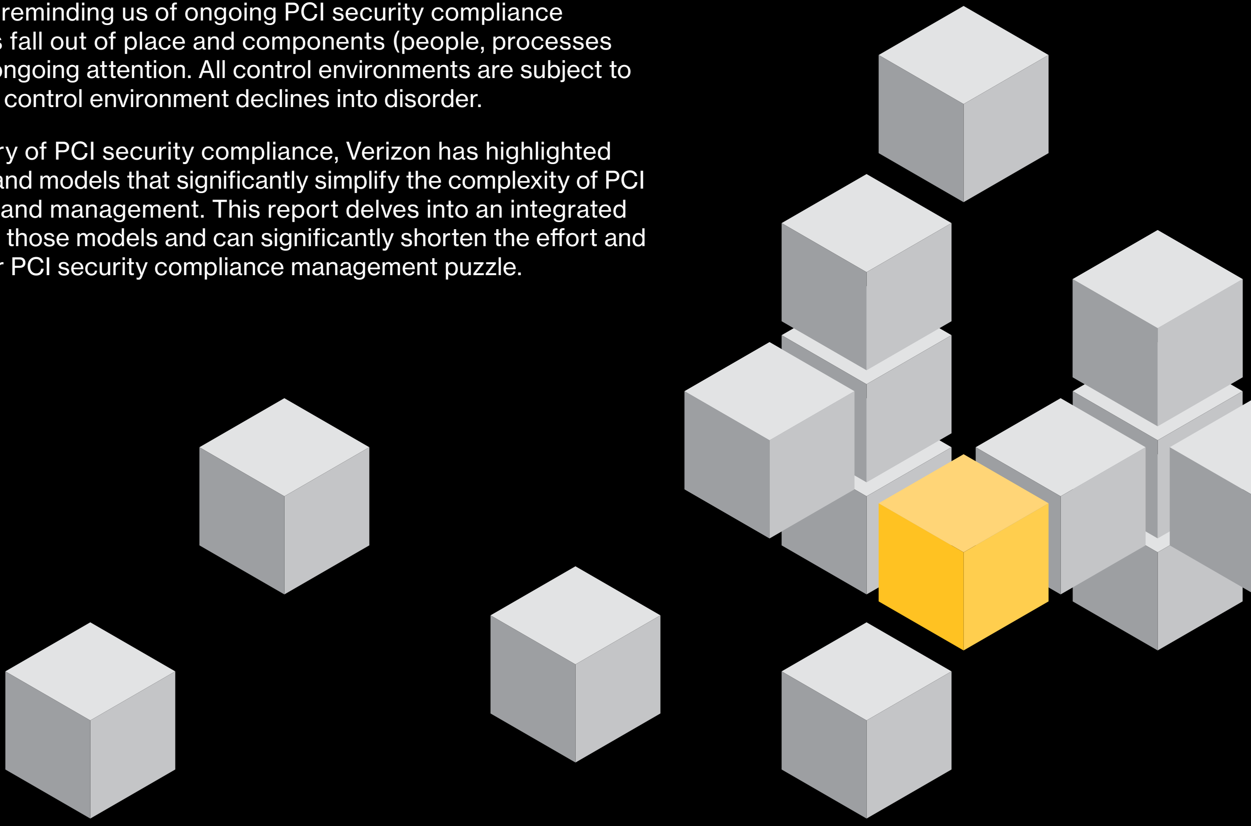
Instead of a trial-and-error approach, combination puzzles are most easily solved by using a method. You can expend lots of time spinning the puzzle's cubes until you line up some semblance of a solution that meets your needs. Or you can use a reliable, logical method to cut time, effort and cost and quickly solve the problem with the best possible results.

Similarly, Payment Card Industry (PCI) security programs require the alignment of multiple elements. This complexity can be vastly reduced with a sound program design—the application of a method to apply the correct sequence of steps—and by understanding the cause-and-effect relationships between moves.

The cube on the cover highlights specific rows and columns (in yellow), representing the need to focus: resolving specific components within the perspective of the larger system. The entire system can be brought into alignment step by step, using a methodical and systemic approach to sequentially align individual layers rather than with random moves and attempts to solve the entire puzzle all at once.

After the 3D combination puzzle is fully solved, it's shuffled, and the entire process is started all over again—reminding us of ongoing PCI security compliance programs where controls fall out of place and components (people, processes and technology) require ongoing attention. All control environments are subject to entropy, where a security control environment declines into disorder.

During the 20-year history of PCI security compliance, Verizon has highlighted several leading methods and models that significantly simplify the complexity of PCI security program design and management. This report delves into an integrated method that incorporates those models and can significantly shorten the effort and time needed to solve your PCI security compliance management puzzle.



