2024 Payment Security Report

Verizon Cyber Security Consulting

verizon
business

About the cover

The unfolded blueprint on the cover is a visual representation of program evaluation architecture with dimensions, specifications and boundaries for the structured measurement of program performance. Tucked inside is a partial cube—either under construction or deconstruction. Through a series of logical steps, the structure can evolve according to an increasingly mature blueprint design.

The different colors of the blocks present an abstract taxonomy of program evaluation functions—such as processes (orange blocks), capabilities (blue blocks) and responsibilities (green blocks).

This concept is a continuation of the cover from our 2023 white paper, "Advanced PCI security program management design," which features a 5x5 cube that depicts the complexity of security program management. The Verizon 2024 Payment Security Report cover is meant to convey the critical next moves—Payment Card Industry Data Security Standard (PCI DSS) post-implementation performance evaluation.

The ongoing investment and economical management of PCI DSS compliance prompts fundamental questions, such as:

- How do you know that you are getting the right work done in the right manner to help secure your payment card data and maintain sustainable compliance?

- How should organizations measure security control effectiveness, report their return on investment and express the business value of their PCI security program?

Without measuring and evaluating the most relevant metrics, your answers to these questions are likely to be merely your best guess. There is no need to guess what your next five moves should be to improve the maturity of your PCI security compliance management capabilities.

"If you don't measure it, you can't manage it" is an often-quoted business maxim. Organizations have yet to sufficiently formalize the methods, metrics and tools for measuring and optimizing the management of their PCI security program performance.

It's not about cramming more activities into an overloaded schedule. When done right, a well-constructed program measurement and evaluation plan is about doing less by focusing on what matters most. To simplify your compliance performance evaluation maturity, this report outlines an integrated set of time-tested program evaluation methods and models.

Table of contents

1

2

3

4

1 | About the report

Each year, Verizon Cyber Security Consulting publishes the Payment Security Report or a white paper to highlight Verizon's approach to some of the most pressing payment security concerns in the industry. Our deep thought leadership keeps you educated on how to problem solve challenges and navigate trends and developments in the increasingly complex, evolving landscape of payment security. Our time-tested models, methods and techniques emerged from 20 years of research highlighted in this report. Readers are left with concrete, practical knowledge and the capabilities to help maintain and sustain their payment security programs year after year.

First published in 2010, the acclaimed report is widely considered among the leading payment security publications in the world and is highly regarded in the industry by analysts, clients and security leaders. Recent thought leadership content has focused on the transition from the PCI DSS version 3.2.1 to version 4.0x.[1] In addition to cutting-edge insights on payment security compliance management, the report includes a "State of compliance" section with valuable data on yearly compliance performance. Reading this publication can help you and your organization problem solve payment security challenges, build sustainable frameworks specific to your needs and improve compliance management efforts beyond merely increasing project execution efficiency.

This report provides tools, tactics and methods that can help you adapt to a constantly evolving payment security landscape and make security and compliance management increasingly robust with more-predictable outcomes.

Ciske van Oosten
Head of Global Business Intelligence
Verizon Security Assurance Division

Reader feedback

"
The Payment Security Report is one of the essential elements to define long-term compliance with the challenges facing us in the financial sector. As part of our multiple certifications, it helps us anticipate difficulties, define in the long term the means to be put in place, and, consequently, maintain our level of security and compliance."

Frank Lavenant
CISO, STET

"
The Payment Security Report is eagerly awaited reading and appreciated every year by the Accor teams. It's a primary source of information for discovering the latest trends and analysis in compliance and data protection. I share, keep and use these reports every year to inspire my PCI DSS community. It is also an excellent training vehicle for our internal users. Testimonials and case studies allow me to illustrate issues that we often do not encounter in our industry but that alert us to potential risks related to payments. The infographics, the information sheet and the full report are very useful."

Marie-Christine Vittet
VP Compliance, Accor

"
This is what I have been talking about for years: how to design a program and have the correct elements in place. I have not seen a publication and presentation like this in the years we've been doing PCI security. Very valuable advice! We can do more to formalize our [security and compliance] life-cycle management. The governance models are very useful and interesting for us, too. We need more guidance like this."

Risk and security management director
Medium-sized Asia-Pacific industry organization

---

1   The "x" designates any incremental or future versions of the PCI DSS.

Verizon Payment Security Report history

Dealing with evolution

A review of the changing compliance requirements, with insights into the importance of sound decision-making and how organizations can position themselves for success

Achieving sustainability

A focused look at improving the sustainability of compliance and a review of the state of scope reduction and payment security

Establishing internal control

The importance of establishing and maintaining an internal control environment and a holistic approach, including security control life-cycle management

Evaluating program performance

How to achieve high-performance security programs with sustainable and effective controls in a predictable manner and address constraints that prevent continual improvement of process and capability maturity

Payment Security Report insights white paper

How to negotiate PCI DSS v4.0: A defined approach to prepare for PCI DSS v4.0 and overcome challenging new requirements

Payment Security Report insights white paper

Advanced PCI security program management design: The fundamental elements for the design and life-cycle management of a PCI security program

2010	v2.0
2011	
2014	
2015	v3.0
2016	
2017	v3.1 / v3.2
2018	
2019	v3.2 / v3.2.1
2020	
2021	
2022	v4.0
2023	
2024	v4.0.1

Complexity and uncertainty

An exploration of the complexity of PCI security, the growing pains of PCI compliance and the need to evolve toward a process-driven approach for compliance

Simplifying complexity

A review of the value of compliance, the effect of PCI DSS changes, the need for sustainability and how to improve scope reduction and compliance program management
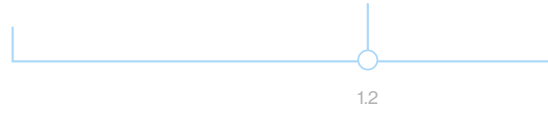
Developing proficiency

Developing data security proficiency, skills and experience, and applying a structured approach to compliance management

Sustainable control effectiveness

Introduction of five practical models to achieve sustainable control effectiveness across your control environment, including the 9 Factors of Control Effectiveness and Sustainability and the 7 Constraints of Organizational Proficiency

The underlying reasons for low control effectiveness and sustainability

The value of a strategic approach to security compliance management and how avoiding the Top 7 Strategic Data Security Management Traps contributes to reduced complexity and helps chief information security officers (CISOs) and their teams be more productive and successful

A logical process for meeting PCI DSS v4.0 goals and requirements

How to navigate the changing requirements introduced by PCI DSS v4.0, with clear goals, a logical process and innovative models that eliminate core conflicts and constraints

Program performance evaluation

Essential PCI security program measurements, metrics and performance evaluation to improve security and compliance outcomes

Executive summary

PCI DSS v4.0x post-implementation measurement and evaluation

Compliance management requires an investment of resources. More than ever before, organizations need to apply management methods that offer clear visibility and perspective to deliver necessary work as economically as possible—with the least amount of waste. They need proven methods that focus on moving from treating symptoms to addressing the causes of poor security program performance—making program input, processes and output highly predictable. Several compliance management program evaluation methods were tried and tested during the past decade. Verizon remains at the forefront, evaluating, designing and publishing a series of models and techniques that can help launch organizations forward to successfully navigate the increasing complexity of PCI security compliance management challenges.

This edition of the Payment Security Report presents an integrated approach, using industry-leading methods and models, for organizations of all sizes and across all industries. Our goal is to take a comprehensive approach based on our telescopic view to help simplify and improve the design and operation of virtually every aspect of your PCI security program.

"

Success is the product of daily habits—not once-in-a-lifetime transformations. ... You should be far more concerned with your current trajectory than with your current results."[2]

James Clear

The methods and concepts highlighted in this report can help organizations evaluate programs and projects, focus on what matters, and simplify security compliance operating environments. They are tailored to help facilitate overcoming the most important constraints by:

- 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

- Bringing the most critical program management evaluation elements to the forefront

- Understanding the necessity for formal program management practices, critical chains and maturity models to guide and assess such an implementation

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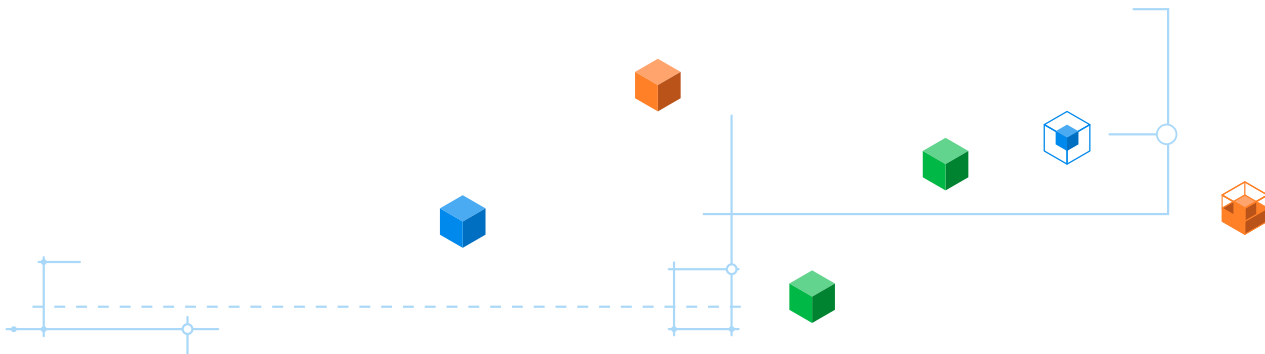
---

2   Excerpt from ATOMIC HABITS: AN EASY & PROVEN WAY TO BUILD GOOD HABITS & BREAK BAD ONES by James Clear, copyright © 2018 by James Clear. Used by permission of Avery, an imprint of Penguin Publishing Group, a division of Penguin Random House LLC. All rights reserved.

PCI security compliance program performance data can and should be a source of strategic value to any compliance initiative. Many organizations already have processes for collecting much of the data needed to measure and evaluate an organization's program. The problem is that organizations often work with various streams of data—different internal sources, operational data from other departments and third-party suppliers. This data usually is kept in different systems. As a result, it may be difficult or impossible for the security compliance management team to maintain a comprehensive view of program and security controls performance. There are often blind spots. For example, lacking the ability to integrate reporting from various internal control environments, the security compliance governance teams may not be able to track certain system components and compliance areas and know the extent to which each area relates to and affects other areas/environments across the organization. It then can become hard to predict how changes in the organization's mix of components and participants would influence the effectiveness and sustainability of the overall control environment.

What organizations need is a way to join the data together—a framework that makes it easy for security compliance program participants to collect and analyze it. Leaders from different parts of the organization need to be able to see the data most relevant to them to evaluate the performance of the PCI

DSS program—and their contribution to it. The process should teach them how to use that data to drive performance improvement and cost management as well as to know where to focus funding and resource allocation related to the PCI security compliance program. Even some of the leading compliance management applications available today lack essential functionality: They are lacking in critical performance measurement areas, which can leave users unaware of significant blind spots in the coverage and perspective of their program evaluation.

"

Ultimately, it is your commitment to the *process* that will determine your *progress*."[3]

James Clear

Overview of content

In this publication, we bring to the forefront the next logical step in the journey to meet PCI DSS v4.0x requirements. We share proven methods for formalizing the evaluation of your security compliance management program. We discuss how to apply an integrated framework for measuring the effectiveness and sustainability of the control environment by mitigating common constraints of program performance across the 4 Lines of Assurance. (See page 27.)

We review the value of measuring and reporting PCI DSS control performance metrics and key performance indicators as well as the limitations of measuring and improving PCI DSS programs using maturity models. These, and many more models highlighted in this report, can help move your program evaluation to a new level.

PCI DSS state of compliance summary

This report's "State of compliance" section strives to show where organizations may not be meeting PCI compliance standards and exposing themselves to business risk. With each edition, we include an analysis based on research to provide a compliance summary. Our 2024 summary is the result of multiyear research we conducted in an attempt to better understand the relative distribution of data security and compliance capabilities worldwide in the past, present and future. The "State of compliance" section includes data collection, normalization and aggregation to uniformly categorize and present information in a manner that views and compares the evolution of PCI DSS compliance over a period of 10 years—from 2014 through 2023.

The "State of compliance" summary provides analyses of the performance of PCI DSS v3.2.1 during its life cycle.

3   Ibid.

Key findings

A review of PCI DSS v3.2.1 effectiveness

With the payment card industry's collective migration from PCI DSS v3.2.1 to v4.0, to what extent can the new standard, with its substantial overhaul of security and validation requirements, drive improvements in sustainable PCI DSS control effectiveness? At the time of this publication, it is too early to tell.

With the expiration of PCI DSS v3.2.1 in March 2024, it is fitting to review, at a high level, the performance of PCI DSS v3.x throughout its 10-year shelf life. We should ponder the lessons learned from the compliance management experience of v3.2.1 to help us better prepare to meet the PCI DSS v4.0x challenge ahead.

PCI DSS v3.2.1, released May 2018, introduced relatively minor changes— mainly clarification updates and a correction to previous requirements. It went into effect January 1, 2019, and remained in effect for more than five years until it was retired in March 2024—making it the longest-running version of the standard to date.

Conducting an independent interim compliance validation assessment several months before the scheduled annual final assessment provides a good opportunity to identify organizations that keep all their security controls in place throughout the year (sustainable compliance). It also highlights organizations that allow controls to fall out of place by giving controls attention only at the end of the compliance validation cycle to achieve a clean annual assessment.

Sustainability: Organizations are required to achieve and maintain a 100% state of compliance, where all applicable security controls continuously remain in place. We measured organizations across our global PCI DSS assessment dataset to determine, for each key requirement, the percentage of organizations that scored 100% during draft (interim) Report on Compliance (ROC) assessments.

During the lifetime of PCI DSS v3.2.1, fewer than half of organizations demonstrated that they developed and maintained a robust, sustainable PCI security program that enabled them to rapidly detect and correct controls that are not in place. Although many organizations showed some improvement in their capability to maintain control over their network vulnerability assessment processes (scans and penetration testing), Requirement 11 consistently remained the least sustainable across all key requirements.

Control gap: In terms of control gap, the same key requirements—11, 10 and 2—posed the most difficulty throughout the duration of v3.2.1. In 2023, Requirement 11 continued to have the largest control gap, followed by Requirements 6, 10 and 2—which all remained in the bad apples barrel.

Compensating controls: The share of organizations applying one or more compensating controls to meet requirements remained steady throughout the five-year duration of v3.2.1. Requirement 8—followed by 6, 11 and 3—was the most compensated key requirement across the standard.

PCI DSS specifies a minimum baseline set of security controls to protect payment card data. However, it doesn't explicitly specify how organizations should go about monitoring and evaluating the effectiveness and sustainability of those controls after they are implemented. PCI DSS v4.0 advanced closer to post-implementation monitoring and evaluation with its increased emphasis on the need for requirements to meet the intent of their control objectives. Without an explicit need to test the robustness, resilience and overall effectiveness of their PCI DSS controls, many organizations took a "fire and forget" approach to PCI DSS v3.2.1 control implementation. Control effectiveness is not a primary concern in their standard compliance operations and programs. It's not just the controls in the PCI DSS themselves but the approach taken to implement them and evaluate their performance that determines their effectiveness.

Appendices

The appendices in the 2024 Payment Security Report comprise insightful, practical content and are often written by contributing authors.

**Appendix A: The rise and risk of third-party scripts in modern websites.** Threat actors increasingly target third-party scripts to steal data at the point of input. This term spotlights the shift in focus from traditional data targets—data in transit or at rest—to the point where users first input their data. Attackers exploit vulnerabilities in third-party scripts to inject malicious code, which enables them to capture data as soon as it's entered into the online forms that power e-commerce. New updates to Requirements 6 and 11 in the PCI DSS include a requirement to inventory and authorize scripts running on payment pages. Monitoring the script behavior and preventing unauthorized access to this sensitive data is key to meeting PCI DSS v4.0x compliance. A highly effective approach to third-party script management and security involves real-time monitoring and control.

Appendix B: A deeper dive into PCI security performance measurement and evaluation. Performance measurement and evaluation are two key management activities available to help stakeholders (such as the board, executives, CISOs, risk managers and compliance program managers) develop systematic evidence, understand how well the PCI security strategy and program are working, and identify possible improvements.