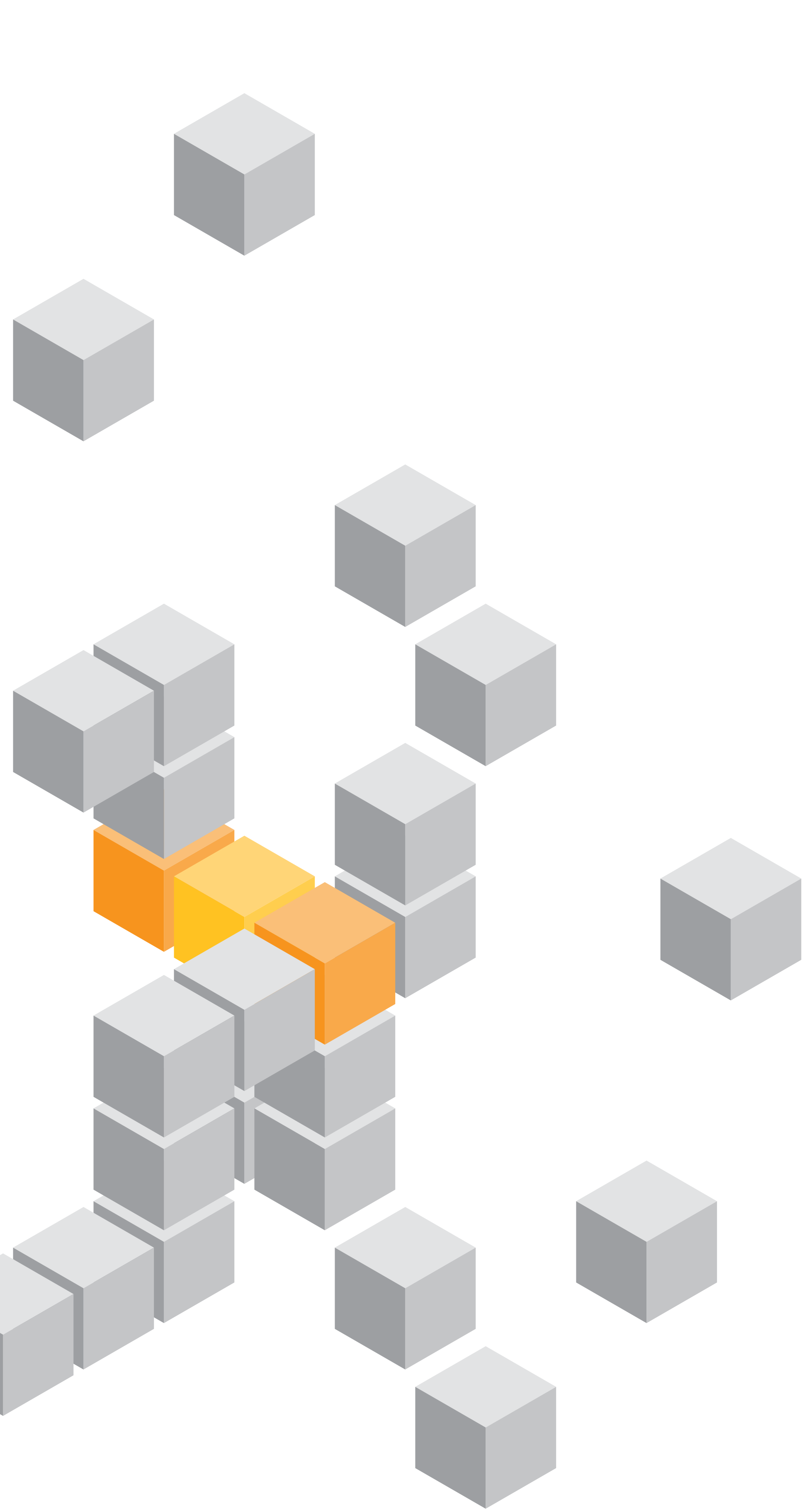


Table of contents

Advanced PCI security program management design

Management models

Integrated program design

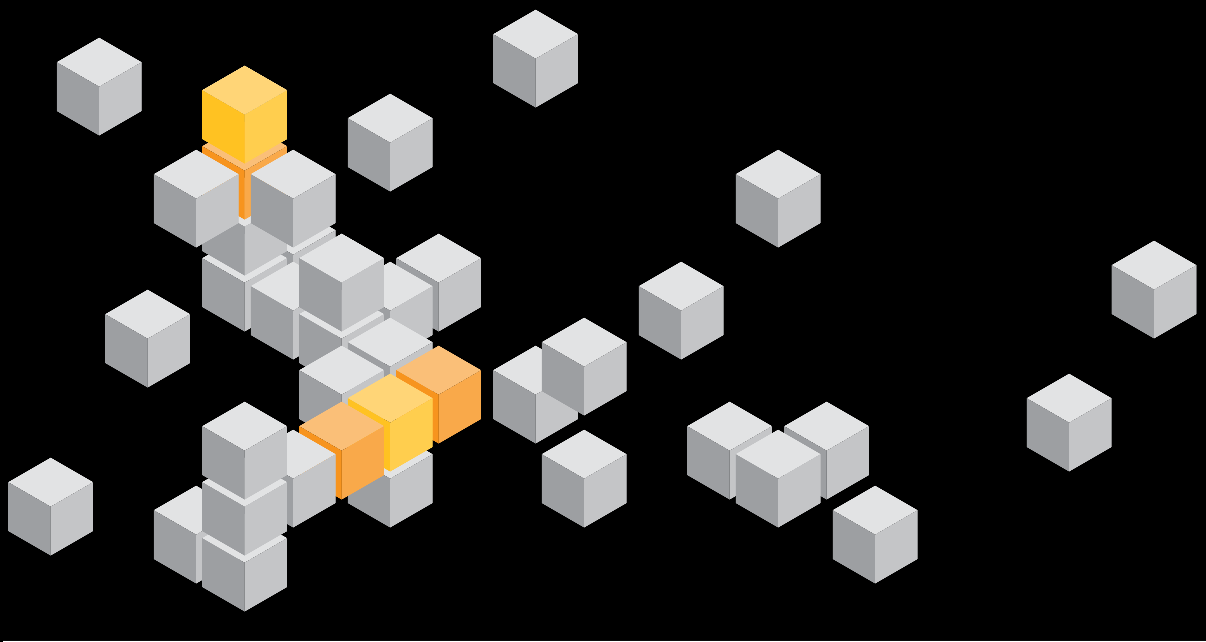
Advanced PCI security program management design

Introduction

This paper provides an overview of what we have learned from 20 years of Payment Security Report (PSR) research on critical success factors and design approaches for Payment Card Industry (PCI) security programs. It presents an integrated set of time-tested models, methods, techniques and concepts highlighted in the PSR that continue to add substantial value to organizations.

Organizations need a method that offers clear visibility and perspective to establish and retain control over their payment card security programs and deliverables. They need approaches with methods that focus on moving from treating symptoms to addressing the causes of poor security program performance—making program input, performance and output highly predictable. Several compliance management program designs were tried and tested during the past decade. Verizon evaluated, designed and published a series of models, methods and techniques to help organizations successfully navigate the complexity of PCI security compliance management challenges.

This paper presents an integrated approach, using some of the best methods and models available, for organizations of all sizes and across industries to help simplify and improve the design and operation of virtually every aspect of their PCI security program.



For more than 20 years, Verizon has been exploring and refining security models and advancing security program designs to help organizations achieve predictable performance and overall program success by design. The methods and concepts highlighted in this paper can help organizations more easily design programs and projects, focus on what matters, simplify security compliance operating environments, and overcome the most important constraints by:

- Formulating and communicating an overall clear goal for a program and for each of the key requirements
- Devising an economical approach with rational choices on the allocation of scarce resources
- Creating critical program design and management elements that can be incorporated into PCI security programs
- Formulating clear program objectives and establishing the frame needed to design a security strategy
- Reducing and actively controlling the scope of the PCI security compliance environment
- Integrating requirements from various security standards into a single set, such as applicable PCI security standards (the Data Security Standard [DSS], PIN Transaction Security, Point-to-Point Encryption [P2PE], 3-D Secure [3DS], Secure Software) as well as other regulations (Society for Worldwide Interbank Financial Telecommunications [SWIFT] Customer Security Control Framework [CSCF])
- Thinking through a logical process for clarifying root causes of poor program performance and program management
- Promoting a process to help teams get the right work done and be confident about what to focus on and what to ignore
- Developing a method for identifying and overcoming the most significant constraints
- Understanding the necessity for formal program management practices, critical chains and maturity models to guide and assess such an implementation

These essential tools and models can help you refine an existing program or design new programs based on lessons learned from thousands of organizations that successfully craft PCI security compliance management.

Welcome to Verizon's unique approach to reducing PCI security complexity.

This paper outlines methods, techniques and models designed to reduce payment security complexity.

The value of mental models

A mental model is a representation of how something works—a concept or process. A model is used to better understand that process by cutting away as much as possible to focus on key aspects.

Benefits of models for improving PCI security programs

It's difficult to keep all of the details of a system or environment in our brains. That's why models are used to simplify the complex into understandable and organizable chunks. The right structure for operational processes, management and controls presents substantial advantages to help a PCI security program run smoothly and efficiently. Within security and compliance programs, mental models are very useful to help determine context for presenting information to security program participants.

Models help us consider why some elements are more relevant than others. They help us reason, see through the process, structure it, summarize and concentrate on what's important. Models shape people's views of the security control environment, how individuals understand the control environment, and the function and relationships between its components. They also shape the views individuals and teams have about their own capabilities, the tasks they perform and their learning curve. All of this depends heavily on the conceptualizations.

For further reading, see "Mental Models: The Best Way to Make Intelligent Decisions (~100 Models Explained)" at https://fs.blog/mental-models.

Mental models simplify complexity.

Models present design, operations and management structures that are important to businesses of all sizes because they provide a way to organize and direct employees, delegate tasks, and make decisions about security compliance programs. They support how organizations can best structure activities to coordinate and manage individuals and teams to achieve organizational goals and objectives. Models help delineate formal communication channels and describe how separate individual actions are linked together.

Mental models are likely to be inaccurate to some extent insofar as they are heuristics, and they cannot encapsulate all aspects of a system.

> **"Essentially, all models are wrong, but some are useful."[1]**
>
> **—George E. P. Box**

> **"Information security practitioners desperately crave new models, further highlighting the cognitive crisis. In fact, we often take good models and overuse them or extend them beyond their practical purpose. ... The problem is that we're model hungry, and we'll rapidly use and abuse any reasonable model that presents itself. Ultimately, we want good models because we want a robust toolbox. But not everything is a job for a hammer, and we don't need fourteen circular saws."[2]**
>
> **—Chris Sanders**

> **"The quality of our thinking is proportional to the models in our head and their usefulness in the situation at hand. The more models you have—the bigger your toolbox—the more likely you are to have the right models to see reality."[3]**

[1] George E. P. Box, "Science and statistics," Journal of the American Statistical Association, Taylor & Francis, Ltd. on behalf of the American Statistical Association, 1976.

[2] Chris Sanders, "Information Security Mental Models," May 29, 2019, https://chrissanders.org/2019/05/infosec-mental-models

[3] "Mental Models: The Best Way to Make Intelligent Decisions (~100 Models Explained)," Farnam Street, accessed July 28, 2023, https://fs.blog/mental-models

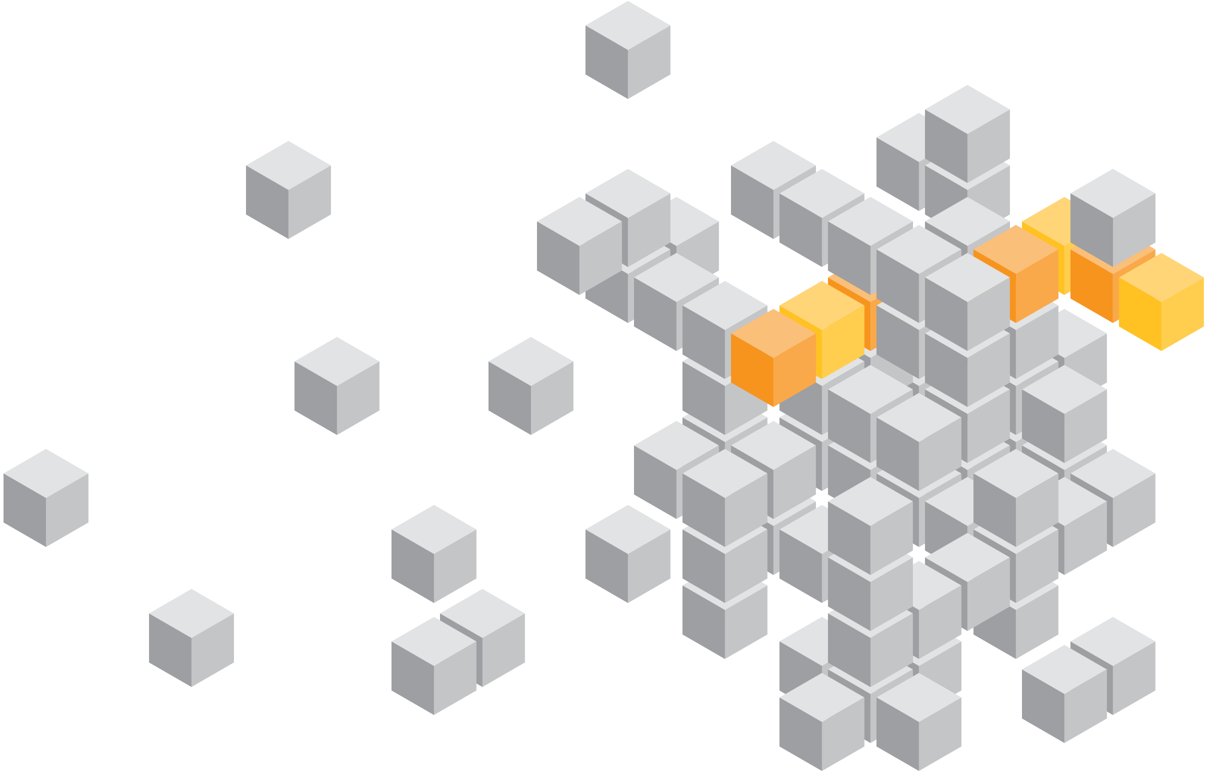
The goal of a PCI security program

Clear specification of the goal of a PCI security program is one of the most important first steps in program design. Communicating why the program exists and what you are aiming to accomplish is a critical success factor for all PCI security endeavors. Specification of the goal is the standard against which you evaluate reality to determine whether the program is succeeding. Yet, despite its importance, surprisingly few organizations include a clearly articulated goal statement in their program documentation. You cannot achieve adequate leadership and strategy without defining the purpose of PCI security compliance.

Passing a compliance validation assessment is hardly sufficient as the specification of the end goal of a PCI security program. The intermediate objectives toward the goal should include the effective and sustainable protection of data. There should be continual improvement toward higher levels of process and capability maturity, with controllable processes, predictable outcomes and measurable performance across the control environment.[4]

The overall organizational goal of a PCI security compliance program is to develop, maintain and continually 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.



[4] See page 17 for an explanation of "control environment."

The overall goal of PCI DSS

Five important components are included in this goal statement:

1. **Develop, maintain and continuously improve**
2. **a mature control environment that**
3. **offers reasonable assurance for**
4. **the effective, ongoing protection of payment card data**
5. **in a consistent, predictable and sustainable manner**

The overall program goal is what your team should and may be aiming for, and it should influence every decision, task and activity within your compliance strategy and program. Therefore, the overall purpose of compliance with the PCI DSS and the intended overall desired outcome should be carefully defined.

Start the design of a PCI security program by identifying the overall goal of your system. Then, develop your strategy around the achievement of the goal with prioritized, intermediate objectives to accomplish the requirements—the critical success factors of the goal. Tactics will follow from this. Organizations that develop tactics first and implement them locally (suboptimization) tend to stall within a few iterations. Usually, the rest of the organization doesn't sufficiently understand the direction of the security and compliance team. You need a systemic/global optimum approach to your strategy and tactics.

For further reading, see the Verizon 2022 PSR,[5] pages 8, 18 and 25 through 31; page 86 on PCI DSS Key Requirements goal statements; and "Appendix A: Primer for crafting security and compliance goals" on page 146.

Defining PCI security program success

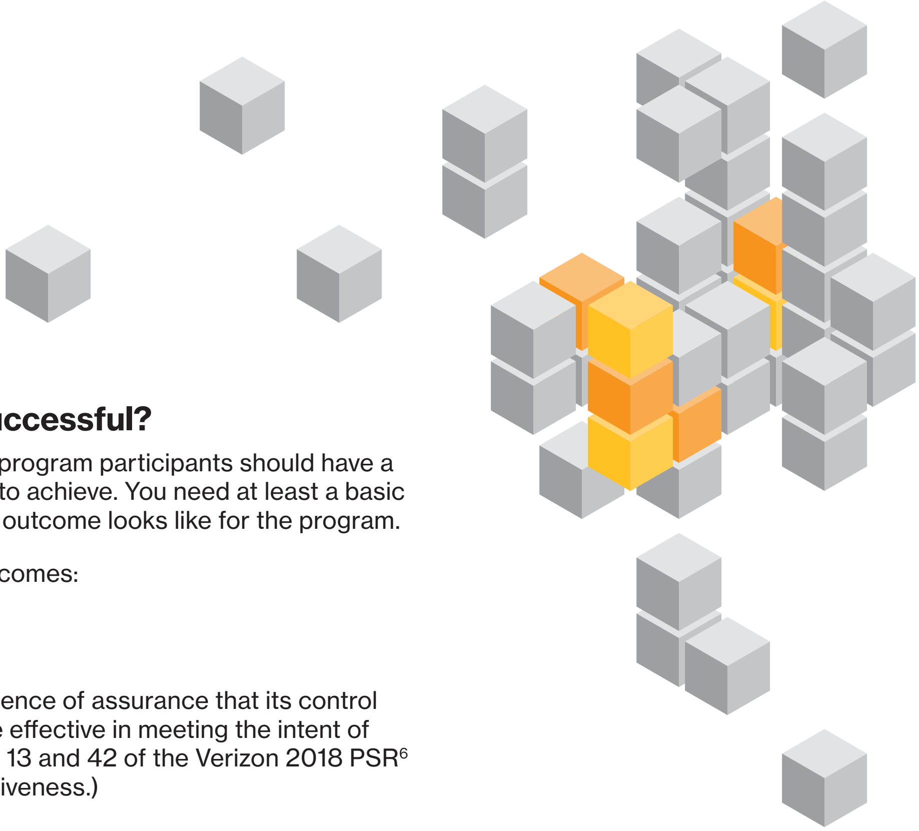
Many organizations continue to measure the success of their PCI DSS programs by the outcome of their compliance validation assessments. That usually only measures the compliance validation side of the endeavor. You can measure the success of a compliance program in various ways. For example, from a project and program management perspective, you can measure the performance of the program in traditional project management metrics, such as time-based key performance indicators (KPIs) (cycle time, one-time completion, number of changes, hours planned vs hours spent), budget-based KPIs (budget vs actual expense), and milestones and phases covered to date. The performance of the project in terms of the efficiency, effectiveness and efficacy of the resources does not tell you much about the extent of the risk and how well payment card account data is protected by the organization. It relates to the progress made toward mitigating the risk of and liabilities associated with noncompliance with the PCI security compliance regulation.

The level of effort of any PCI security program is ultimately determined by three major factors:

- **Complexity:** The level of complexity of the control environment
- **Proficiency:** The level of proficiency (the skill and experience/competence and capability) to design, implement, maintain and evaluate a security control environment
- **Focus:** Optimization of attention with a focused goal, including a business model for investment, a strategy to direct resources with precision, operations, application of supporting frameworks, and focused design and execution of the program

Even when a team is very proficient, it cannot perform well when it's distracted and lacks focus.

[5] "2022 Payment Security Report," Verizon, 2022, https://www.verizon.com/business/resources/reports/2022-payment-security-report.pdf



When is a PCI security program successful?

Begin with the end in mind. Define the goal. All program participants should have a clear understanding of what the program aims to achieve. You need at least a basic definition and consensus on what a successful outcome looks like for the program.

Success is recognized by the following five outcomes:

1. **An effective program**

   Get the right work done with evidence of assurance that its control environment and key controls are effective in meeting the intent of all control objectives. (See pages 13 and 42 of the Verizon 2018 PSR[6] on how to measure control effectiveness.)

2. **Efficiently executed**

   Produce economical program results, executed in a better manner with minimum waste of resources.

3. **Strategically aligned**

   Program design and execution are neither tactical nor reactive and are strategically aligned to support the overall business strategy. (See pages 29 and 30 of the 2022 PSR for how to measure strategy.)

4. **Sustainable performance**

   Compliance management is a marathon, not a sprint. It requires sustainable life cycle management of the controls and the environment.

5. **Ongoing maturity improvement**

   Program processes must continually progress toward higher process capability maturity. (See pages 25 through 29 of the Verizon 2019 PSR[7] for measurement and maturity models.)

Each of these outcomes can be achieved by design. To achieve these five critical success criteria, you need to know the basic scope of each and how to design, execute and measure them.

[6] "2018 Payment Security Report," Verizon 2018, https://www.verizon.com/business/resources/reports/payment-security/2018/

[7] "2019 Payment Security Report," Verizon 2019, https://www.verizon.com/business/resources/reports/payment-security/

Management models

The Security Management Canvas

The design and management of a successful, strategic PCI security program requires an integrated perspective. This means end-to-end visibility of the primary building blocks and critical inputs and outputs of the program. This is also a critical success factor for the program to be effective and sustainable. PCI security management programs are not temporary endeavors. Compliance with PCI security regulation is a long-term business concern that requires strategic planning to develop the capability to sustain ongoing compliance operations for many years. Organizations that attempt to design and operate security compliance programs without the deliberate, structured integration of the security business model, security strategy, security operating model, and security frameworks and standards face an uphill battle treating the consequences. They step straight into program design and management pitfalls that should be avoided. Poorly designed programs continually demand treating symptoms because they were not created on a solid foundation sufficiently aligned with the business mission, vision and operations of the rest of the organization. The Security Management Canvas (TSMC) addresses several root causes for poor program performance.

An exceptionally powerful framework that unlocks the potential for doing the right work in the right order

This management model is based on 20 years of experience with PCI security program performance management and was developed and published by Verizon in the 2020[8] and 2022 PSRs. (See pages 15 through 17, "Elements of a high-performance data security environment," in the 2020 PSR.) TSMC is an exceptionally powerful framework that places any PCI security program into the correct perspective and ordered sequence. Its five pillars present an integrated set of documents that all organizations should develop, maintain and apply.

Note that the security program is on pillar five—for very good reason. It highlights the dependencies on the output of the preceding pillars. It provides a rich, contextual perspective on what the team needs to know about the scope as well as the necessary inputs and outputs for successfully managing an efficiently effective PCI security compliance management program. This structure unlocks the potential for doing the right work in the right order and doing it well. Every decision and action taken for your security compliance program fits into this canvas. Every organization needs to invest in these pillars of activity for a solid foundation.

For further reading, The Security Management Canvas is explained in greater detail in the 2022 PSR, pages 32 through 41.