Appendix C: PCI DSS compliance schedule. The 2024 updated compliance calendar is a visual representation of the schedule of tasks (such as quarterly vulnerability scans and annual penetration testing) with their frequency, action items, resource needs and justifications. By adhering to the PCI DSS recommended compliance schedule for applicable controls that must be performed at various times throughout the year, organizations systematically address many PCI requirements and enhance security practices.
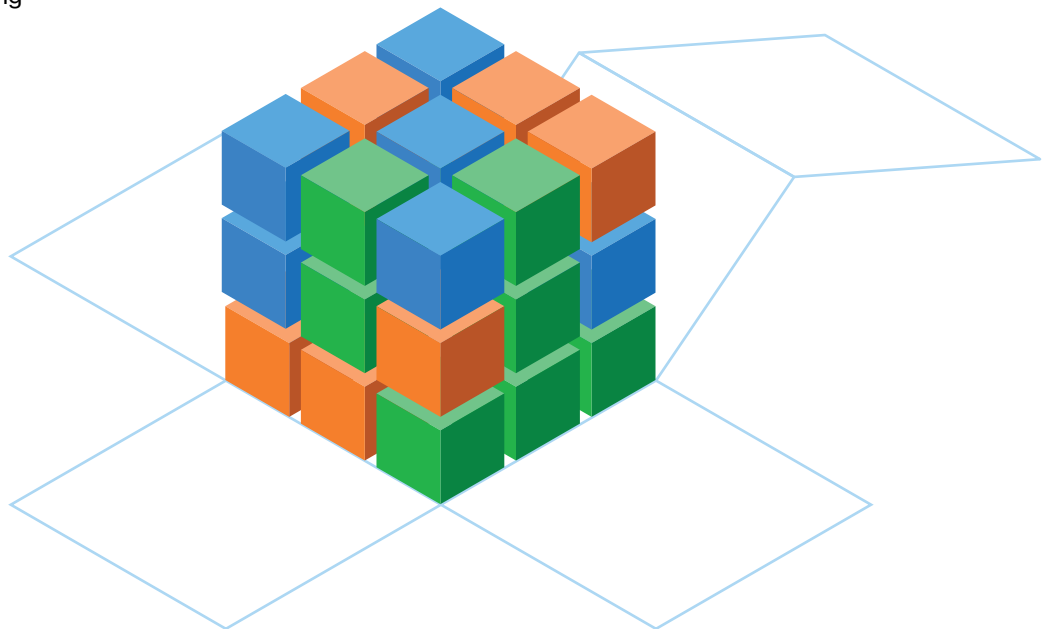
The compliance landscape

PCI DSS v4.0x post-implementation performance measurement and evaluation

PCI DSS v4.0 is arguably the most significant update since the initial release of the PCI DSS in December 2004. The latest version is aimed at improving the requirements and how compliance is measured to meet the intent of the standard—an ongoing, effective security guide for payment card data. Since its release in March 2022, organizations across the world are implementing and maintaining PCI DSS v4.0 requirements. Many focused on the requirements that became effective immediately in March 2024; present efforts continue to meet applicable future-dated requirements that need to be in place on March 31, 2025.

In our previous payment security publications, we looked at the need for a strategic approach to PCI security compliance management[4] and how to design and execute PCI security strategies and programs using logical thinking.[5] In this companion report, we look at performance measures and program evaluation in relation to strategy.

Effective performance measures should drive the behaviors necessary to make changes to continually improve PCI security program performance. Performance measures need to support the organization's data and compliance security strategies. They should provide information for analysis on where improvement is needed and should help manage organizational risk.

Learning from 20 years of compliance validation

Various methods exist to measure the performance of a PCI security program. Even today, after 20 years of PCI security compliance validation, there are still several organizations that do not or barely go beyond tracking and reporting the number and percentage of controls that are in place across their control environment. They do not take necessary additional steps beyond the minimum formal compliance validation and reporting requirements. This is woefully inadequate to manage the input, processes, performance and outcomes of a program and can make it nearly impossible to determine the effectiveness and sustainability of the control environment.

Several new and updated controls in PCI DSS v4.0 include more explicit requirements on evidence of compliance to substantiate that the assessed entity developed, implemented and is maintaining processes to ensure ongoing data security. Evidence of compliance should substantiate that the requirements are effective and processes are maintained to keep them functional and operational, i.e., in place.

Specifically, teams should provide documentation of an organizational capability to rapidly detect requirements that aren't in place combined with the capability to rapidly correct controls and address the causes of such deviations through a functional, ongoing improvement process. This has always been the intent of PCI DSS since its inception 20 years ago. PCI DSS v4.0 brought this to the forefront with several requirements that explicitly demand evidence that such a capability is in place.
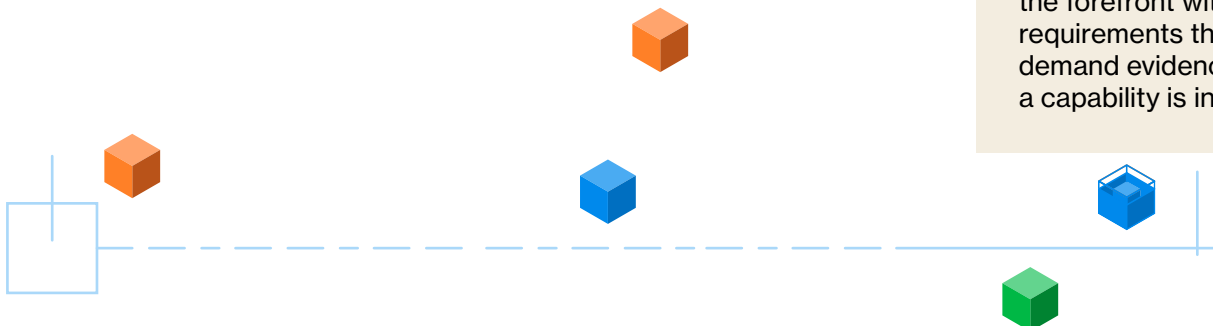
---

4   "2020 Payment Security Report," Verizon, 2020. https://www.verizon.com/business/resources/reports/2020-payment-security-report.pdf
5   "2022 Payment Security Report," Verizon, 2022. https://www.verizon.com/business/resources/reports/2022-payment-security-report.pdf

Many organizations apply a very narrow view of the scope of program evaluation. They erroneously assume that it mainly consists of accurately measuring and reporting:

• The scope of the PCI DSS compliance environment

• The status of each applicable in-scope PCI DSS control requirement (in place, not in place, etc.)

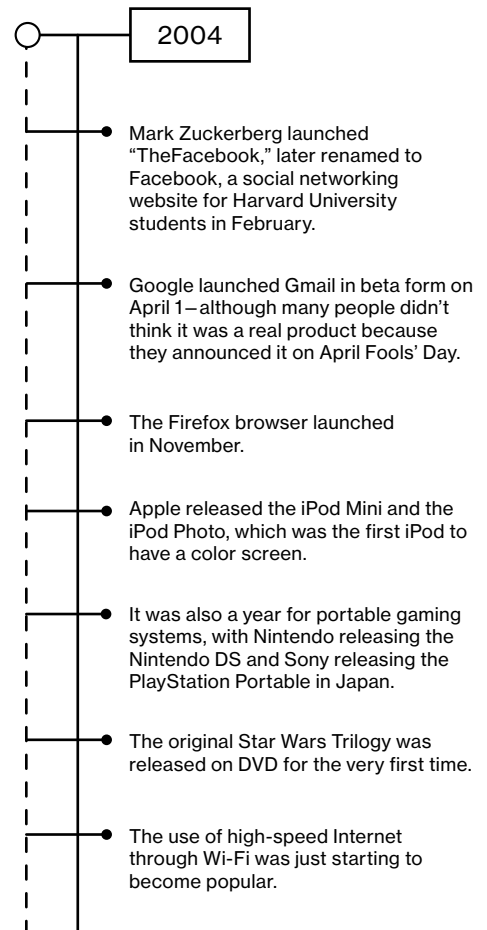• The adequacy of the evidence of compliance and reporting requirements

Although these objectives and deliverables are an essential part of the basic PCI DSS program and performance evaluation, they are a far cry from what is necessary to meet the intent of the PCI DSS control objectives.

It's essential to evaluate the processes that are in place to determine the effectiveness and efficiency of your organization's team, its IT systems and the individual capabilities needed to support the control environment.

Understandably, in the body of knowledge (i.e., the papers and books written on PCI security) over the course of the past 20 years, the scope and methods of evaluating the full extent (strength and maturity) of PCI security program management have not yet received sufficient coverage.

The 20-year anniversary of PCI DSS

Nearly 20 years ago, the first version of the PCI DSS was released in December of 2004. PCI DSS v1.0 was initially developed by Visa Europe and Visa Inc. and released under the Visa brand. The familiar 6 Control Objectives and 12 Key Requirements included in the PCI DSS are the foundation of Visa's data security compliance programs—the Account Information Security (AIS) and Cardholder Information Security Program (CISP).

The founding payment brands, along with participating card brands, aligned their programs to foster broad compliance with the PCI DSS. In 2006, the formation of

the PCI Security Standards Council (PCI SSC) was announced to develop and evolve the PCI security standards focused on protecting cardholder data (CHD) throughout the payment transaction life cycle. Subsequent updates to the PCI DSS resulted from a cooperative effort between Mastercard and Visa and other payment brands to create common industry security requirements.

We have come a long way in the past two decades not only in terms of the evolution of technology but also in our understanding of the cybersecurity threat landscape and how to secure sensitive data.

2004 in history

Technology has made giant evolutionary steps in the 20 years since 2004.

2004

Mark Zuckerberg launched "TheFacebook," later renamed to Facebook, a social networking website for Harvard University students in February.

Google launched Gmail in beta form on April 1—although many people didn't think it was a real product because they announced it on April Fools' Day.

The Firefox browser launched in November.

Apple released the iPod Mini and the iPod Photo, which was the first iPod to have a color screen.

It was also a year for portable gaming systems, with Nintendo releasing the Nintendo DS and Sony releasing the PlayStation Portable in Japan.

The original Star Wars Trilogy was released on DVD for the very first time.

The use of high-speed Internet through Wi-Fi was just starting to become popular.

Worth noting is that YouTube had not yet hit computer screens, Netflix did not have a streaming service, and widespread cloud storage services were mere pie in the sky. The smartphone as we know it—Apple iPhone (in 2007), Android devices (in 2008) and other models—was still many years away. This adds some perspective on how much technology has evolved in two decades.

As mentioned in previous editions, the performance of any PCI security compliance program depends largely on three main factors:

- **Complexity:** The complexity of the control environment and control systems

- **Proficiency:** The proficiency (resources, capability and experience) of the teams managing the control environment

- **Focus:** The level of focus (and investment) put into the planning and execution of the security strategy and program

Central to the factors that determine the performance and outcome of a PCI security program are design and evaluation. A program can only perform as well as it is designed to function and operate. What gets measured (and reported) gets done.

Significance of PCI DSS at the turn of the century

Before the release of PCI DSS 20 years ago (in 2004), no globally standardized yardstick existed for measuring and reporting how well organizations secure payment card data. PCI DSS became the go-to measure that allowed comparisons of data security within industries across the globe. The Verizon Payment Security Report was the first—and remains the leading—industry publication to track the performance, since 2008, of PCI DSS with data-driven grounded analysis.

PCI DSS has been updated 11 times since 2004 to keep pace with the evolution in technology, the threat landscape, and our improved understanding of data security design and management. PCI DSS v4.0 was

released in March 2022, allowing organizations two years to update their compliance environments to meet the new requirements before PCI DSS v3.2.1 expired. Despite this extended lead-in period, several organizations failed to beat the clock. Various Qualified Security Assessor (QSA) organizations continued to observe ongoing 2024 PCI DSS v4.0 transition projects past the March 2024 deadline. While others succeeded, often it required substantial effort. Several aspects of the transition from PCI DSS v3.2.1 to v4.0 may seem complex, challenging and even daunting. And this may be true—especially for organizations that lack a logical method to deconstruct the complexity by first establishing clear goals and objectives, building the capability and capacity to achieve them, and using logical decision-making along the way.

If you want to try and predict how a PCI security program will perform and its outcomes, follow the curve of tiny gains or tiny losses each day, week and month. Observe how the choices made will compound several months and years down the line. Breakthrough performance on compliance management and outcomes can be achieved. It's often the result of many previous actions that build up the potential required to unleash a major change.[6]

6   Adapted from ATOMIC HABITS: AN EASY & PROVEN WAY TO BUILD GOOD HABITS & BREAK BAD ONES by James Clear, copyright © 2018 by James Clear. Used by permission of Avery, an imprint of Penguin Publishing Group, a division of Penguin Random House LLC. All rights reserved.

Which is why this edition is focused on helping readers evaluate the outcomes of their PCI DSS v4.0x projects through time-tested methods and integrated frameworks. In our 2023 insights white paper, "Advanced PCI security program management design," we covered some of the essential elements of program design based on an actionable strategy to overcome the complexities of PCI security compliance management.[7] Continuing on that theme, this report highlights the critical importance of evaluating each aspect of your security program—starting with an assessment of the planning and design of the program as well as analyzing the overall ongoing performance and outcomes.

An articulated overall organizational goal of a PCI security compliance program should be clearly communicated (for example: 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 help achieve this goal, a PCI security compliance program should be integrated with and supported by additional security, risk management and governance frameworks; a security operating model; a strategy; and a security business model.

We highlighted most of these critical success factors of a PCI security program in previous Payment Security Report editions. (See the 2023 insights white paper on program design, pages 14 through 16.)

The business need for compliance performance evaluation

Effective performance measures communicate what is important to the organization. Organizations are required and prepared to invest the time and resources to meet PCI DSS v4.0x compliance requirements. To support business interests, management should maintain effective follow through and measure the performance and outcomes of that investment. The formalization of the PCI security compliance program evaluation is increasingly viewed as very important to an organization's business leadership. If the performance measures do not drive change (such as improved focus and return on security and compliance investment), leadership needs to know the value of the time and resources invested and exactly what needs to be changed and improved first (i.e., the next steps). The performance measures themselves point to where further investigation is required to understand the underlying reasons for the current performance. Organizations need to know what to measure, why it should be measured, how to measure it and how to report the measurements so the necessary changes can be applied for ongoing performance improvements.

Improving the return on investment

Combating cybersecurity threats continues to be of strategic importance to organizations, with security budgets increasing across most industries. Yet there is also a corresponding increase in the emphasis on scrutinizing expenditures to optimize return on investment.

With the introduction of PCI DSS v4.0 in 2022, many organizations realized that they could not continue to keep doing the same activities in terms of program and control evaluation.

They could not keep hanging on to an evaluation approach built for past practices and an outdated standard (PCI DSS v3.2.1). They needed to adapt. Brought sharply into focus, and made an important program priority, is the urgent need to develop a PCI security program performance evaluation approach that is aligned with the latest standard. This approach supports an emphasis that is not on preparing for an annual review but instead on frequent and informal ongoing evaluations.

7   "2023 Payment Security Report insights: Advanced PCI security program management design," Verizon, 2023. https://www.verizon.com/business/resources/whitepapers/2023-payment-security-report-insights.pdf

Security teams are under competitive pressure to upgrade their program management efforts. They are held accountable for designing and implementing updated practices aligned with current requirements. Specifically, decision-makers are held accountable for the outcome of past decisions, especially when they are made at the expense of improving current data security performance and being best positioned for the future—both of which are critical for organizations' long-term survival.

Acknowledging the limitations of PCI DSS

Updating your PCI security program—in terms of both design and evaluation—does not need to be a complex, lengthy and costly process. A PCI security program should not generate mountains of paperwork that serves no real purpose. Organizations need to be aware of and know how to address the biggest limitations of compliance reviews. Specific, measurable and quantifiable metrics should be used to track progress toward goals or objectives. It is within reach of every organization to know what and how to measure program performance and develop the capabilities to keep stakeholders informed on the status and progress of achieving the overall goal of PCI security compliance.

PCI DSS v4.0 introduced numerous new requirements and fundamental changes to the compliance validation and reporting criteria. One example is the customized control approach that provides an unprecedented level of flexibility for organizations to no longer be constrained by the defined approach for security controls. "With great power comes great responsibility."[8]

PCI DSS v4.0 provides a much-improved yardstick to measure data security and compliance capability. In terms of overall page length, the PCI DSS document expanded from 139 pages to 360 pages—mainly due to the substantial volume of additional guidance that is included in the new standard.

The outcome of the changes to the requirements introduced by PCI DSS v4.0, in terms of the ability to sustain compliance and the improvement of control environments, will be increasingly visible by 2025. By then, organizations across the world are required to have completed their validation assessments of current and future-dated controls.

Yet some argue that PCI DSS v4.0 still falls short of the requirements and guidance needed to understand how to move from implementation of the baseline set of applicable controls toward sustainable control effectiveness. It's important to understand the inherent limitations of PCI DSS as a generic industry standard that pertains to all organizations large and small, across all industries and geographic regions, as well as its intended purpose and function of a baseline catalog of security controls.

PCI DSS compliance assessments can and are intended to provide largely objective evaluations of cardholder data security. Even PCI DSS v4.0.1 (the most current version at the time of publication) is not a comprehensive standard by itself to accurately determine the true effectiveness of an organization's data security strategy and to evaluate the distribution of factors and capabilities across a corporate control environment. PCI DSS requirements do not account for all key components of data security. For example, PCI DSS does not include explicit requirements for the evaluation and reporting of security control strength—measuring control design to determine control risk, robustness and resilience—most of which are quantifiable (e.g., training hours). The extent to which a requirement is in place (and its capability to remain in place) still is largely a matter of subjective opinion based on the evidence presented (or lack thereof) and the willingness of the assessors to probe deeper to understand how, in reality, a control environment is capable of supporting controls to be both effective and sustainable.

---

8   The original source of this expression is unknown. It has been incorrectly attributed to Voltaire, but no evidence has been found to support this. Prominent leaders including Theodore and Franklin D. Roosevelt and Winston Churchill made similar statements. It even made its way into a Spider-Man story. "With Great Power Comes Great Responsibility," Quote Investigator®, July 23, 2015. https://quoteinvestigator.com/2015/07/23/great-power

Conclusion

Not all security and compliance spending translates to a proportionate increase in capability. In deciding what data security and compliance capabilities to procure—or simply to maintain in service—executives, decision-makers and planners need to find solutions that bring into some sort of equilibrium the available resources, threat analysis and protection of business interests in increasingly difficult economic conditions.

You can learn how to improve PCI security program evaluation and reporting to stakeholders, including management, employees and regulatory agencies. The research in this report reveals several measurements and metrics to focus on to help achieve clear and concise reporting and to provide actionable insights using dashboards, scorecards and reports.

In conclusion, measuring and monitoring PCI security program performance and operational success is essential to help ensure that your organization is on track to achieve its security compliance goals and objectives. By defining metrics and key performance indicators (KPIs), collecting data, measuring and monitoring progress, and reporting performance outcomes, you can improve your organization's PCI security performance and help not only meet compliance reporting standards but also demonstrate the extent to which your control environments are effectively protecting payment card data.

It's our hope that digesting the methods, techniques and framework for measuring, evaluating and improving PCI security programs described in this publication will be instrumental in helping individuals and teams determine with confidence what work they should be focusing on each day to move forward in achieving each of their data security and compliance program performance and compliance management capability goals.

Program evaluation: Key questions to ask and answer

- Do you know how to evaluate your program management capability? (See page 11 of the 2023 insights white paper for The Security Management Canvas, which highlights the five pillars of security management.)

- Do you know how to evaluate the effectiveness of PCI security controls and the effectiveness of the various control environments? Which methods do you use to determine control effectiveness?

- Do you know how to determine the sustainability of your controls and control environment? (See page 31 for the 9 Factors of Control Effectiveness and Sustainability.)

- Do you know how to identify the top constraints that hamper program performance and how to identify and remove/reduce the most important constraint first?

- Do you know how to construct your compliance evaluation program to integrate each of the 4 Lines of Assurance?

- Do you know how to incorporate respective decision-making and execution authorities and responsibilities?

- Do you know how to make maturity models part of your program evaluation and understand the limitations of maturity models?

Evaluating PCI security program success

A data security compliance program can be considered successful when it delivers a mature control environment with the ability to improve continually in a structured, controlled, cost-effective and predictable manner. This requires the achievement of clearly defined security objectives and outcomes that are aligned with the corporate data protection and compliance strategy, resulting in a control environment that meets or exceeds regulatory requirements.

It's essential that the control environment be demonstrably sustainable, with levels of robustness and resilience, i.e., the ability to operate for extended periods with the available resources without significant deviation from its performance standards. Controls within the environment should operate according to documented design specifications—the ability to frequently measure, monitor, evaluate, report and improve the effectiveness of control systems and their supporting capabilities and processes. These are hallmarks of a successful data security compliance program. (See the Verizon 2019 Payment Security Report, page 21.)[9]

Some components of a successful, mature security strategy and navigational map include:

• Clearly defined program objectives, activities and priorities supported by all stakeholders

• Adequate capacity, capability and competence for ongoing support of all critical processes

• A structure that maximizes the problem-solving capability and agile operations

9   "2019 Payment Security Report," Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security
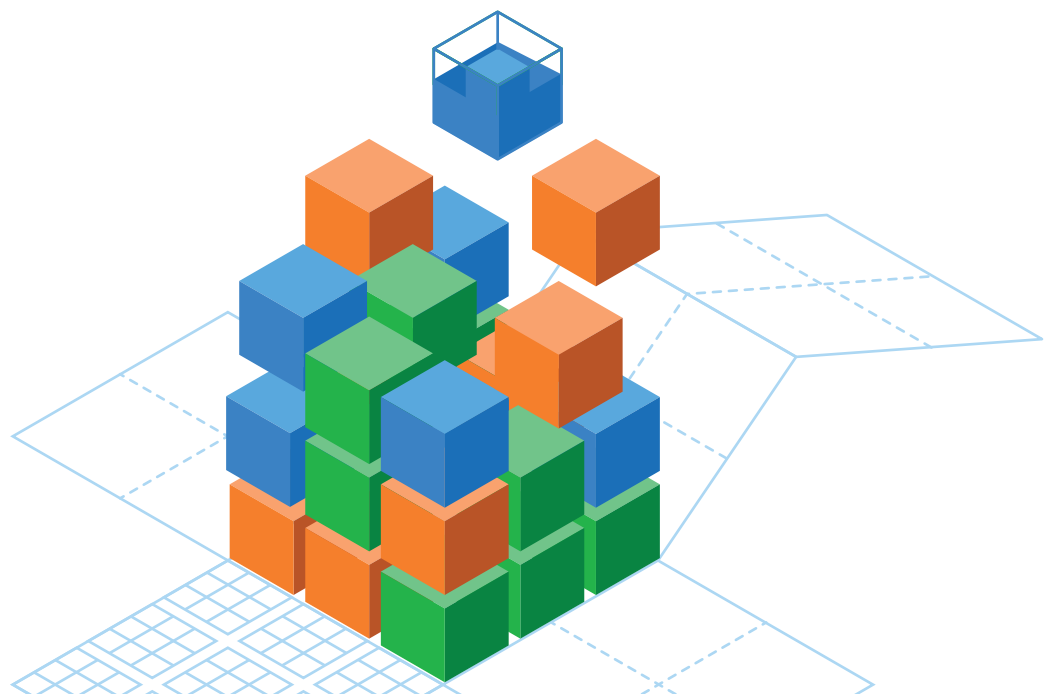
The three stages of compliance management failure

Mistakes happen. The challenges organizations encounter, and the mistakes that occur during the planning and execution of PCI security compliance programs, can generally be divided into three stages of failure: We describe this in the Verizon 2022 Payment Security Report, page 57.

Unraveling the root causes of poor PCI security program performance often reveals a series of undesirable cause-and-effect relationships occurring somewhere within the life cycle of the program (design, implementation, operation, evaluation, etc.):

1. **We don't understand the problem:** the nature, scope and cause of the problem. The security and compliance teams busy themselves by working on problems that do not influence the overall goal of their security program. They focus on symptoms instead of addressing the causes.

2. **We don't understand the solution:** the nature, the scope, how to overcome the obstacles to identify and define the solution, and how to obtain agreement on the solution.

3. **We don't understand how to design and implement the solution:** Design: We don't understand how to obtain buy-in on the solution design.

   Implementation: We don't understand how to overcome the negative ramifications.

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, objectives 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 (e.g., the 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

Figure 1. The three common stages of compliance management failure

Evaluation of a corporate compliance program

You should assess whether your program has established, sustainable procedures that incorporate the culture of compliance into its day-to-day operations.

The three top life-cycle stages
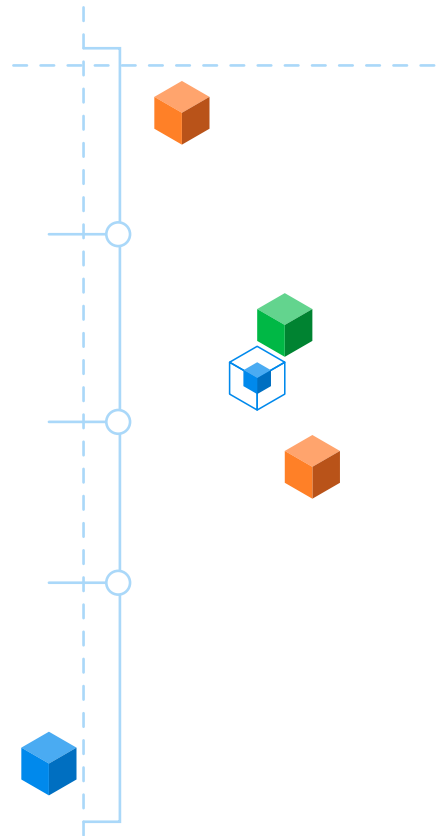
Stage 1: Program planning and design
This is the conception and initiation stage of the program, which is followed by the planning activities to scope out the work.

Stage 2: Program execution and management
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.
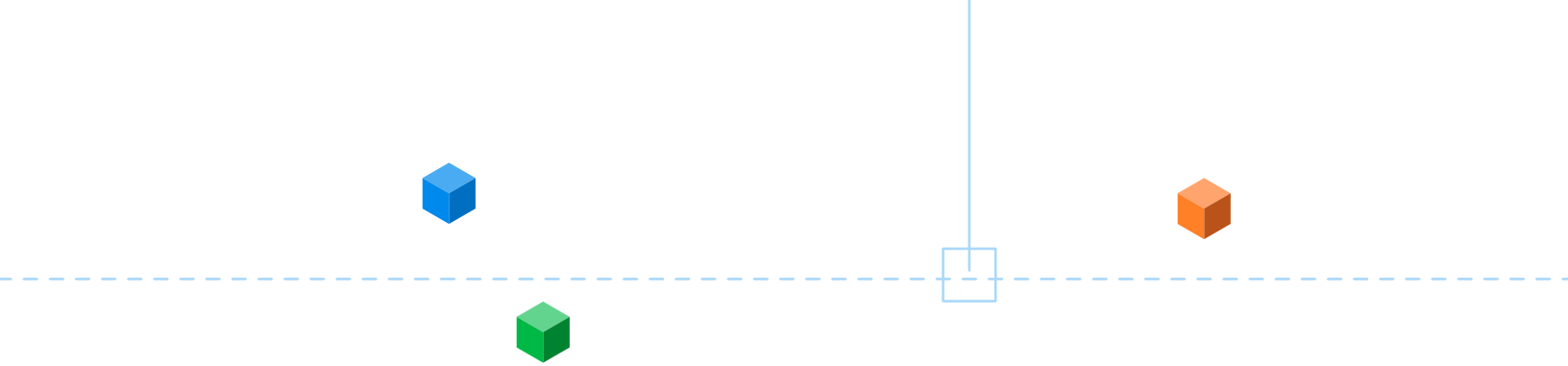
Stage 3: Integrated program performance evaluation and improvement
Initiated after the launch of the program, it runs in parallel with program management. You need to measure the effectiveness and efficiency of the program, review the qualities of the program deliverables, and evaluate the maturity of capabilities and processes.

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 2. The PCI security program management life cycle

Performance evaluation with accurate measurements and metrics plays a pivotal role in any PCI security compliance program. Every PCI security program should have a formalized performance evaluation component to define the performance levels expected of the security compliance processes and operations and ongoing structured evaluation of various aspects of the program. The right process metrics allow you to identify inefficiencies, evaluate the effect of process changes and drive continual improvement—which is part of the overall goal of PCI security compliance. Every organization should be aiming for that target.

Security compliance process metrics provide the data and insights to objectively evaluate how your PCI security processes are working and whether they're aligning with the security program; governance, risk management and compliance (GRC) initiatives; and company business goals. They also facilitate evidence-based decision-making, which enables teams and leaders to make informed decisions to manage business operations, process redesign and strategic planning.

Every PCI security program should have a formalized performance evaluation component to define the performance levels expected of the security compliance processes and operations as well as ongoing structured evaluation of various aspects of the program.
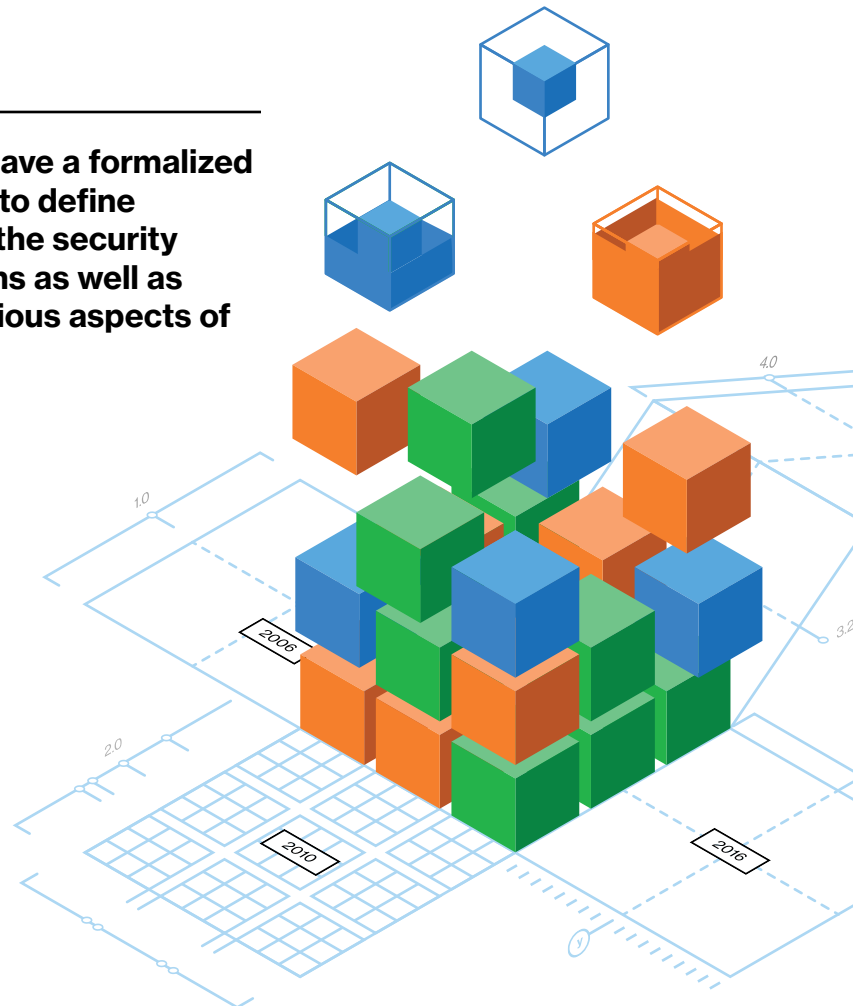
Program evaluation areas in need of attention

Each organization should maintain a documented plan for the development and execution of ongoing evaluation of the following essential program areas:

• The security compliance business case and strategy

• The organizational structure, people (department, team and individual) capabilities, lines of reporting, authority and responsibilities

• Evaluation of (core and supporting) processes

• Evaluation of suppliers and technology

• Evaluation of program and control performance

This should include the full life-cycle performance evaluation, including consistency in reporting, actioning improvements and follow-ups. Other important components to include in your program evaluation are:

• **Design:** What is the organization's process for designing and implementing, monitoring, and evaluating controls? Has that process changed over time? Who is involved in the design of security controls? Are business units consulted before rolling them out?