A single view

The Security Management Canvas provides a single view of the entire security and compliance management process. It presents the foundational blocks of an effective management system. The design and implementation of a program based on TSMC structure can produce highly valuable, essential documents and produce the exact input needed to make important decisions throughout the program life cycle.

You may save yourself a lot of time and effort if you use TSMC to evaluate the progress of your program against the components and their relationships on this canvas, find what you missed, calculate the consequences of missing or neglecting steps, and make the correction.

[8] "2020 Payment Security Report," Verizon, 2020, https://www.verizon.com/business/resources/reports/2020-payment-security-report.pdf

The Security Management Canvas

Pillars	Security business model	Security strategy	Security operating model	Frameworks and standards	Security program
Documents	**Business model** Value proposition Stakeholders Goals and objectives Core processes 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
Descriptions	An overarching model that ties all the elements together. It facilitates obtaining support for investment in security and compliance. The business model defines objectives and the structure of core processes to deliver maximum value to stakeholders. It supports the alignment between the strategy operations, security frameworks and security program.	Defines the approach and determines the careful selection and prioritization of security compliance objectives – guiding the allocation of resources. The strategy defines the what and the why but not the how-to. To be successful, the security strategy must be aligned with the security business model.	A collection of documents that presents the functional components within your security and compliance operations. It aligns resources and core processes and visually presents how value is created for the organization from the security and compliance operations. It's great for diagnosing performance issues, such as understanding how your control environment functions and where improvements are needed. You have a current operating model but also need a target operating model to define how your operations should improve.	Act as support guides for your security and compliance management system. They drive the structure of your program and projects. Their success is determined by how well you implement them.	Delivers outcomes by designing and managing a collection of projects to achieve long-term objectives. The program success depends on its interaction with and support from the preceding four pillars – the business model, strategy, operating model and frameworks.

Figure 1

The GRC^2 Model

Goals
Requirements
Constraints

X

Governance
Risk management
Compliance

Many organizations isolate their PCI security compliance programs from broader governance programs, not realizing the effectiveness and efficiency of a synchronized approach, which avoids overlap and repetition of tasks between various programs. A unified compliance approach to meet various regulatory requirements under a single corporate governance umbrella has significant compliance and risk management benefits. Organizations should, at least annually, revisit the goals, requirements and constraints of their governance program.

Is your PCI security program fully integrated with your larger corporate governance, risk management and compliance initiatives?

GRC is an umbrella term for a management discipline and operational framework. To ensure the realization of organizational goals and objectives, GRC—which stands for governance, risk management and compliance—requires an integrated, organizationwide approach to establish clearly defined, measurable standards of performance. In other words, the main purpose of GRC as a business practice is to develop and maintain a well-coordinated and integrated collection of capabilities to support predictable and reliable performance at every level of the organization. It’s a structured approach to align IT with business objectives while effectively managing risk and meeting compliance requirements. Organizations should develop this essential capability to achieve goals and strategic objectives and meet stakeholder needs.

The scope of GRC does not end with just governance, risk management and compliance. It includes assurance and performance management. When done right, a GRC approach offers better decision-making agility and confidence; reduction in costs, duplication and affected operations; sustained, reliable performance; and delivery of value.

The value of integrating a PCI security program with GRC

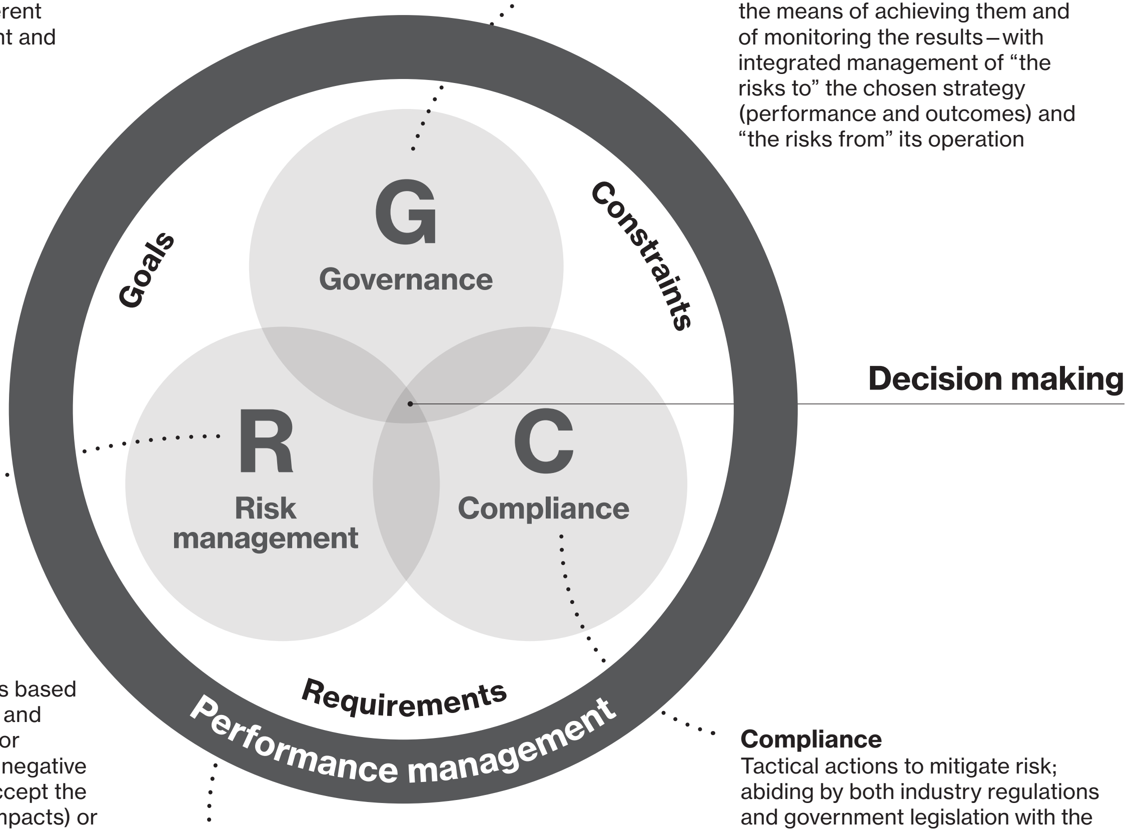
Verizon developed and published the GRC^2 Model in the 2022 PSR, page 21. The synchronized integration of all GRC activities translates into increased efficiency and bottom-line financial benefits for businesses.

The interactions of the GRC^2 Model

The three practices that make up GRC share common and interrelated tasks, with overlapping areas of responsibility and processes. They are more effective when integrated and dealt with as combined practices.

GRC
A management model that promotes criteria unification, communication and collaboration between different stakeholders in the management and control of the organization

Governance
Decides the structure to define an organization's goals and objectives, the means of achieving them and of monitoring the results—with integrated management of "the risks to" the chosen strategy (performance and outcomes) and "the risks from" its operation



Risk management
Makes and carries out decisions based on the identification, evaluation and forecasting of possible events or circumstances that can have a negative influence on assets, to either accept the risk (threats, vulnerability and impacts) or mitigate the adverse effects by applying risk treatment options

Performance management
An ongoing process of communication in support of accomplishing the strategic objectives through evaluation, reporting, correction and improvement that requires clear specification of goals, objectives, requirements and mitigation of constraints—an important task in each GRC domain

Compliance
Tactical actions to mitigate risk; abiding by both industry regulations and government legislation with the communication and enforcement of policies, standards and procedures

Figure 2

For a detailed description of the GRC^2 Model, see pages 20 through 24 of the 2022 PSR.

Integrated program design

The value of tools, models and methods

Why are tools, models and methods important in program design?

For many organizations, a large part of the journey in PCI security and compliance is about moving from a disjointed set of activities to creating a formalized program. When an organization's security direction becomes a series of disjointed initiatives and policies, the outcome is inevitable: a drop in compliance, reduced control effectiveness and increased risk of a breach. To recover, the chief information security officer (CISO) must provide agile leadership and well-structured governance supported by clear communication and strong directives. The use of models and methods can play a significant role in the process of reorganizing to move forward.

Too often, security programs are developed in an ad hoc manner—in a reactive mode with little advanced planning. A well-defined program provides guidance on how to make decisions and allocate resources to achieve overarching program objectives.

Program and project design and management are fundamental skills and processes for PCI security success. Program design is important because it oils all of the parts that make the program run efficiently as a whole. Program and project design typically refer to the initial planning phase conducted by the PCI security compliance steering committee, project managers and primary stakeholders. This planning phase develops important project elements to help ensure success.

Strategy is the heart that pushes a program forward. Instead of short-term projects with small, immediate goals, security must evolve into a long-term program with a mission, objectives and strategy that improves the security posture of the organization. The key objectives of the CISO often include formulating an information security program that leverages collaborations and organizationwide resources, facilitating information security governance, advising senior leadership on security direction and resource investments, and designing appropriate policies to manage information security risk.

A PCI security program should be designed to deliver predictable performance throughout the life cycle of the program. It requires resources to be directed toward a clearly defined goal and establishment of an economical road map with milestones and critical success factors. A well-designed program increases efficiency, accomplishes objectives, and gives internal and external stakeholders what they want every single time. It's a solution for eliminating the waste of resources, addressing low productivity, preventing excessive costs and avoiding stakeholder dissatisfaction.

A well-designed PCI security program:

- Offers substantial support for the development and management of processes and systems
- Uses various techniques to direct and control each step to design and execute activities
- Determines how and when people communicate and form decisions as well as how rational positions are established that serve as a basis for program managers and participants

Integrated security program design models and methods

Change and situation	Model	Application and value
• How do I obtain visibility of the control environment? • How do I design the entire management program? • How do I remove the causes of design and operational flaws and weaknesses?	**The Security Management Canvas**	• Integrated, contextual perspective on the entire management domain • Ordered, structured architecture
• How do I integrate governance, risk management and compliance into one seamless process? • How do I remove inefficiency due to overlapping efforts?	**The GRC^2 Model**	• Synthesizes governance, risk management, compliance and performance management • Improves and achieves economies of scale
• How do I design a management program without missing critical steps and success factors? • How do I establish a critical chain of program activities for optimized execution efficiency?	**The program management life cycle**	• All the critical program management objectives in the correct order • Designed input-process-output chains
• How do I manage the identification, design, introduction and management of security controls? • What are the essential control evaluation steps to ensure effective and sustainable operation of controls?	**The security control life cycle**	• A structured, end-to-end process throughout the life cycle of controls from introduction to retirement • Structured processes for each step across the life cycle of controls
• How do I meet updated requirements in PCI DSS v4.0 to measure and report control effectiveness? • How do I design a process for building, evaluating and monitoring security controls?	**The security control design template**	• All the essential control design elements in a structured template • Critical input for control management and performance evaluation

Figure 3

Program management design mistakes

The following list contains common mistakes organizations make when designing security management programs:

- Neglecting to secure early stakeholder buy-in when establishing the compliance program
- Failing to clearly identify goals and desired outcomes (including building in sustainability and effectiveness of the control environment)
- Setting up a project instead of a program; focusing on project rather than program outcomes
- Underestimating the comprehensive nature and complexity of a security program, thereby not securing the capabilities needed for ongoing program support
- Failing to establish clear program objectives; focusing on compliance and not on effective data protection
- Neglecting to build sustainable processes
- Maintaining organizational silos – hampering communication, performance and sustainability
- Focusing on technology; undervaluing processes and procedures
- Forgetting, underinvesting, rushing – inadequate organizational competency development
- Falling short on training and educational efforts

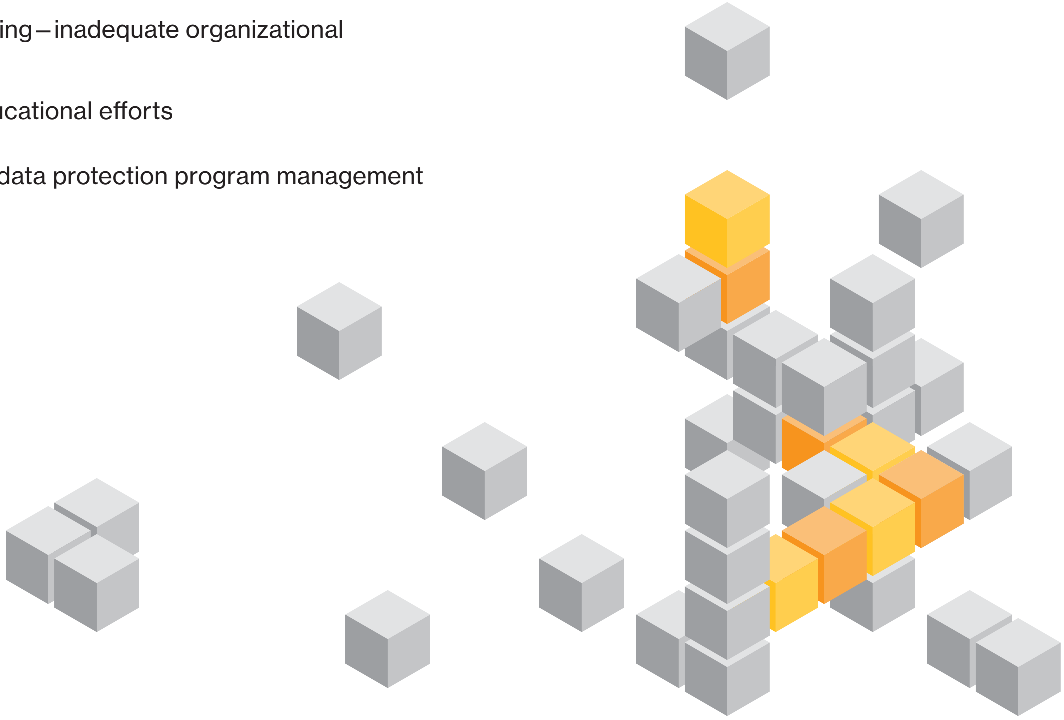
For further reading, see "General data protection program management principles," 2019 PSR, page 18.

Program improvement initiatives

There are only two ways to improve the performance and outcome of a PCI security program:

- Improve the procedure or steps in the process.
- Improve the component parts used in that procedure (including people).[9]

There is no other way. Best results are achieved when you apply a method for logically integrating the improvement of components and procedures.



[9] Ron Carroll, "Box Theory™ for small business – create high-performance systems," accessed August 7, 2023, https://www.boxtheorygold.com/blog/box-theory-for-small-business-create-high-performance-systems

Control environment

It's important to know that the achievement of sustainable control effectiveness depends on the overall control environment. You should never assume you can improve your compliance environment without including in the equation the effects of your higher-level environments. You need to know how your PCI security compliance subsystems relate to the larger systems in which they operate. This requires the application of systems thinking (see the 2022 PSR, pages 9 and 71).

An organization's control environment has a pervasive impact on the overall system of control. Most aspects of program performance are directly or indirectly influenced by other components within the (larger) control environment. Designing and performing tests at the control environment level can be a complex and challenging task—hence, many organizations focus their attention only on the lower-level subenvironments.

Defining the PCI security control environment

We often refer to control environments to explain the overall larger system within which a PCI security compliance environment operates. A control environment is a continual managerial process with structures and standards that provides the basis for carrying out internal control across the organization. It should be clearly defined, documented, communicated, evaluated and maintained. It's comprehensive—meaning it includes all the actions taken by management to manage the environment; strategic governance and operational day-to-day management of activities; and all participants, policies, standards and procedures, tools, processes, and documents.

Control environment: The entire environment—the combination of all environments and components that exercise influence over your compliance environments and the security of data

Compliance environment: The entire PCI security compliance environment—all components included in the scope of compliance and validation, including requirements from several security standards

Cardholder data environment (CDE): The core payment account data storage, transmission and processing environment

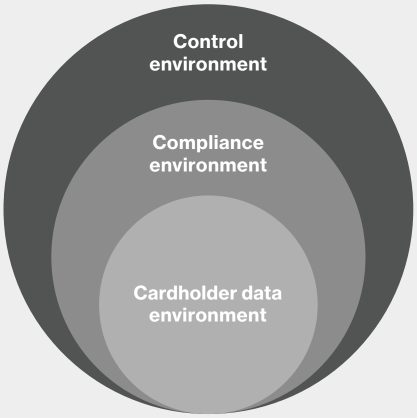
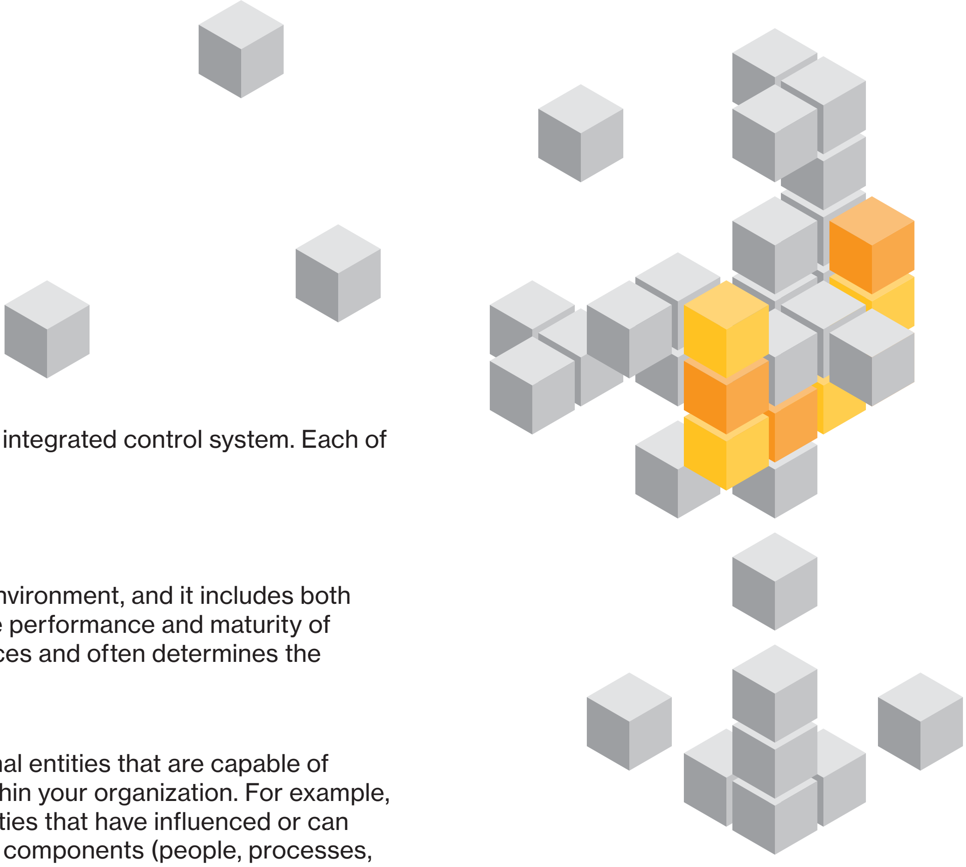


Figure 4. Mapping the overall in-scope environment



These three environments make up your entire integrated control system. Each of these environments is briefly explained below.