• **Comprehensiveness:** Does the program incorporate all or nearly all elements or aspects of program management? What

efforts has the organization made to monitor and implement controls that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

• **Risk assessment:** Do you understand the organization from a commercial perspective; how it has identified, assessed and defined its risk profile; and the degree to which the security program devotes appropriate scrutiny and resources to the spectrum of risks? Is the program appropriately designed to detect the particular types of threats and vulnerabilities most likely to occur in the organization's line of business?

• **Risk management process:** What methodology does the organization use to identify, analyze and address the particular risks it faces? What information or metrics does the organization collect and use to help detect weaknesses in the control environment? How do information or metrics inform the organization's compliance program?

• **Responsibility for operational integration:** Who is responsible for integrating security controls? Are they rolled out in a way that ensures employee understanding of the control purpose, necessity and function? In what specific ways are controls reinforced through the organization's internal control systems?

• **Gatekeepers:** What, if any, guidance and training is provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)? Do they know how to detect deviations from procedures and performance standards and which misconduct to look for? Do they know when and how to escalate concerns?

• **Training and communications:** Does the compliance program have appropriately tailored training and communications? You should assess the steps taken to ensure that controls are integrated into the organization, including periodic training and certification for all directors; officers; relevant employees; and, where appropriate, agents and business partners.

• **Accessibility:** How does the organization communicate its security controls to all employees and relevant third parties? If the organization has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access?

To cover this wide spectrum of measurement, it's essential to know what to focus on by applying a tested program evaluation framework.

Effective security program evaluation

It can be argued that many PCI security management programs tend to achieve mediocre performance when viewed in the context of the desired process and capability maturity levels many observers expected across the industry 20 years after the release of PCI DSS v1.0. However, breakthrough solutions do exist and are tried and tested. In the Verizon 2020 Payment Security Report, we summarized the top seven causes for poor PCI security performance. With the release of the new standard, many organizations want to know how they can overcome PCI DSS v4.0x challenges with confidence.

What is needed is a logical approach to solving complex challenges associated with PCI security compliance management. It's about the process of change. Many improvements can be made to PCI security programs—yet every improvement does not contribute to achieving the goal of the program. The likelihood of going astray and losing focus is ever present, and your time and resources come in limited numbers.

The description of the recommended method for achieving continual improvement for PCI security compliance involves a process of change that is oversimplified when you define it in three steps:

1. What to change

2. What to change to

3. How to cause the change

This leaves out an important question that might easily remain unanswered if not asked—why change? (See the 2022 Payment Security Report, page 66.)

Control effectiveness: The degree to which a control is successful at meeting the intent of its control objectives and sustaining the intended vulnerability or threat risk mitigation throughout the life cycle of the control. This is applicable from the functional and operational design, implementation and operation of the control to its end-of-life expiration.

There are four basic questions about change that every manager needs to ask and answer:

1. Why change (what is the goal)?

2. What to change (where is the constraint, the problem; what is the root cause)?

3. What to change to (what to do with the constraint; what is the solution)?

4. How to cause/affect the change (how do you implement it)?

After you add this initial step (Why change?), you can then use the process of change for your whole security and compliance program strategy as well as operational problems—in alignment with the overall goal of the program.

Answering the question "Why change?" tells us something about the direction of a desirable PCI security compliance program, even if that direction still needs articulation. "Why change?" is a result of the dynamic tension between where we are now and where we want to be in the future. Sometimes we don't even write down where we want to be in the future. We just feel that we are not taking the right actions now to be in the right place in the future.

Step 1 tells us about the desired direction of the security strategy and program. Steps 2, 3 and 4 tell us about the direction of the solution and how to implement it.

A logical approach for the design of an effective management program

Following a logical, step-by-step process for an effective management approach is best. This will avoid omitting important steps and making mistakes that result in poor compliance performance and nonachievement of objectives and your goal.

Security compliance steering committees and persons responsible for designing compliance strategies and programs can incorporate this high-level, stepped approach to evaluate and improve their own approach to compliance management.

Step 1: Purpose before planning. Before you start to plan any activities, understand your goals. What are you aiming for? How will you recognize success? What should you change? What should you change it to?

You need to complete this important first step even before you formulate or update your security and compliance strategy.

Step 2: Then, clarify the objectives — the intermediate steps to achieve your goals.

Step 3: Clearly define the necessary and sufficient requirements for achieving those objectives.

Step 4: Identify the constraints, and determine the most significant constraint for achieving each objective.

Usually, five or fewer constraints really matter. These four steps (in the upper portion of Figure 3) include the groundwork to understand the problem — the scope and impact.

Step 5: Formulate a sound strategy with quality input.

Step 6: Execute your strategy with a well-defined program design and management.

Step 7: Have a basis for continual improvement and performance management.

If properly followed, these steps are an effective management approach for achieving PCI security compliance management success. The execution of this process can be facilitated with the Logical Thinking Process. (See the 2022 Payment Security Report, page 69.)

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)

5 — Strategy development and communication (focused allocation of resources)

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

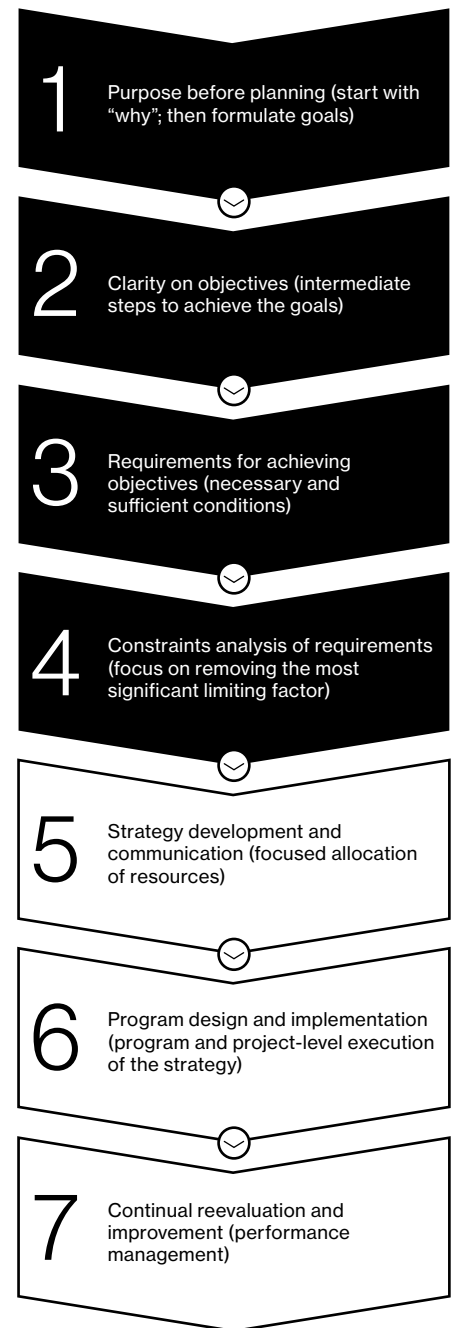7 — Continual reevaluation and improvement (performance management)

Figure 3. An effective approach for security program design, operation and evaluation

As Albert Einstein purportedly pointed out, "The significant problems we face cannot be solved at the same level of thinking we were at when we created them." To get different results—change! Do things differently.

The framework of this model is divided into seven distinct levels—from easy to impossible—across a spectrum of continual change (continual innovation) over increasing levels of difficulty.

The 7 levels of change[10]

To help assess levels of maturity and move programs forward, use this seven-step growth path for innovation and continual improvement:

Level 1: Effectiveness—doing the right things

Level 2: Efficiency—doing things right (with less waste)

Level 3: Improving—doing things better

Level 4: Cutting—cease doing things

Level 5: Copying—doing things other people are doing very well

Level 6: Different—doing things no one else is doing

Level 7: Impossible—doing things that "can't be done"

Each level is progressively more complex, more difficult to undertake, than the preceding level. The higher the level of change, the more time, resources and personal energy are required for implementation.

1. **Effectiveness:** Learn and consistently apply the basics of data security and compliance. Ask, "What are the right things to do?" and, "What needs to immediately change enough to become effective?" The Pareto principle[11] suggests that in most situations, 20% of what's being done actually yields 80% of the total payoff. To maximize effectiveness, energy must be shifted to and focused on doing that 20%.

2. **Efficiency:** This change requires a thorough understanding of all aspects of data security and compliance to identify and focus on doing very well those processes that have the most important impact and make the largest contribution. Level 2 changes are based largely on personally adjusting to new standards and procedures, and they involve coaching or explanations by others familiar with the job or business activity.

3. **Improving:** This involves thinking about ways to improve or fine-tune—speeding things up, shortening delivery time, increasing functionality and reducing downtime. It makes activities more effective, efficient, productive and value-adding.

4. **Cutting:** This involves analysis of core functions and applies the Pareto principle to cease doing things—cutting out the 80% of

activities that only yield 20% of the value. It focuses on eliminating waste. If performed systemically while keeping organizational interrelationships and subsystems in perspective, major organizationwide results can be achieved.

5. **Copying:** Level 5 marks the transition from incremental to fundamental change. Copying, learning from and reverse engineering can dramatically boost innovation at significantly lower costs than starting from scratch. Benchmarking how other organizations perform tasks and enhance their processes is the hallmark of a successful innovator.

6. **Different:** This change is about either doing something very different or very differently—and transitions into degrees of novelty that not only move an organization out of the box but also move it into areas where nobody else is doing it.

7. **Impossible:** Market constraints, resource limitations and/or organizational culture are too often seen as insurmountable barriers. As a result, discoveries at Level 7 frequently build on major mind shifts connected with exploratory thrusts into the unknown—bold, significant and long-term visions and change so different that it cannot be compared to anything else known at the time.

Source: 2019 Payment Security Report, page 29, and "The 7 Levels of Change: A Strategy for Creativity, Innovation and Continuous Improvement"

---

10 Adapted from "The 7 Levels of Change: A Strategy for Creativity, Innovation and Continuous Improvement," Rolf Smith, The School for Innovators, 1991. http://www.thinking-expedition.com/change7.html

11 "Understanding the Pareto Principle (The 80/20 Rule)," Better Explained. https://betterexplained.com/articles/understanding-the-pareto-principle-the-8020-rule

Integrating PCI security program evaluation frameworks

The lack of sustainable control environments is a top contributor to ineffective controls and data breaches. Sustainable security and compliance are achieved by demonstrating a consistent capability to maintain the ongoing operation where all required security controls meet the intent of their relevant control objectives. This capability prevents or minimizes future deviation from required performance standards. Organizations achieve sustainability by design: They build sustainability into the functional and operational specifications of the security compliance program and reinforce it through frequent education, training and awareness.

To address concerns relating to sustainability, the Verizon Payment Security Practice developed an integrated compliance management performance evaluation framework to serve as a navigational aid for organizations to enhance the clarity of their security compliance programs. Formally called the 9-5-4 Compliance Program Performance Evaluation Framework, it provides a new level of visibility and control to achieve repeatable, consistent and highly predictable outcomes.

The framework allows organizations to map, monitor and report the status of sustainability and effectiveness for each of the 9 Factors of Control Effectiveness and Sustainability across each of the essential 4 Lines of Assurance by evaluating the 7 Constraints of Organizational Proficiency. The 9 Factors, described on page 31, help organizations structure compliance programs and establish key success factors for evaluating security program management. (The framework was first published in the Verizon 2018 Payment Security Report,[12] pages 4 through 23, and updated in the 2019 Payment Security Report, pages 9 through 29.)
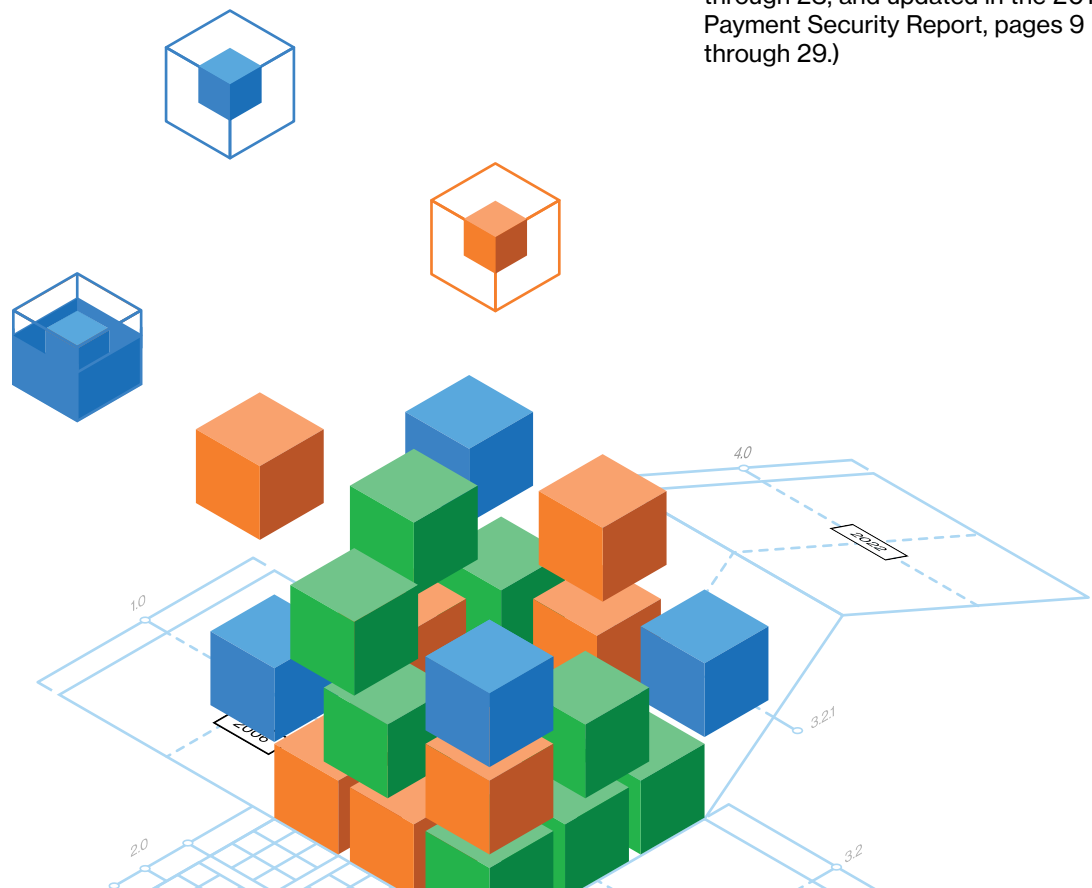
12   "2018 Payment Security Report," Verizon, 2018. https://www.verizon.com/business/resources/reports/payment-security/2018

The 4 Lines of Assurance

A theoretical assurance model that appeared in a position paper published by the Institute of Internal Auditors (IIA), "The Three Lines of Defense in Effective Risk Management and Control,"[13] received a fair amount of critique for its perceived oversimplification. An extended model called the Five Lines of Assurance[14] was proposed to correct these "deficiencies." In our opinion, Verizon's 4 Lines of Assurance model, which we developed specifically for the payment security environment, is a better fit.

In brief, assurance comes directly from work units: through the individual accountability of the front-line staff, operational management and directors— those responsible for delivering specific objectives or processes. This line is the function that owns and manages risks, and it is executing risk and control procedures to maintain adequate internal controls. While these workers may lack independence, the value is that the operational staff and management know the day-to-day challenges and are crucial in anticipating and managing operational risks. The decisions and actions occur between the front-line staff, who need to be held individually responsible as the first line of assurance. These individuals are responsible for delivering specific objectives or processes.

The next line of assurance comes with the risk management and compliance functions and responsibilities that monitor the implementation of policies and procedures and serve as the management oversight of the first line. The second line should remain engaged with the first line during the execution and evaluation of strategic and operational decisions.

The third line of assurance provides a level of objective, independent assurance and also timely information to the executive oversight committee or the board that the compliance and risk management and internal control framework is working as designed, with reasonable (not absolute) assurance of the overall effectiveness of governance, risk management and controls.