1. Control environment

The control environment is the broad, overall environment, and it includes both external and internal control environments. The performance and maturity of the overall control environment directly influences and often determines the performance of its subenvironments.

External control environment
This environment includes all the external entities that are capable of exercising influence over conditions within your organization. For example, each business has various external entities that have influenced or can influence aspects of their business and components (people, processes, documentation and IT systems) and that also affect the organization's internal control environment.

Internal control environment
This environment is governed internally by a set of structures, policies, processes and standards that provides the basis for carrying out internal control across the organization. It includes all the control activities, information and communication, risk assessments, and monitoring activities that the organization applies to adhere to internal policies, standards and procedures. This environment typically includes your broader governance, risk and compliance scope – PCI security as well as other regulations to which an organization must adhere.

What is an effective control environment?

Competent people understand their responsibilities and the limits of their authority within an effective control environment. 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 continually improved.

2. Compliance environment

This environment includes all compliance components (system components and other components within the scope of compliance and validation). Some are included in the CDE, and some are outside the CDE, such as the connected-to and security impacting system components.

Scope of compliance: This scope includes all applicable system components, people and processes that are subject to PCI DSS control requirements. In addition to the CDE, other in-scope components include:

- Any component that can affect the security of account data or a store, process, transmit (SPT) component
- Any component required for the compliance of an SPT component
- Any system component that can directly connect to any SPT component
- Any system component that can indirectly connect to any SPT component
- Any system component with unrestricted connectivity to any SPT component
- Any system component that segments CDE systems from out-of-scope systems

Scope of validation: This scope includes all of the compliance validation assessment tasks that must be applied to system components, people and processes – regardless of whether they are included or excluded from the scope of compliance. For example, during external assessments, qualified security assessors are required to sample various components, even when they are excluded from the defined scope of compliance. This is done to confirm that all the required scoping and compliance criteria are met, to validate the accuracy of the defined scope, and to confirm the compliance of all components. The validation scope will always be larger and include more system components than the scope of compliance. Any system that is in scope of compliance is automatically also included in the scope of validation, but not the other way around.

Compliance environment

The compliance environment may also include components subject to requirements from other PCI security standards (apart from the DSS) that make up the broader organizationwide scope of the payment card data security compliance environment. This presents the body of in-scope components that are required to be in place for the security of payment card account data and compliance with PCI DSS requirements.

To reduce the scope of compliance, organizations should avoid any unnecessary inclusion of system components, people and processes from the CDE. Such components often still need to be included in the scope of validation to substantiate and confirm the validity of their exclusion from the scope of compliance.

3. Cardholder data environment

The CDE is the core payment account data storage, transmission and processing environment in the scope of PCI DSS compliance and validation. It includes all system components that store processes or transmit payment account data (cardholder data or sensitive authentication data) – referred to above as an SPT component.

Control environment sustainability

Sustainable security and compliance are understood as the development of a control environment that meets the needs of the present without compromising the ability to meet goals and objectives in the future.

According to 2022 PSR key findings (page 82), fewer than half (about 43%) of organizations maintain sustainable control environments. Too many organizations don't know how to effectively measure the strength of their PCI security programs. Control environments and security controls tend to degrade if they are not maintained. Organizations often don't notice a deviation from the performance standard because they don't monitor and measure the performance. They also may not have a standard against which they can measure the performance of the program or an effective method for executing program evaluation. This deficiency usually results in a series of negative consequences, such as:

- The control environment sustainability is unspecified, undocumented or not known.
- Objectives don't drive the program toward sustainable control effectiveness.
- Capability maturity is not known or is poorly understood; the path to improvements is unclear.
- Individual control and control system effectiveness aren't known, are unspecified or are undocumented.
- There is management of individual controls instead of control systems, and control systems are not identified (groups of related controls that support a specific control objective).
- Control performance capabilities are uncertain, not measured and not reported (lack of critical oversight).
- The environment experiences unpredictable security control breakdowns.
- The response and recovery of control failures are unstructured and outcomes uncertain.

To address this need, Verizon published 9 Factors of Control Effectiveness and Sustainability in the 2018 PSR (pages 4 through 23). This important model helps organizations apply an integrated evaluation framework for determining the sustainability and effectiveness of a PCI security program. The framework allows for a highly structured, repeatable and consistent method to identify blind spots across the PCI security program. It also facilitates the process of obtaining critical input to define and monitor the internal and external control environment and the controls needed to mitigate risks. At the same time, organizations also need to identify and define the constraints that affect control performance and data protection effectiveness and sustainability as well as define and communicate performance requirements and standards for the design and operation of the control environment.

Control sustainability

In addition to being effective, all critical controls need to be sustainable to reliably meet control objectives. It's important to monitor, frequently measure and report the ability of all critical security control systems to consistently meet all applicable control objectives over extended periods of time. This required level of security control performance needs to be maintained without critical control systems experiencing any significant deviations from their standards of configuration and functional specifications.

The level of sustainability that any security control system can achieve depends largely on the extent to which it's aligned and integrated with its control environment. Therefore, the sustainability of the control environment directly influences the sustainability of controls within the environment.

Tracking the amount of effort and resources (cost, people, attention and time) needed to maintain the required performance and effectiveness can provide important indicators of control sustainability. It's also necessary to monitor the sufficiency of the capacity, capability, competence, commitment and communication requirements in all critical process areas across the environment. (See page 26, "The necessity and value of control design templates.")

Guidance for designing a sustainable program

In general, sustainability issues can get introduced in various stages of the program. For more information, see "The PCI security program management life cycle" on page 22.

To achieve sustainable compliance and data protection, you need to remain in control and proactively manage two challenges: the volume of the workload and the complexity of the tasks. If the volume exceeds your capacity to process it or the complexity exceeds your comprehension to understand and manage the cause-and-effect interaction between components, it will directly affect sustainability.

Rules for achieving manageable compliance and data protection:

- Do not allow the volume of components (information, systems or tasks) to exceed the resource capacity of the people and systems to process it in a timely manner.
- Do not allow the complexity of the tasks to exceed the capability or competence of the people and systems.

The typical steps for managing the volume problem include:

1. **Reducing the scope**

   Control and reduce the scope wherever possible to reduce the amount of work associated with the control environment.

2. **Automating**

   Use templates, and establish work routines and workflows. Automate as many tasks as possible to reduce the manual input required.

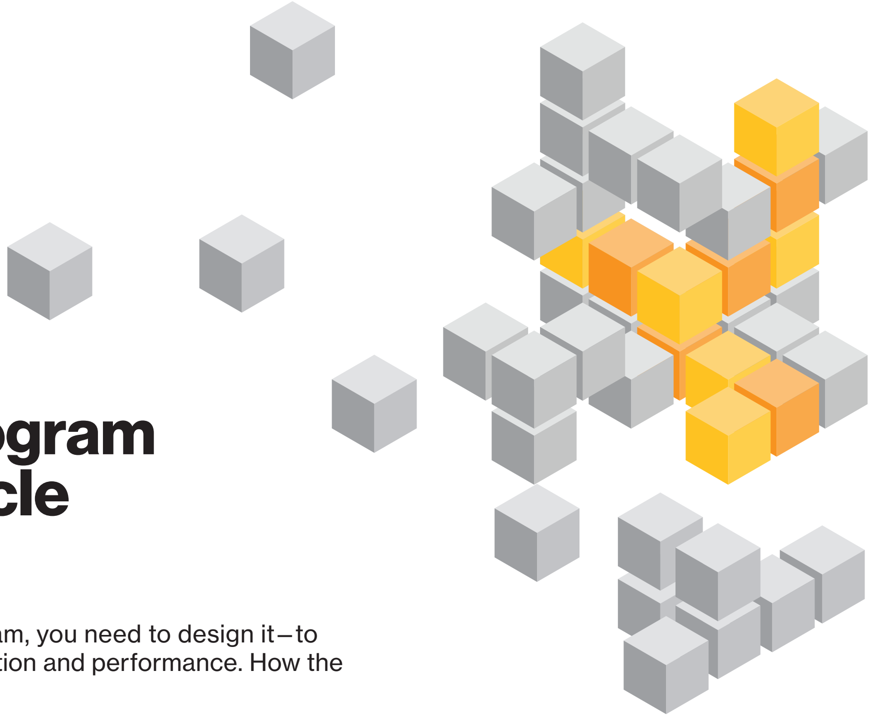
3. **Increasing focus**

   Only work on tasks that contribute to the achievement of the program goal.

4. **Investing**

   Increase the available resources (i.e., hire more people or outsource tasks to third parties).

In general, most issues surrounding complexity can be resolved through analysis and communication and working in a structured manner. That is why integrating your compliance program into a structured change control process is so beneficial to achieve sustainability.



The PCI security program management life cycle

Program architecture

To deliver a high-performance PCI security program, you need to design it–to achieve success by design–with predictable evolution and performance. How the program is constructed matters.

All programs have critical elements and fundamental components. To help address root causes of poor program performance, programs should contain all of these critical components. The components have dependencies and interdependencies and come into focus within various stages of the program's life cycle. All programs have life cycles–stages they go through from conception to eventual end. Life cycles are essential for delivering and improving the sustainability of program performance.