Some organizations prefer to separate internal auditing and internal assessors from the second line and place them in the third line. The role of internal auditing, assessors, and the board or executive oversight committee is largely detection and correction, i.e., detecting control weaknesses or breakdowns and suggesting improvements or remedial action.

Then in the fourth line are the regulators and other external bodies, outsourced security professionals, external assessors, and auditors that provide input and assurance on the effectiveness of governance, risk management and internal controls. They should evaluate how the first three lines of assurance achieve control objectives. External assessors can provide comprehensive assurance based on a high level of independence and objectivity because they reside outside the organization's structure, and they are usually trained to objectively interpret compliance requirements.

For more details on the degree of collaboration needed across the organization, we reviewed the 4 Lines of Assurance model in the 2018 Payment Security Report (page 15) and how assurance should come directly from work units: the front-line staff, operational management and directors.

13 "The Three Lines of Defense in Effective Risk Management and Control," Institute of Internal Auditors, January 2013. https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf

14 "The Handbook of Board Governance: A Comprehensive Guide for Public, Private, and Not-for-Profit Board Members," Chapter 17: "Three Lines of Defense versus Five Lines of Assurance: Elevating the Role of the Board and CEO in Risk Governance," first edition, Tim J. Leech and Lauren C. Hanlon, Wiley & Sons, 2016.

The 7 Constraints of Organizational Proficiency

The ongoing identification and management of constraints—factors standing in the way of positive change—is a very important activity for the management and improvement of any PCI security program.

The table below presents a categorized list of primary constraints that Verizon introduced and refined over the past decade. These are the 7 Cs that organizations need to navigate to improve the performance of their PCI security programs: capacity, cost, competence, capability, culture, communication and commitment.

These are common constraints preventing organizations from developing the process and capability maturities needed to achieve a sustainable and effective control environment that operates with consistent performance and predictable outputs. It's certainly not an exhaustive list, but rather it's a useful frame or mental model that can facilitate categorization of limitations and restrictions within the control environment. (For additional information, the 7 Cs are published in the 2022 Payment Security Report, page 68.)

These constraints can be categorized into three top-level domains—resources, production and work culture—each with several constraints that negatively affect performance:

- **Resources:** What you have to work with

- **Production:** How you apply resources to achieve objectives and goals

- **Culture:** The conditions under which the work is done, how performance is measured, incentives and how employees respond to their work environment

#	Constraint		Description
1	Capacity	⇄	Limitations on the amount of resources that can be allocated to security and compliance
2	Cost	$	The amount of time and money allocated and required to achieve objectives and goals
3	Competence		The level of experience and skill at an individual level to support security and compliance
4	Capability		The level of proficiency at team and organization levels—what people can achieve collectively
5	Culture		The sum of an organization's attitudes, actions and behaviors toward security and compliance
6	Communication		The frequency and quality with which stakeholders exchange information
7	Commitment		The pledge from stakeholders to undertake the actions needed to achieve the security goals

Resource capacity	The amount of resources to apply toward objectives and goals					
	Time/attention	Cost/budget	People	Tools/technology	Processes/techniques	Energy
Production abilities	The throughput of resources to plan, design, implement, operate, improve, manage, monitor and evaluate inputs, processes and outputs					
	Competency			Capability		
	The availability and application of knowledge, skills and experience from individual people to tasks and activities (efficiency and effectiveness)			The integrated application of resources in workstreams/processes and the collective ability of teams/business units to produce required output		
Work culture	The attitudes, behaviors, knowledge, norms and customs of employees in the workplace					
	Communication		Compliance		Commitment	
	Communication methods and quality Communication frequency		Internal policies, standards, procedures External regulations and legislation		Commitment to goals and requirements Commitment to continual improvement (maturity)	

Figure 4. An integrated view of the common constraints that limit organizational proficiency and performance of PCI security programs

Integrated program performance evaluation

An integrated program performance evaluation framework

The Verizon Security Compliance Program Performance Evaluation Framework integrates and presents the various elements to help develop and improve capability and process maturity across the control environment. If any of the 9 Factors are significantly deficient or missing from a security program, the program likely will fail to achieve a sustainable level of process maturity. We also pinpoint the typical constraints that limit the performance and achievement of control objectives across the 4 Lines of Assurance.

The 9 Factors of Control Effectiveness and Sustainability	1. Control environment 2. Control design 3. Control risk 4. Control robustness 5. Control resilience 6. Control life-cycle management 7. Performance management 8. Maturity measurement 9. Self-assessment
The 7 Constraints of Organizational Proficiency	1. Capacity 2. Cost 3. Competence 4. Capability 5. Culture 6. Communication 7. Commitment
The 4 Lines of Assurance	1. Front-line staff 2. Compliance and risk management teams 3. Internal audit, assessors, executive oversight 4. Regulators, external audit, external professionals

Verizon's unique security program evaluation framework allows for a highly structured, repeatable and consistent method to map, monitor and report the status of sustainability and effectiveness for each of the 9 Factors of Control Effectiveness and Sustainability across each of the essential 4 Lines of Assurance by evaluating the 7 Constraints of Organizational Proficiency. This mapping presents 63 control points across each of the 4 Lines of Assurance—252 metrics (control points) in total per assessed environment.

Evaluation questions to consider

- Is your organization's compliance program well-designed?

- Is your program being managed effectively?

- Does your compliance program work in practice?

- How sustainable is your control environment?

- Do you know how to pinpoint your program's constraints and deficiencies?

Security control sustainability evaluation

Sustainability factor		Capacity	Cost	Competence	Capability	Culture	Communication	Commitment
1	Control environment	?	X	✓	?	X	X	X
2	Control design	✓	✓	X	X	✓	✓	✓
3	Control risk	✓	✓	X	✓	✓	X	✓
4	Control reliability and robustness	✓	✓	X	✓	✓	✓	✓
5	Control resilience	✓	✓	?	X	✓	✓	✓
6	Control life-cycle management	✓	✓	✓	✓	✓	✓	✓
7	Performance management	✓	✓	X	?	✓	✓	?
8	Maturity measurement	✓	✓	✓	✓	✓	✓	✓
9	Self-assessment	?	✓	X	?	✓	✓	✓

Evaluate, report on and track each of the 9 Factors of Control Effectiveness and Sustainability and 7 Constraints of Organizational Proficiency across each of the 4 Lines of Assurance.

4 Lines of Assurance

1. **Front-line staff, individual accountability**

2. **Compliance and risk management teams**

3. **Internal audit and management**

4. **External audit, regulators**

Legend

✓ = In place

X = Deficient/conflict

? = To be determined/unsure

At many organizations, the front-line staff (first line of assurance) outsource a significant portion of their compliance responsibilities to the second line of assurance, relying on the function of the risk, security and compliance teams for everyday compliance-related business and control decisions. In organizations with more mature capabilities, all lines of assurance are involved in supporting the security program. When roles and responsibilities are appropriately defined, duplication of work and fragmentation of effort are avoided. There is real value in having a strong first line of defense handling everyday business and in-line control activities. (For more details about the 4 Lines of Assurance, see the 2018 Payment Security Report, page 15.)

An overview of the 9 Factors of Control Effectiveness and Sustainability

The relationship between the 9 Factors and the sustainable performance of PCI security requirements can be summarized as follows:

1. The sustainability and effectiveness of the 12 PCI DSS Key Requirements depend on a healthy control environment (Factor 1).

2. Proper control operation to meet PCI DSS security control objectives depends on sound control design (Factor 2).

3. Without ongoing maintenance (security testing, risk management, etc.), controls can degrade over time and eventually break down. Mitigation of control failures requires integrated management of control risk (Factor 3).

4. Controls operate in dynamic business and ever-changing threat environments. They must be robust (Factor 4) to resist unwanted change to remain functional and perform to specifications (configuration standards, access control, system hardening, etc.).

5. Security controls can potentially still fail, despite adding layers of control for increased robustness; therefore, control resilience with proactive discovery and quick recovery from failure is essential for effectiveness and sustainability (Factor 5).

6. To achieve all of the above, it's necessary to monitor and actively manage security controls throughout each stage of their life cycle (Factor 6) from inception to retirement.

7. Establishing and communicating performance standards to measure the actual performance of the control environment (Factor 7) improves control effectiveness and promotes predictable outcomes of your data protection and compliance activities, allowing for early identification and correction of performance deviations.

8. A control environment should never be stagnant—it must improve continually. To accomplish this, you need a road map—a target level of process and capability maturity (Factor 8) to track the degree of formality and optimization of processes as an indicator of how close developing processes are to being complete and capable of continual improvement.

9. Achieving all of the above requires in-house proficiency—resource capacity (people, processes and technology), capability (supporting processes), competency (skills, knowledge and experience) and commitment (the will to consistently adhere to compliance requirements). In short, it requires a self-assessment proficiency (Factor 9).

Benefits of the compliance program performance evaluation framework

This program evaluation framework and associated integrated evaluation processes present a simplified and structured approach to:

- **Precision:** Provides a detailed and exact focus on each of the core components to measure the sustainability and effectiveness of a security program; allows for precise tailoring of the controls and up-front measurement of control effectiveness

- **Clarity:** Asks the right questions, corrects program scope, drives strategic outcomes, clarifies objectives

- **Identification of constraints:** Affects control performance and data protection effectiveness and sustainability to pinpoint deficiencies in the design and operation of a program

- **Measurability:** Presents a comprehensive, integrated set of metrics; useful for identifying blind spots and supplying critical input to define and monitor the internal and external control environment

- **Connectivity:** Provides a high degree of transparency and visibility into the value of compliance investments by tying processes, constraints and outcomes together

- **Scalability:** Allows for the incremental development of maturity; increases capability and process maturity as the capacity and other resources become available

- **Flexibility:** Complements other frameworks; enables organizations to measure control effectiveness and use this data to precisely tailor controls and operating procedures across the environment

4.0
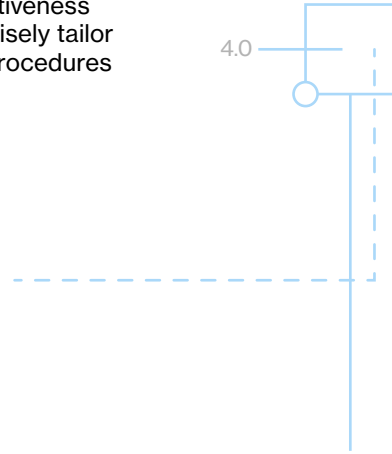
Evaluating control effectiveness

CISOs can't be confident that their organization's security compliance program is satisfactory unless they can produce verification of the effectiveness of all the control requirements and the overall compliance environment. Frequent measurement, reporting and evaluation of the effectiveness of controls and the overall control environment are essential to integrate into all PCI security program objectives.

Compliance with PCI DSS requires an ongoing investment of resources—money, time and attention from teams of people; ongoing technology costs; and compliance validation assessment and reporting fees. After 20 years of global compliance regulation, the value of PCI DSS compliance is firmly understood: It's a starting point of minimum baseline security measures to secure payment card data against compromise, as opposed to compliance for the sake of compliance (checkbox).

A basic but essential question to ask and answer at least once a year is, "How effective is the implementation of our PCI DSS program to secure our payment card data?" Effectiveness can generally be defined as doing the right things to achieve the right outcomes—as opposed to efficiency, which is doing things better with less waste. The efficiency with which a PCI security control environment is operated has direct and indirect impacts on the effectiveness of the environment and the controls within the environment.

Implementation of PCI DSS requirements involves two interdependent aspects: effectiveness and correctness. While controls may satisfy correctness criteria (compliance), they may fail to meet effectiveness criteria (actual security), particularly under unanticipated conditions. Effective controls need to meet a resilience standard when carrying out their intended functions and withstand environmental changes in system operations as well as attacks. (See the Verizon 2017 Payment Security Report, page 9.[15])

15   "2017 Payment Security Report," Verizon, 2017. https://www.verizon.com/business/resources/reports/2017-payment-security-report-en.pdf
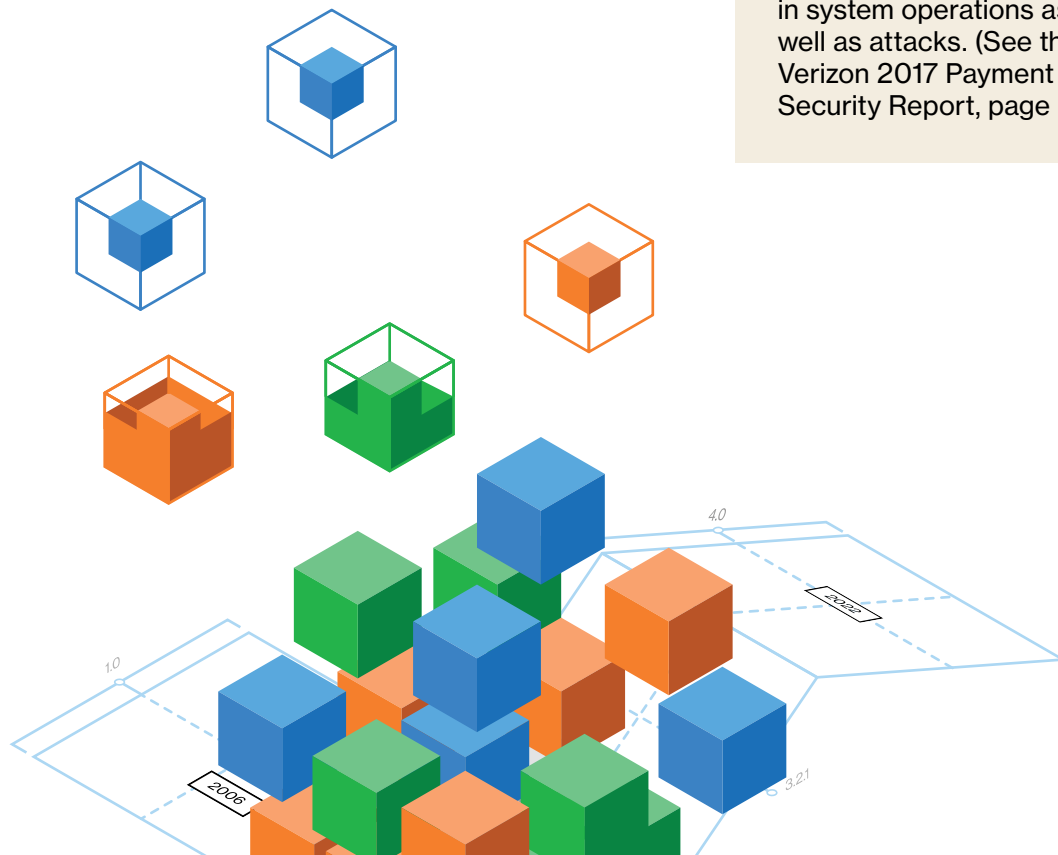
The answer to that question is complex since effectiveness depends on multiple factors. It's seldom, if ever, that merely the basic implementation of PCI DSS controls results in effective payment card data security. In reality, you are asking how effective your overall control environment is—its ability to achieve the right outcomes given the structure, design and performance of the system components within the environment. One question usually leads to more specific questions, such as, "Just how effective is PCI DSS at preventing payment card data from being compromised, and is this achievable upon completion of the implementation of all applicable PCI DSS controls?"

Several security teams choose to answer the question by not merely reporting the PCI DSS scope and coverage of PCI DSS controls that are in place but also tracking and reporting the failure rate—the frequency of errors or performance deviations. In other words, how often do the PCI DSS controls break down? In addition to failure rate, organizations with slightly higher evaluation maturity also measure and report the duration that controls were not in place. While this is a good practice that more organizations should embrace, it's still a reactive measure that likely may not address the underlying reasons for poor control performance.

4.0

0.7

Data breach vs. compliance validation correlation

In several previous editions, we compared organizations that validated their PCI DSS compliance against organizations that experienced confirmed payment card data breaches after they either validated their PCI DSS compliance but did not keep their controls in place or never validated their PCI DSS compliance (see the 2019 Payment Security Report, page 32).

The results of the comparison remain consistent year after year. To date, we are not aware of any disclosed public records of any organization experiencing a confirmed payment card data

breach that validated its PCI DSS compliance and was found to be in full compliance with the requirements at the time of the breach.

That said, many organizations that did not suffer payment card data breaches usually also implemented security measures that go beyond the PCI DSS baseline set of requirements. They understand the limitations of the PCI DSS and the need to complement and supplement it by implementing and adhering to additional industry governance, risk management and other compliance standards and frameworks.
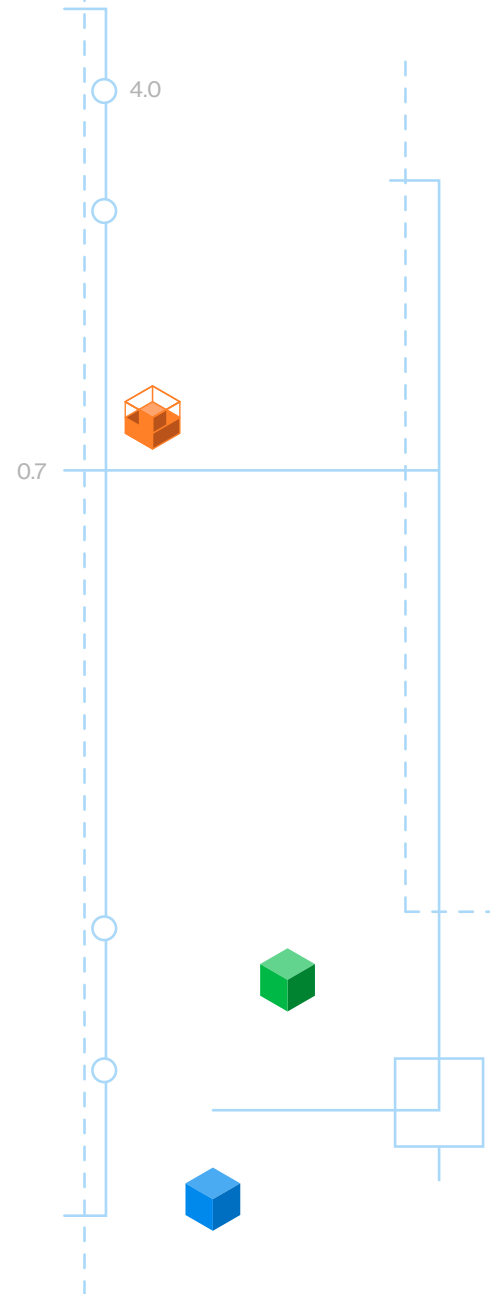
The question about effectiveness should address sustainable compliance and control strength—specifically, by asking additional questions, such as:

- How do we know that we have done enough to ensure that our data is sufficiently secured now and in the foreseeable future?

- Is PCI DSS by itself sufficient to secure payment card data against compromise?

- What else needs to be done to develop and maintain the conditions needed for each control within the various control systems to function as intended without deviation over long periods?

It does not take much thought to understand that it's not merely the presence of PCI DSS controls but instead how each control is designed, implemented, operated and maintained throughout its life cycle as an integrated security control system across the control environment. Verizon's research suggests that these factors mostly determine the effectiveness of controls and the control environment.

"

Security breaches and data compromises occur either because a control is missing (i.e., not in place; inactive/not operational) or the control was operating as designed but was knowingly or unknowingly ineffective."[16]
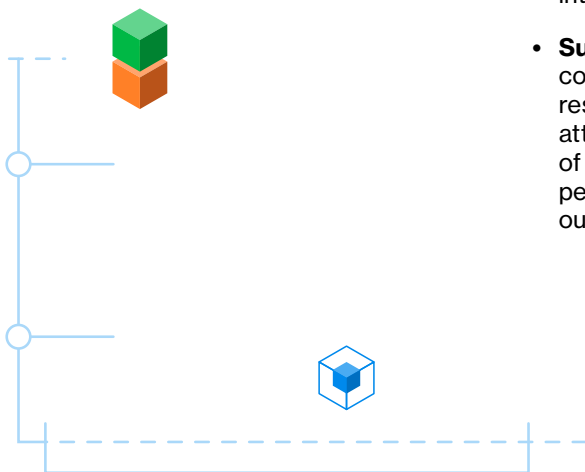
Verizon 2016 Payment Security Report, page 8

The true level of effectiveness of any control is based on the capability of the organization to achieve the functional and operational integration of several combined critical factors:

- **Design:** Successful design of effective controls and control environments (fully integrating control risk, robustness, resilience and evaluation)

- **Implementation:** Applying the controls correctly (effectively) across technology, processes, people

- **Maintenance:** Maintaining the controls to keep them operating and functioning as intended to be effective

- **Sustainability:** Ensuring that the control environment is capable (with resources, supporting processes, attention from people, technology) of sustaining the required level of performance (inputs, processing and outputs, level of throughput)

- **Risk management:** Confirming that the risks to payment card data are sufficiently and consistently mitigated so there is a reasonable degree of assurance that:

  - Existing vulnerabilities within the control environment are identified, mitigated or removed

  - New vulnerabilities are rapidly detected, identified and remediated in a consistent and timely manner (proficiency)

  - Threat actors are prevented from obtaining access to and exfiltrating payment card data (See the 2016 Payment Security Report, page 8, "The data breach chain.")

Effectiveness is not absolute. It's more useful to express the degree of effectiveness in terms of level of assurance. (See the 2017 Payment Security Report, page 11.)

---

16 "2016 Payment Security Report," Verizon, 2016. https://www.verizon.com/business/resources/reports/2016-verizon-psr-mainreport.pdf

To properly answer the question of security control effectiveness, it's evident that you need the ability (reliable methods) to identify, collect, measure, report and explain these performance areas as an integrated set of metrics that provide perspective on effectiveness, efficiency and sustainability of the control environment. It requires proper attention to every step of the security control life cycle. For example, a clear, documented expression of:

- The initiation/conception of each security requirement (control system) — its purpose or reason to exist and scope

- Which risks (threats, vulnerabilities and assets) the control is intended to mitigate and how the design of each control supports its robustness (withstands unwanted change) and resilience (recovers from unwanted influence/change)

- How well control design and operation meet the prescribed level of performance when measured against relevant industry standards, etc.

See the 2023 Payment Security Report insights white paper, pages 24 and 25, for the complete security control life cycle.

Evaluate PCI security programs with a systems-view perspective

It's important to remember that PCI security controls function as systems.

A systems thinking theory addresses the dynamics of a system where there is an underlying order. Small changes can cause complex alterations in the overall system. By applying a method that focuses on the entire system — its goals, requirements and constraints — organizations can identify solutions that address multiple problems. (See the 2022 Payment Security Report, pages 9 and 71.)

You will be hard-pressed to find a single PCI DSS security control anywhere across the standard that can achieve its intended control objective independently, in isolation by itself. Every control requires the functional operation of several other controls to achieve its intended function and output. A breakdown in one control will negatively affect the performance of at least one other control — but more likely will affect a series of other connected and interconnected controls.

The level of integration of controls across the control environment is a process that requires a lot of time — in most cases, it needs years of work to complete, not months, and remains an ongoing process that never ends.

To help facilitate this journey of control design and evaluation, it helps to have proven methods, models and frameworks that enable you to measure, evaluate, report and explain fundamental and critical elements of the security control environment. Presenting the effectiveness and sustainability of each environment in a visual way obviates which areas need attention. It provides a high-level perspective on the overall condition of each environment.

"

Goals are about the results you want to achieve. Systems are about the processes that lead to those results."[17]

James Clear

17   Excerpt from ATOMIC HABITS: AN EASY & PROVEN WAY TO BUILD GOOD HABITS & BREAK BAD ONES by James Clear, copyright © 2018 by James Clear. Used by permission of Avery, an imprint of Penguin Publishing Group, a division of Penguin Random House LLC. All rights reserved.

PCI DSS control systems

Each PCI DSS control operates as part of a control system—without exception. Therefore, the effectiveness of controls should be evaluated in the context of their applicable control systems. Often when failures occur, it's because controls aren't properly evaluated for robustness and resilience in the context of their dependent and interdependent controls within its control system or other connected control systems. In addition, they often lack sufficient operational support from a sustainable environment and, therefore, may be substantially less effective.

A method for measuring control effectiveness

> 💡 **Control effectiveness and control performance should be measured at various stages of the control life cycle. (See the 2023 insights white paper, page 25, for more details on the security control life cycle.)**

Many organizations erroneously assume that PCI DSS controls can be implemented right out of the box and expect them to be effective by default without the need for evaluation and careful tailoring. In addition, it is observed that formal payment security assessment training by the PCI SSC and other training providers usually does not include specific instruction and thorough guidance on how to measure control effectiveness and performance.[18],[19]

The control specifications included in the PCI DSS are not defined in detail at all. They are fairly vague and described in broad, general terms. When controls are not properly interpreted, analyzed, documented and tested for application to their unique environment, it can result in misplaced trust and a false sense of security. That happens when you rely on controls that seem to function as intended but contain a flaw in design, implementation or operation—or all three.

You cannot evaluate overall control effectiveness without also measuring its contribution toward risk mitigation. Controls should only be considered effective when their contribution to their control system and control environment mitigate risk to an acceptable level.

> 💡 **Recommended reading:** The 2017 Payment Security Report, page 12

---

18 Verizon published guidance on control effectiveness in the Verizon 2018 Payment Security Report, page 42, which referenced the DIME model.

19 Additional guidance on efficiency and effectiveness measures is described in the PCI SSC Information Supplement "Best Practices for Maintaining PCI DSS Compliance," released by the PCI SSC in January 2019 and available here: https://listings.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

Example of how to measure control effectiveness

An example of applying the DIME model "Design, Implementation, Monitoring, Evaluation" for scoring the effectiveness of security controls in four steps:

- **Measuring control design:** How well it should work in theory

- **Measuring control implementation:** How well it actually performs in practice

- **Measuring control monitoring:** How we know that it's still working

- **Measuring control evaluation:** How frequently we evaluate effectiveness and efficiency

NOTE: If either design or implementation is zero, then the total score becomes zero.

Control effectiveness guide

Fully effective	Nothing more needs to be done except reviewing and monitoring the existing controls.
Substantially effective	Most controls are designed correctly, but more work needs to be done on design and control validation.
Partially effective	Some controls are designed correctly and operate effectively, but many need work to ensure that they address root causes and/or contributing factors.
Largely ineffective	Significant control gaps exist, or controls do not operate effectively at all.
Totally ineffective	Management has no confidence that any degree of control is being achieved.

The program evaluation methods reviewed in this publication can be used to inform qualitative and quantitative assessments of relative data security. For a rigorous evaluation of data security compliance management, a large number of quantitative and qualitative variables need to be assessed. However, for a basic judgment on what kind of security program an organization has and aspires to develop, the Payment Security Report distills down the essential elements and core capabilities that should suffice for any organization to evaluate its PCI security program.

Scoring			
1	**Measuring control design:** How well it should work, in theory, if it's always applied in the way intended		
Control is very limited or badly designed, even where used correctly; provides little/no protection.	Control is designed to reduce some areas of risk.	Control is designed to reduce most aspects of risk.	Control is designed to reduce risk aspect entirely.
0	1	2	3
2	**Measuring control implementation:** The way the control performs in practice		
Control is not applied or applied incorrectly.	Control is sometimes correctly applied.	Control is generally operational but on occasion is not applied as intended.	Control is always applied as intended.
0	1	2	3
3	**Measuring control monitoring:** How we know that the control is continuing to operate		
Operation is not monitored at all.	Operation is monitored on an ad-hoc basis.	Operation is usually monitored but not always.	Operation is always monitored.
0	1	2	3
4	**Measuring control evaluation:** How frequently control effectiveness/efficiency is evaluated		
Control is never evaluated.	Control is evaluated very infrequently.	Control is occasionally evaluated for effectiveness/efficiency.	Control is regularly evaluated for effectiveness/efficiency.
0	1	2	3
5	**Scoring control effectiveness (no weighting)** Apply DIME.		
Design 2 (out of 3)	Implementation 3 (out of 3)	Monitoring 3 (out of 3)	Evaluation 1 (out of 3)
Total = 9/12 = 75% total effectiveness			

Figure 5: Measuring control effectiveness[20]

20 Originally presented by Dr. John Mitchell, LHS Business Control, "Measuring Control Effectiveness – GRC 2.0 – Breaking Down The Silos," ISACA Ireland Conference, October 3, 2014.

Evaluating program maturity

The maturity of a compliance program provides a window into how serious an organization is about protecting data. How much an organization invests in the improvement of data protection capabilities and progress toward optimized processes can be a barometer for security success. (See the 2019 Payment Security Report, page 19.)

Successful, continual compliance improvement and sustainability seldom, if ever, diverge from a systematic, step-by-step approach. In the words of management expert Peter Drucker, "The most efficient way to produce anything is to bring together under one management as many as possible of the activities needed to turn out the product."[21]

Proper design and evaluation of a data security compliance program are critical to its overall success. Getting it right the first time will save you time, money and the sanity of your workplace, but it requires considerable clarity and commitment to doing the right things right, which depends on:

- How well the program is structured

- What and which outcomes are focused on

- The assignment of resources and priorities

"

Small changes often appear to make no difference until you cross a critical threshold. The most powerful outcomes of any compounding process are delayed. You need to be patient."[22]

James Clear

Not defining program management success is a common program management design mistake. Defining success is vital to drive the program toward outcomes that will support control effectiveness and sustainability.

How is this best accomplished? Begin with the end in mind. Start your program by clearly defining the exact outcomes you want to achieve. At the end of your initial program development, you want an environment with well-defined visibility on program performance—both in terms of individual project performance and how predictable you can be in achieving your key milestones and overall program objectives.

Achieving clarity and predictability milestones is done by optimizing the in-house and acquired capacity, cost, capability, available competence, commitment and communication across all lines of assurance. Follow these steps for integrating maturity models into a PCI security program:

1. Clearly define and communicate the overall program goal and the intermediate objectives.

2. Map where you are in relation to the goal and objectives.

3. Identify and apply appropriate metrics and maturity models.

4. Encourage teams to actively participate in performance measurement and improvement.

5. Create a hypothesis narrative for how you might get to where you want to be.

6. Test, report and monitor your progress.

7. Adapt as needed, and repeat.

For an overview of the application of metrics and maturity models to enhance the process capability maturity of a PCI security program, see the 2019 Payment Security Report.

For more details, see Appendix B, "A deeper dive into PCI security performance measurement and evaluation," on page 97 of this publication.

---

21 "Management Cases, revised edition," Peter F. Drucker, 2009, reproduced with permission from the Drucker 1996 Literary Works Trust.
22 Excerpt from ATOMIC HABITS: AN EASY & PROVEN WAY TO BUILD GOOD HABITS & BREAK BAD ONES by James Clear, copyright © 2018 by James Clear. Used by permission of Avery, an imprint of Penguin Publishing Group, a division of Penguin Random House LLC. All rights reserved.

On measurement and maturity models

When projects or processes fail, it's tempting to blame faulty technology or human error. However, they will continue to fail when organizational processes and capabilities aren't mature enough to handle the scale or complexity of their requirements.

A mature organization efficiently and effectively adapts to change. Employees feel empowered to make job-related decisions following documented procedures. A mature organization is always working to improve process capabilities and usually is at the fourth or fifth level of maturity. Organizations with this level of maturity have streamlined processes in place to make continual, incremental improvements. This compliance reduces waste and discord.

On the other hand, an organization with low maturity won't have these processes in place. There is likely to be poor communication between team members and departments, and management will emphasize immediate results over long-term growth.

The role and value of process capability maturity models

An organizational maturity model is a framework for measuring process and capability maturity. Usually, these models divide maturity into levels or stages. Understanding their current organizational maturity is a good starting point for working toward higher maturity levels.

The application of maturity models to identify problem areas and measure success can benefit PCI security programs of any size or type of organization, from large financial organizations to small retailers. These models can be applied to individual departments within an organization. It is important to understand and communicate the role and application of a maturity model to improve security compliance management capabilities and processes. A maturity model serves as a measuring stick and an indicator of progress that can help to identify weaknesses in processes and capabilities. Measuring a PCI security program against the criteria of a maturity model can help to generate an improvement plan. The application of a maturity model, by itself, does not ensure organizational development and improvement. It does not execute a plan and fix deficiencies.[23]

Three important considerations

There are three important considerations about using maturity models to improve the processes and capabilities of a PCI security program.