This visual model (Figure 5) is a great way to establish a perspective on how program activities should be structured and how the workflow progresses from conception to completion.

Program life cycle management

A security compliance program refers to the life cycle management of a program with defined stages such as:

1. **Conception and initiation**
2. **Definition and planning**
3. **Launch and execution**
4. **Performance and control**
5. **Continual improvement**

Programs do not exist and operate by themselves. They are created, and their performance is a consequence of how they are designed and interact with the rest of the organization. Therefore, the program structure and approach taken to produce the program architecture–the organization of and relationships between the components and order of execution–matters a great deal. Clear and well-known dependencies and cause-and-effect relationships determine the effectiveness, efficiency of execution and outcomes of a program.

The life cycle of a program is not too different from project life cycle management–but essential differences exist. The difference between programs and projects is that projects have relatively shorter durations than programs.

The three top life cycle stages:

1. **Stage 1: The program planning and design stage**
This is the conception and initiation of the program followed by the planning activities to scope out the work

2. **Stage 2: The program execution and management stage**
After the program is launched, a structured, predetermined method is needed for managing and controlling the performance of the work. This includes control of the scope, resource capacity and other key metrics within all associated projects.

3. **Stage 3: The integrated program performance evaluation and improvement stage**
It is initiated after the launch of the program and runs in parallel with program management. You need to measure the effectiveness and efficiency of the program. Review the qualities of the program deliverables, and evaluate the maturity of capabilities and processes.

You shouldn't ignore life cycle management when aiming for a successful program. If you skip one of these steps in any of the stages, it will have a negative effect down the line.

Program and project life cycle management is, and should be, an integrated part of PCI security program management. It's part of the solution to a high-performance program. The performance of a program, the collection of projects managed collectively by the program, and the rate at which objectives (throughput) are achieved toward the overall outcomes and goals is directly dependent on the quality of the design and execution during each life cycle stage.

1 Program planning and design		**2 Program execution and management**		**3 Evaluation and improvement**	
Conception and initiation	**Definition and planning**	**Program launch**	**Program performance and control**	**Program effectiveness**	**Program efficiency**
Program office Program charter – Purpose – Stakeholders – Assumptions – Risks Program approval	Program plan – Program goal – Requirements – Objectives – Constraints Scope – Work breakdown schedule Budget Risk management	Communication Program and projects kickoff Status and tracking Quality Forecasts	Milestones and objectives Execution and delivery performance – Throughput Monitoring and reporting Management – Scope – Resources – Constraints – Input: Time and effort – Budget	Program outcome evaluation – Quality of deliverables Program process evaluation – Capability maturity – Process maturity Projects performance evaluation – Project postmortems Program design evaluation Continual improvement	

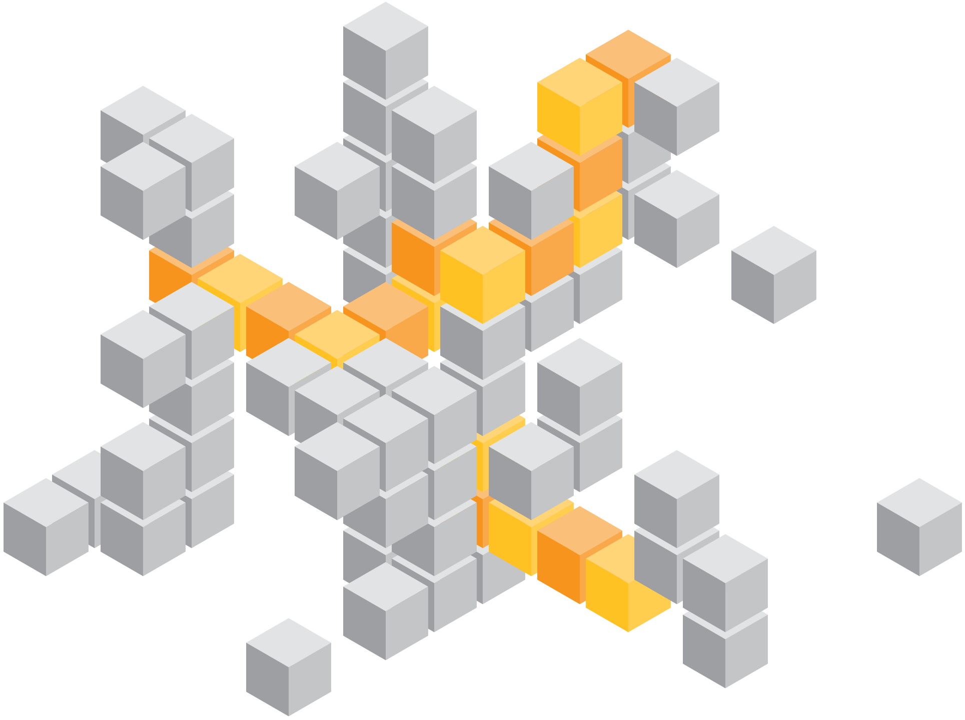
Figure 5. The PCI security program management life cycle

The security control life cycle

In addition to program management life cycles, program designs should also incorporate security control life cycles.

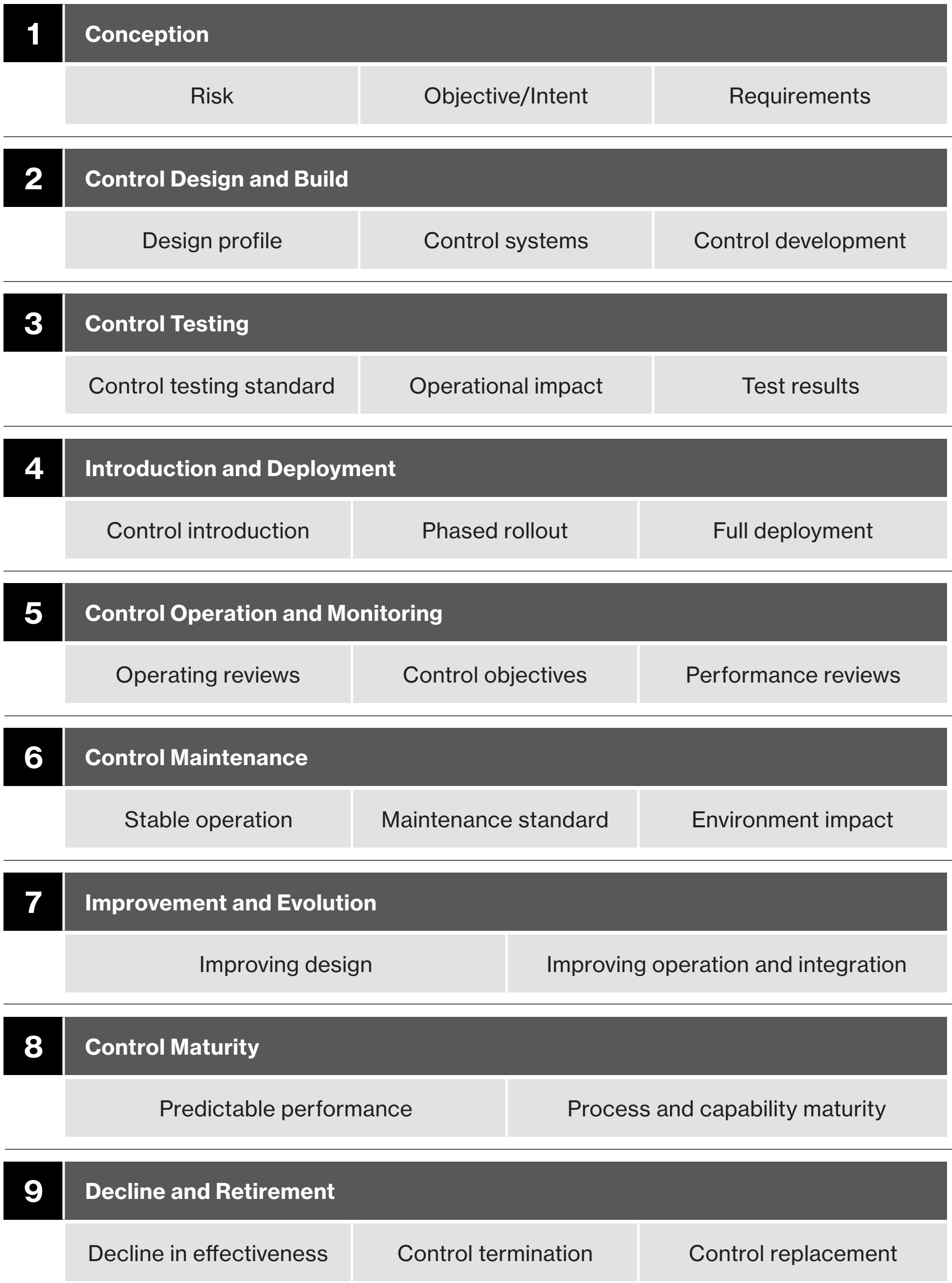
Verizon published a security control life cycle framework in the Verizon 2016 PSR[10] (page 7), republished an updated version in the 2017[11] edition (page 10) and expanded on the framework in the 2018 PSR (page 17).