- Models are meant to simplify the complexities of reality. Describing something as a model implies a degree of rigor or scientific method. Many maturity models don't have a sufficient, formal theoretical basis and are built on arbitrary decision-making and untested assumptions.

- The improvement of capabilities and processes is seldom the neat, linear progression depicted by most maturity models. The performance and output of PCI security programs tend to be subject to obstacles, detours and constraints that don't follow an ordered path. A good outcome is more likely to involve a nuanced blend of capabilities, sound program design and execution rather than an arbitrary level of maturity. People generally find it difficult to understand how the professional growth of individuals, teams and organizations actually fits into an easily digestible model.

- Maturity, or more specifically higher performance, doesn't have an end state. Defining a final state of maturity can be problematic. In the real world, any ideal state tends to vary according to circumstances. You may not even want to define a final state as it can undermine a drive toward continual improvement.[24]

23   Adapted from Project Management Institute Inc., Rosenstock, C., Johnston, R. S., & Anderson, L. M. (2000). "Maturity model implementation and use: a case study." Seminars & Symposium. https://www.pmi.org/learning/library/maturity-model-implementation-case-study-8882. Copyright and all rights reserved. Material from this publication has been reproduced with the permission of PMI.
24   The section "Three important considerations" is adapted from "The case against maturity models," Ben Morris, June 8, 2019. https://www.ben-morris.com/the-case-against-maturity-models

The origin of capability maturity models

The quality and process models of the 1970s and 1980s evolved into today's organizational maturity models and assessments. Many maturity models used today are rooted in the Capability Maturity Model (CMM), which was created for measuring software development capabilities, and the Carnegie Mellon Institute's Capability Maturity Model Integration (CMMI).

The five maturity levels are:

1. Initial

2. Repeatable

3. Defined

4. Managed

5. Optimizing

These stages map a possible path from enterprise mayhem to industry leadership. Most organizations are at the first two levels of maturity. Not every process capability needs to achieve the highest maturity level.

Integrating maturity models

Fixed progression in a maturity model can set the wrong motivation for the program team. Program participants may be encouraged to celebrate the achievement of maturity levels rather than focus on meaningful outcomes. It's not always obvious what tangible benefits maturity levels might have on the progression toward the achievement of the overall program goal. Instead, many organizations achieve success more quickly by focusing on incremental learning and improvement—following an agile philosophy in the design and execution of their PCI security programs. Maturity models and frameworks can be adapted to align with agile principles.

High organizational maturity means higher efficiency and effectiveness: better communication, alignment on goals and streamlined processes. Many challenges—or constraints—can prevent organizations from improving their maturity level. For information on methods for identifying and eliminating constraints, see page 68 in the 2022 Payment Security Report on the Logical Thinking Process.

> **Recommended reading:**
> "Risk Maturity Models: How to Assess Risk Management Effectiveness," Domenic Antonucci, 2016, Kogan Page.
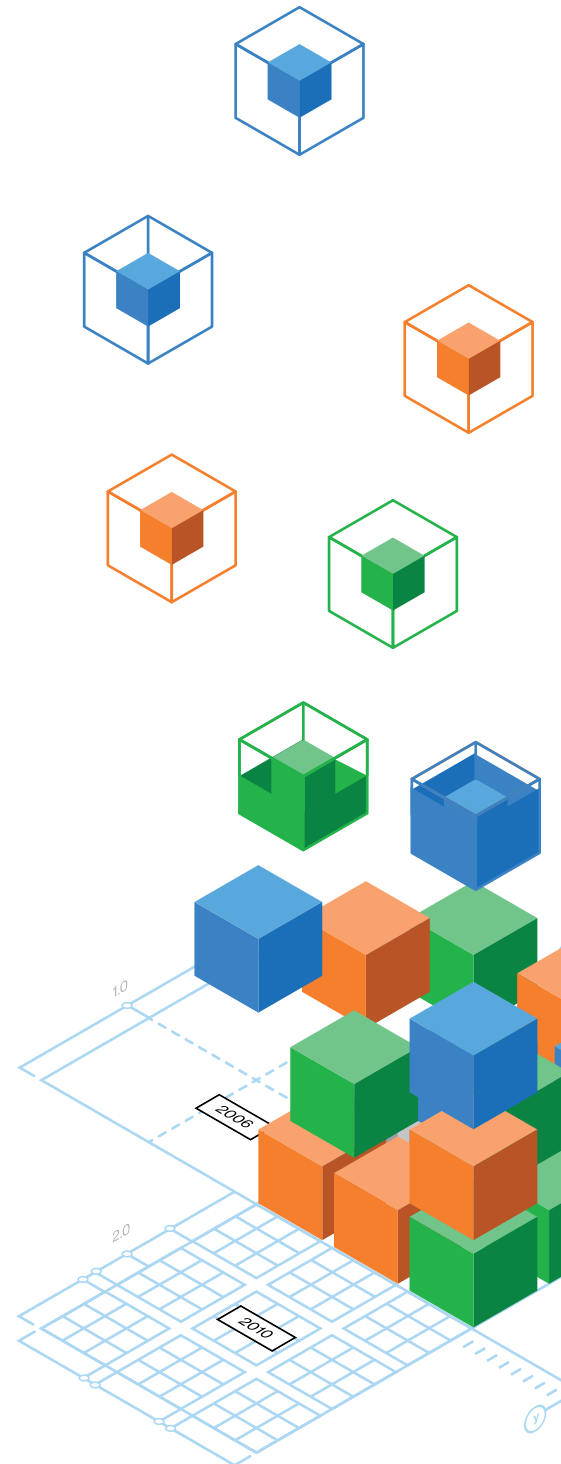
3 | State of compliance
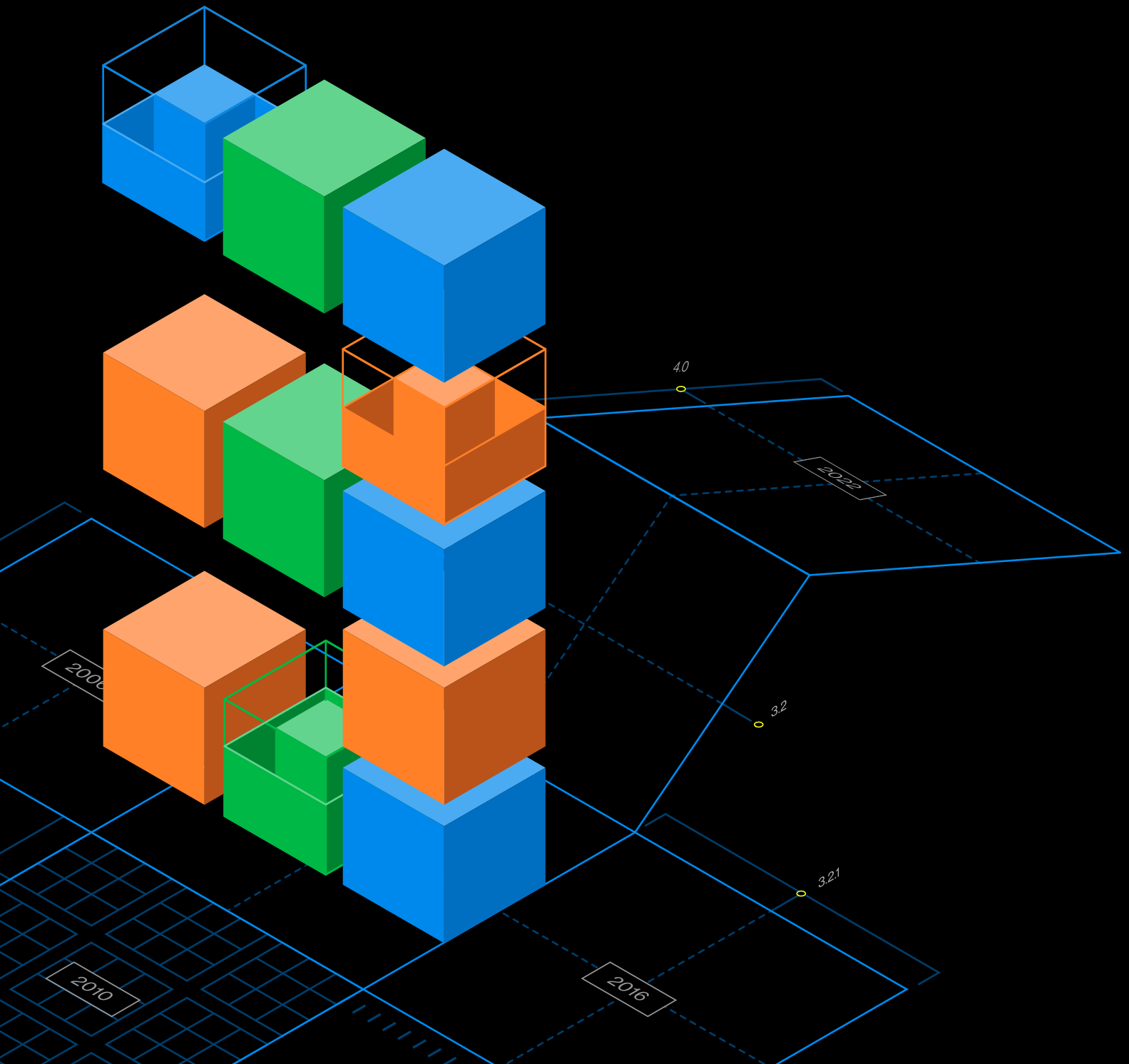
The state of PCI DSS compliance

Verizon published what is believed to be the first global analysis of PCI DSS assessments in 2010 and presented several groundbreaking short-, medium- and long-term trends in PCI DSS compliance. More than a decade later, these trends continue to reveal insightful payment security patterns, as well as specific compliance strengths and weaknesses, within each industry and geographic region. This section of the report pinpoints the best- and worst-performing requirements, with a breakdown ranging from high level—PCI DSS Key Requirements and base controls—down to granular details about which test procedures need the most attention.

PCI DSS v3.2.1 in review

PCI DSS v3.0 was the second major update of the PCI DSS. To date, PCI DSS v3.0 has been updated more times than any other major release version of the standard. PCI DSS v3.0 was released in November 2013 and updated to v3.1 in April 2015, with v3.2 following a year later (April 2016). The refinements in PCI DSS v3.2 added clarity and guidance to help organizations maintain data security standards in everyday business practices. For example, PCI DSS v3.2 added multifactor authentication (MFA) requirements and service provider scrutiny as well as an introduction to the Designated Entities Supplemental Validation (DESV) oversight program (Appendix A3). The v3.2 appendices helped organizations migrate from Secure Sockets Layer (SSL) to secure versions of Transport Layer Security (TLS).

With the release of PCI DSS version 3.2, the PCI SSC declared that this standard had reached maturity. Then, in May 2018, PCI DSS v3.2.1 was released and introduced relatively minor changes, such as clarification updates and a correction to previous requirements. After v3.2.1 went into effect on January 1, 2019, it remained in effect for more than five years until retired in March 2024—making it the longest-running version of the standard to date. Comparatively, PCI DSS v4.0, which has been the most significant update to the standard, went into effect March 2024 and will be retired on December 31, 2024, and replaced by PCI DSS v4.0.1 as the only active version of the standard supported by the PCI SSC.

The state of PCI DSS compliance: Key findings

Verizon measures compliance performance of PCI DSS requirements and controls on three metrics:

- Full compliance: The share of organizations achieving 100% PCI DSS compliance during an interim validation assessment

- Control gap: The gap between the measured state of compliance versus having 100% of required controls in place

- Use of compensating controls: The share of organizations that used one or more compensating controls

The performance of each metric was tracked over the lifetime of PCI DSS v3.x—from 2015 through 2023.

Full compliance trends

Bar chart showing full compliance percentages by year:
- 2015 DSS 3.0: 48.4%
- 2016 DSS 3.1: 55.4%
- 2017 DSS 3.1/3.2: 52.2%
- 2018 DSS 3.2: 36.7%
- 2019 DSS 3.2/3.2.1: 27.9%
- 2020 DSS 3.2.1: 43.4%
- 2021 DSS 3.2.1: 38.9%
- 2022 DSS 3.2.1: 32.4%
- 2023 DSS 3.2.1: 14.3%
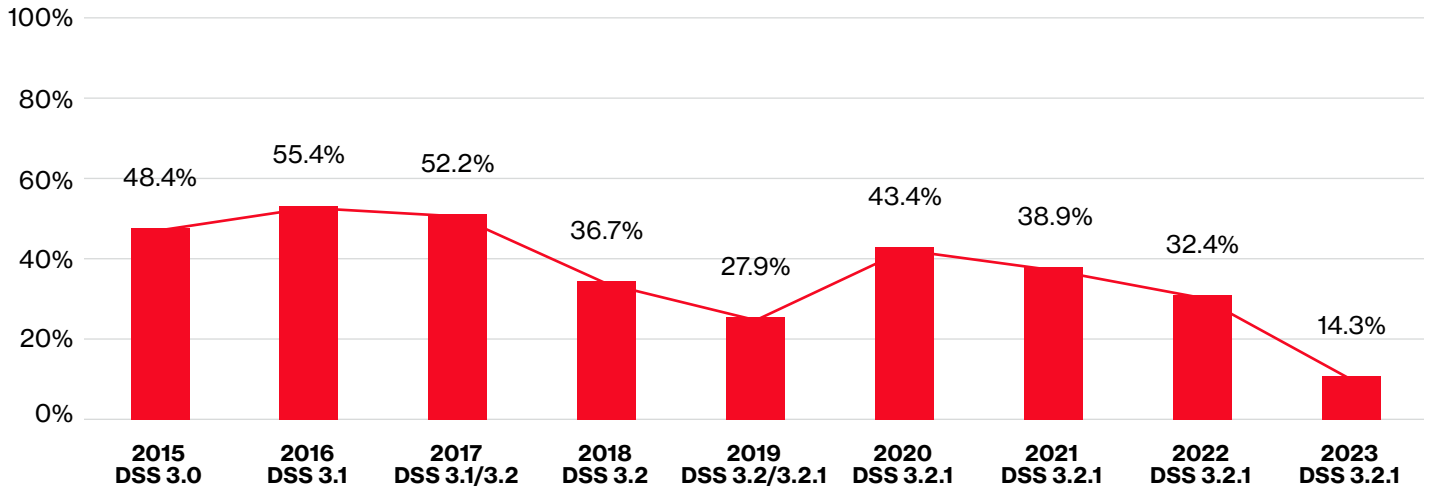
Full compliance (control sustainability)

The share of organizations achieving 100% PCI DSS compliance at interim validation is considered full compliance. This is a reasonable indicator of how well organizations within the dataset managed to sustain compliance by rapidly detecting and correcting controls that fell out of place and then demonstrating 100% compliance when tested prior to their formal annual validation. Nearly all organizations studied had passed a previous validation assessment.