Data should always be protected by layers of security. The effectiveness with which security controls are managed at each step of their life cycle determines the likelihood of control risk creating exposure and a potential data breach. Lack of understanding of the control life cycle is a factor that can lead to atrophy in control environments. This can ultimately result in security breaches and data compromises. Breaches occur because of the absence or failure of multiple security controls. Controls fail as a result of weaknesses in design, operation or maintenance. In many cases, this is the result of an ineffective control environment. Therefore, it's essential that organizations understand how each stage of the control life cycle can influence the underlying processes, operational efficiency and effectiveness of security controls.



[10] "2016 Payment Security Report," Verizon, 2016, https://www.verizon.com/business/resources/reports/2016-verizon-psr-mainreport.pdf
[11] "2017 Payment Security Report," Verizon, 2017, https://www.verizon.com/business/resources/reports/2017-payment-security-report-en.pdf

The security control life cycle



1 Conception
- Risk
- Objective/Intent
- Requirements

2 Control Design and Build
- Design profile
- Control systems
- Control development

3 Control Testing
- Control testing standard
- Operational impact
- Test results

4 Introduction and Deployment
- Control introduction
- Phased rollout
- Full deployment

5 Control Operation and Monitoring
- Operating reviews
- Control objectives
- Performance reviews

6 Control Maintenance
- Stable operation
- Maintenance standard
- Environment impact

7 Improvement and Evolution
- Improving design
- Improving operation and integration

8 Control Maturity
- Predictable performance
- Process and capability maturity

9 Decline and Retirement
- Decline in effectiveness
- Control termination
- Control replacement

Conception: During the first stage of the security control life cycle, the need for a new control or applicability of an existing control is realized to mitigate a risk or to meet a requirement. The intent and related control objective(s) of the control are clarified and communicated.

Design and build: During Stage 2, the exact purpose and functional parameters of the control or control system are defined. This includes control dependencies and the formulation of control systems. See page 26 for a control design profile template.

Control testing: This is the application of a documented control testing standard and procedure to evaluate the extent to which the control meets prescribed functional and operational specifications in actual practice within its target control environment. Documenting test results.

Introduction and deployment: This is the phased introduction and broader deployment of the control or control system. New controls seldom perform flawlessly from the start and likely require tailoring during and after deployment to iron out shortcomings.

Operation and monitoring: This is the systematic review, by collecting, storing and reporting state and performance data over time, and supervising control activities to determine if control objectives and performance targets are being met.

Control maintenance: This is the operation of the control system, with planned, predictive, preventive, corrective or adaptive control maintenance to keep the control operating to standards. Reducing impact from and adapting to changes in the control environment.

Improvement and evolution: This is the application of control modifications or improvements to strengthen the design, integration and operation of the control system. They improve efficiency and effectiveness within the control operation and interaction between environment components.

Control maturity: During the maturity stage, the control system is established and has a track record of performance meeting functional and operational requirements, with a reasonable level of robustness and resilience. Control design and operation capable of continuous improvement.

Decline and retirement: This is the replacement or termination of a control from an operational environment when it has reached the end of its useful function or is being replaced by a more effective or efficient control.

Figure 6. The security control life cycle (2018 PSR, page 17)

The necessity and value of control design templates

Using templates provides substantial benefits for control system improvement, including the ease, transparency and consistency they provide in deploying, operating and maintaining controls. Templates assist in the early detection of control design and control operation issues. They also contribute toward the effectiveness and strength of the control environment, providing much-needed perspective on control purpose, function and operational limitations.

At a basic level, a typical PCI DSS control profile document should include the following:

Control objective

Defines the applicable control objective(s) of the control or control system

Control owner

Assigns ownership and responsibilities

Control function

Describes the control function, e.g., management, procedural, technical

Control type

Describes the control type, e.g., preventive, detective, corrective, directive

Architecture

Defines the control architecture, e.g., system-specific, common, hybrid

Control risk

Describes key risks that the control mitigates, e.g., using control-to-risk matrix or mapping

Control testing

Describes or references control test procedures and standards

Implementation

Specifies implementation scope, control, procedure implementation and dependencies

Operation

Documents control operation specifications; defines scope processes, operational dependencies, supporting processes and control support requirements, and impact (people, systems, processes, third parties)

Maintenance

Addresses control maintenance specifications, scope and maintenance processes

Performance metrics

Provides a list of PCI DSS KPIs and other metrics by which control performance should be measured

Governance

References related policies, standards, frameworks and regulations

Figure 7

For more details on documenting control profiles, see page 12 of the 2018 PSR and page 60 of the 2022 PSR.

Efficiency vs effectiveness

Many organizations overemphasize efficiency with their PCI security program management approaches. Such approaches tend to measure and incentivize the implementation of PCI security requirements in the shortest possible time. This often leads to a "checkbox" approach, which may not result in producing a truly effective control environment.

It's important to differentiate between an efficient and effective PCI security approach.

- **Efficiency**
  Doing specific tasks in an optimized way that results in the least waste of time, effort and resources
- **Effectiveness**
  Doing the right tasks to achieve the required outcome, regardless of the time it takes—the ability to produce a better result that delivers more value or achieves a better outcome

So effectiveness is doing the right tasks, while efficiency is doing tasks right. Either requires the assumption that you can define what the right outcome is and what tasks should be done.

And it isn't one or the other. Although you should try to be effective first, you also need to consider how efficiently you are spending your time and resources. Efficiently doing the wrong tasks is a waste of time; efficiently doing the right ones is how you succeed.

How do you create efficient teams?

- Focus on getting maximum output with the least amount of time and effort.
- Use a methodical work process.
- Define and follow rules.
- Embrace standardization and automation.

A team that is highly efficient but lacks effectiveness may spend too much time ensuring that deadlines are reached and boxes are ticked. They may do this without prioritizing the right projects. Teams need to identify what needs to be done (establish the correct goals and objectives). Only then should investments be made to optimize processes to work more efficiently. Improved efficiency increases the speed and volume of output. But the results can still be wrong. A focus on efficiency can also be a distraction from achieving goals. Keep in mind that any task that isn't furthering your organization's security and compliance goals doesn't really matter.

The 7 Data Security Principles

There is immense value in understanding the principles of data security. These are the fundamental building blocks for the design and management of a successful PCI security program:

- Success is achieved by design, not luck.
- All controls must be effective, not just present.
- Controls have dependencies and function with control systems, not in isolation.
- For controls to be sustainable, their control environment must also be sustainable.
- Operating performance indicators should be measured and reported.
- The input, activity and output of all core processes must be consistent and predictable to support timely detection, prevention and correction of performance deviations.
- Continual improvement must be made toward adequate process and capability maturity.

Do not neglect the fundamental principles.

Source: 2020 PSR, page 14

How do you create effective teams?

- Focus on doing the right things in the right way.
- Stay results driven.
- Focus on the big picture.
- Shift priorities as necessary.

Effectiveness means understanding that the best outcome is a moving target. It requires using foresight to determine where resources should be invested for the best results. Effective teams invest time and energy where their influence will be greatest.[12] Improved effectiveness increases the achievement of the intended results. However, it may be achieved at a slower rate if the production process has low efficiency. Do you want to go faster in the wrong direction or slower toward the correct destination?

Top 7 Strategic Data Security Management Traps

Lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational architecture design and execution. (See the 2020 PSR, pages 12 and 22 through 61, for elaboration on these traps.) Addressing these impediments will not only build a strong compliance bridge but also a program that can adapt when necessary.

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

Finding the balance – becoming efficiently effective

With so much to do, organizations understand the value of being productive. Although security and compliance teams strive to be more efficient and want to tick off more daily to-do list items and complete more in less time, they need to prioritize work that contributes to the achievement of goals – that is, prioritizing effectiveness over efficiency.

All PCI security programs should be designed to prioritize effectiveness before efficiency.

Ultimately, teams should strive to become efficiently effective, which means doing the right things well and maintaining the correct balance between efficiency and effectiveness.

[12] Maggie Wooll, “Still chasing efficiency? Find out why effectiveness is a better goal,” BetterUp, 2022, https://www.betterup.com/blog/efficiency-vs-effectiveness

This concludes this brief paper on advanced payment security program design. For details on advanced security program evaluation, please reach out to the Verizon Payment Security Practice at paymentsecurity@verizon.com.

About Verizon Cyber Security Consulting

This research publication is a product of Verizon Cyber Security Consulting, a global leader in payment security with a security team of more than 600 consultants in 30 countries. Verizon has one of the leading teams of PCI qualified security assessors.

Verizon is the longest-running global PCI security services provider in the world, offering services since 2002. Our payment security practice provides PCI security and SWIFT consulting, assessments and program maturity improvement services. Across our Cyber Security Consulting portfolio, Verizon offers services that help clients identify, protect, detect, respond and recover from cyberthreats while helping ensure compliance with applicable regulations and standards.

Payment Security Report

Direct access to our collection of payment security research reports: https://www.verizon.com/paymentsecurityreport

Verizon 2023 Payment Security Report insights

Advanced PCI security program management design white paper

Published August 2023

Editorial team

Lead author
Ciske van Oosten

Lead editor
Cynthia B. Hanson

Verizon Cyber Security Consulting

Managing Director, Security
Kristof Philipsen

Associate Director,
Global GRC leader
Sam Junkin

Payment security consulting practice

Global lead
Sebastien Mazas

Americas region
Matt Arntsen

APAC region
Ferdinand Delos Santos

EMEA region
Loic Breat

Global business intelligence
Ciske van Oosten

Legal review
Rishard Cooper
Sudha Kantor

Team email
paymentsecurity@verizon.com

verizon.com/paymentsecurityreport