The percentage of organizations maintaining full compliance has steadily declined since 2020. This is, in part, due to a reduction in assessment reports included in the aggregate dataset for 2021 and 2022, when assessments and compliance initiatives were affected by the consequences of the COVID-19 pandemic. Significantly fewer organizations achieved 100% compliance in 2023 compared to previous years. During the run-up to the 2024 PCI DSS v4.0 deadline, a likely contributing factor for the decline in full compliance in 2023 is the additional workload, time and attention the transition from v3.2.1 to v4.0 demanded from organizations. In many cases, control environments received increased scrutiny and attention to meet new requirements.
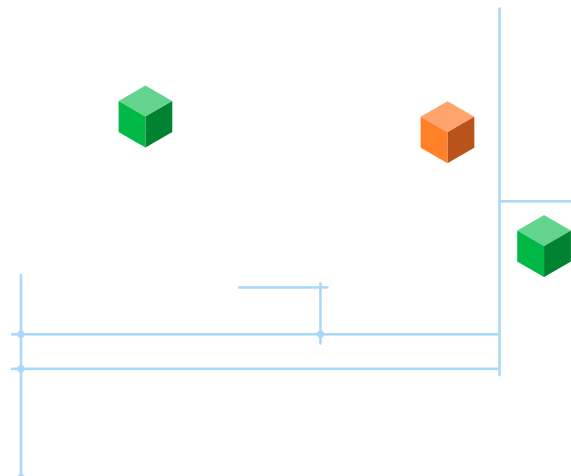
Control gap trends

	2015 DSS 3.0	2016 DSS 3.1	2017 DSS 3.1/3.2	2018 DSS 3.2	2019 DSS 3.2/3.2.1	2020 DSS 3.2.1	2021 DSS 3.2.1	2022 DSS 3.2.1	2023 DSS 3.2.1
	6.8%	5.8%	7.2%	7.2%	7.7%	4.0%	5.9%	3.2%	4.5%
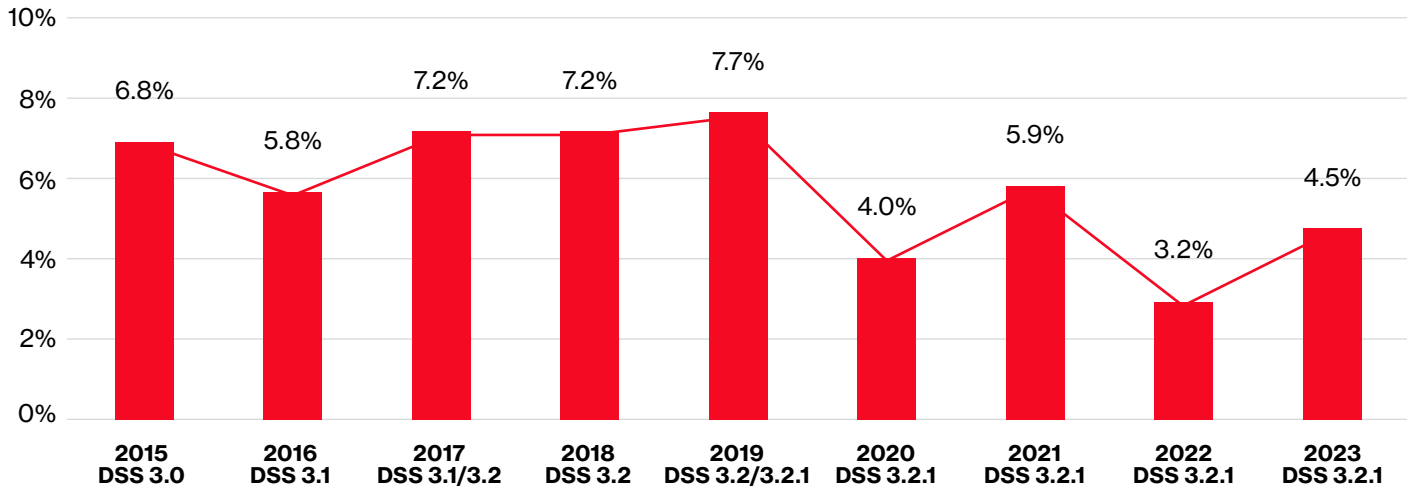
Control gap

The gap between the measured state of compliance versus having 100% of in-scope required controls in place when measured during an interim compliance validation assessment is called the control gap. In other words, the number of failed requirements divided by the total number of requirements expected.

This is an average figure that gives a measure of how far the assessed organizations were from full compliance. For clarity, a low gap is good, and a high gap is bad.

When measured across the PCI DSS (all 12 Key Requirements), the overall control gap remained consistently below 10%. Throughout the lifetime of PCI DSS v3.x, it fluctuated, with a high of 7.7% (PCI DSS v3.2.1 in 2019) to a lower (better) 4.5% gap in 2023.
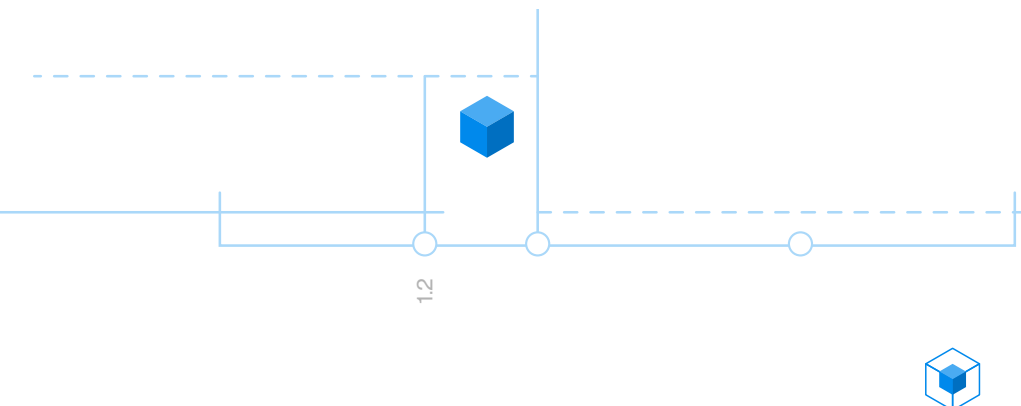
Compensating control trends

Year	Percentage
2015 DSS 3.0	37.5%
2016 DSS 3.1	30.2%
2017 DSS 3.1/3.2	41.8%
2018 DSS 3.2	20.6%
2019 DSS 3.2/3.2.1	24.7%
2020 DSS 3.2.1	30.1%
2021 DSS 3.2.1	22.2%
2022 DSS 3.2.1	17.6%
2023 DSS 3.2.1	25.4%
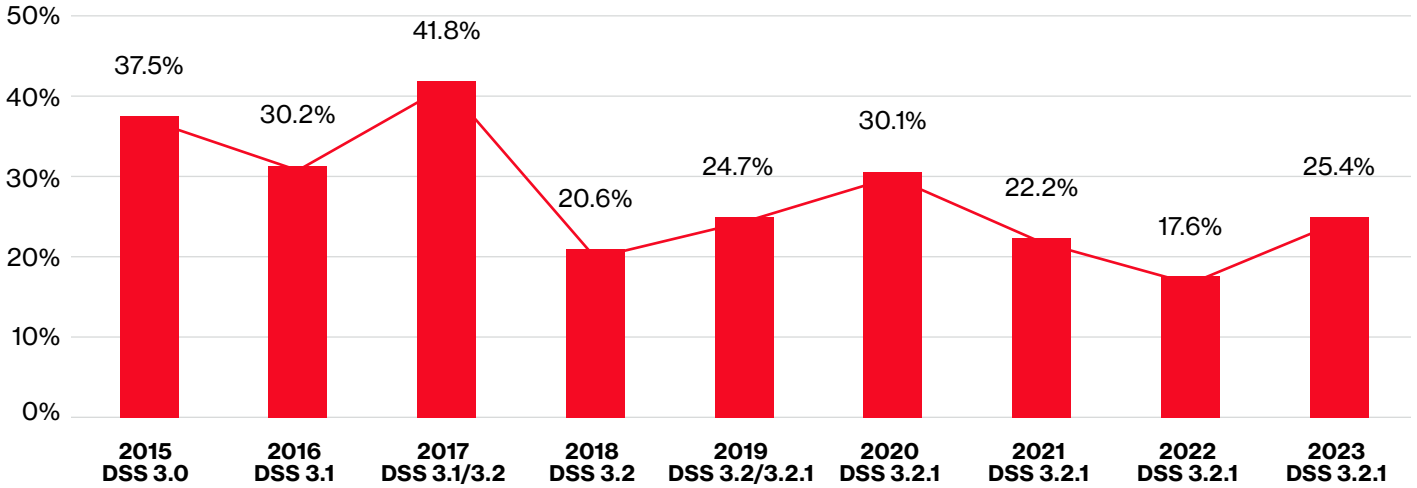
Compensating controls

This percentage indicates the share of organizations in our dataset that used one or more compensating controls when a legitimate technical or business constraint prevented them from meeting a requirement explicitly as stated in the PCI DSS.

This percentage is not an indication of the number of compensating controls used.

For most years during the lifetime of PCI DSS v3.2.1, approximately a quarter of organizations applied compensating controls to meet PCI DSS requirements.
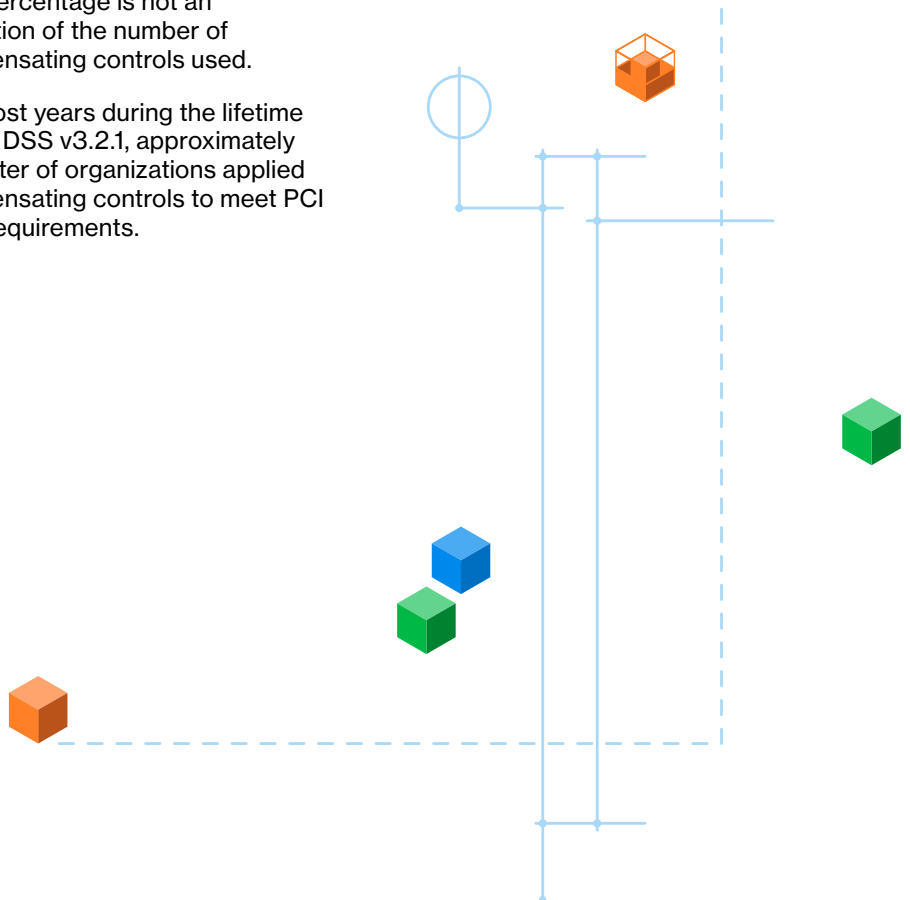
Long-term key requirement trend analysis

These trend graphs present an overview of the compliance performance across all PCI DSS requirements for all regions and industries across the globe for the 10-year period from 2014 through 2023.

Full compliance (control sustainability) trends: 2014 through 2023

Full compliance measures the percentage of organizations that achieve 100% compliance on a particular base control. It's determined by calculating the total number of organizations included in the dataset divided by the number of organizations that achieved full compliance for a particular requirement.

A 10-year analysis of the compliance sustainability of PCI DSS Key Requirements reveals interesting patterns of consistency. Figure 6 ranks the full compliance of PCI DSS validations by key requirement for assessments conducted from 2014 through 2023.

Full compliance										
PCI DSS	v2.0/3.0 2014	v3.0 2015	v3.1 2016	v3.1/3.2 2017	v3.2 2018	v3.2/3.2.1 2019	v3.2.1 2020	v3.2.1 2021	v3.2.1 2022	v3.2.1 2023
Position/ Rank	Key Requirement									
1	9	7	5	7	7	7	7	4	9	4
2	5	9	7	5	5	5	4	9	5	7
3	7	4	9	4	4	4	5	6	7	9
4	12	5	4	9	9	9	9	7	4	5
5	4	10	8	8	1	3	3	8	3	1
6	6	1	10	10	3	1	8	1	12	3
7	3	8	2	2	6	2	1	2	10	12
8	1	2	3	1	8	10	10	3	2	10
9	8	12	1	12	2	8	2	5	1	2
10	10	6	12	6	10	12	6	10	6	8
11	2	3	6	3	12	6	12	12	8	6
12	11	11	11	11	11	11	11	11	11	11

Rank position (most to least compliant)

Figure 6: Full compliance ranking—10-year trend analysis

It's fairly easy to spot the patterns, with the same key requirements appearing in similar ranking positions year after year. For example, Key Requirements 5 and 7 frequent the top two spots, and Requirement 11 is consistently the least compliant key requirement (at the bottom). Following Requirement 11, Requirements 6 and 12 are among the lowest-performing (least sustainable) key requirements.

Long-term control gap trends: 2014 through 2023

Control gap measures the percentage of controls found not in place and in need of remediation when checked during an interim compliance validation assessment. It's determined by calculating the failed controls and failed test procedures divided by the total number of controls assessed for all the related test procedures under a particular control.

Figure 7 indicates the ranking of the control gap of PCI DSS Key Requirements measured from PCI DSS assessments conducted from 2014 through 2023. For the majority of years, PCI DSS Key Requirements 5 and 9 nabbed the top spot (ranking position No. 1). These had the lowest control gap, i.e., the fewest number of controls not in place.

Key Requirement 11 appeared at the bottom with the largest control gap more times than any other key requirement. Outliers appearing in the 2021 data are mainly a result of a lower volume of data for the year compared to the aggregate data from the 10-year analysis. Several of the results for 2021 seemed skewed. For example, Requirement 6 took the top spot and Requirement 5 the bottom spot in 2021. Those are statistical outliers and data anomalies likely due to the low volume of data that affected the statistical validity. The results of the 2021 analysis therefore are not considered to be sufficiently reliable.

Control gap										
PCI DSS	v2.0/3.0 **2014**	v3.0 **2015**	v3.1 **2016**	v3.1/3.2 **2017**	v3.2 **2018**	v3.2/3.2.1 **2019**	v3.2.1 **2020**	v3.2.1 **2021**	v3.2.1 **2022**	v3.2.1 **2023**
Position/ Rank	Key Requirement									
1	5	9	5	7	9	9	4	6	9	9
2	9	7	9	5	12	3	3	4	5	3
3	12	4	8	8	1	7	9	3	12	4
4	4	6	6	9	6	1	6	8	6	7
5	6	1	7	1	5	5	2	9	3	5
6	7	8	12	6	7	6	7	12	4	1
7	1	10	1	10	4	8	1	7	2	8
8	8	3	10	12	8	4	8	10	10	12
9	10	2	2	2	10	10	12	2	7	6
10	2	12	3	3	2	2	5	1	1	10
11	3	5	11	11	3	12	10	11	8	2
12	11	11	4	11	11	11	11	5	11	11

Rank position (smallest to largest control gap; most to least compliant)

Figure 7: Control gap ranking—10-year trend analysis

Dataset

The data reported in this section is taken from draft (interim) ROCs. These are PCI DSS assessment reports that serve as a snapshot of an organization's PCI DSS state of compliance at a point in time prior to final assessment. These insightful interim reports capture lapses in controls that can occur as a result of poor compliance management practices or ineffective control design. (See pages 85 and 86 for additional details and our research methodology.)

A note about compliance and control sustainability

Compliance sustainability is the ability of organizations to design, implement and maintain robust and resilient control environments that meet regulatory requirements over extended periods. PCI DSS compliance is evaluated through point-in-time validations during interim and final compliance assessments. It presents a reasonable determination of the sustainability of PCI DSS controls by identifying how many controls remained in place throughout the annual validation period, evaluating organizational competence and commitment toward early detection and correction of significant control performance deviations.

Data security is an ongoing, 24/7 activity. For it to be effective, multiple layers (of processes, controls, people, systems) must work together in a series of control systems that make up the control environment. Organizations cannot allow any significant weaknesses to be present in the environment and expect sensitive data to be effectively protected. All control systems need to consistently meet their respective control objectives.

Drawing a distinction between general failures and the failure of control objectives is important. All organizations experience various forms of control failure throughout the year. Failures of individual controls at some point are largely inevitable—but they should be brief. Deviation from control standards (including defined processes and operational performance benchmarks) should be rapidly detected and corrected. In addition, failure of one or more controls should, in general, not result in a collapse of the entire system, just as the failure of one system (a set of interacting controls) should not result in the complete failure of control objectives nor of the entire environment.

This is the defense-in-depth principle: To maintain effective data security, control environments need sufficient robustness and resilience built in, even as temporary failures occur.
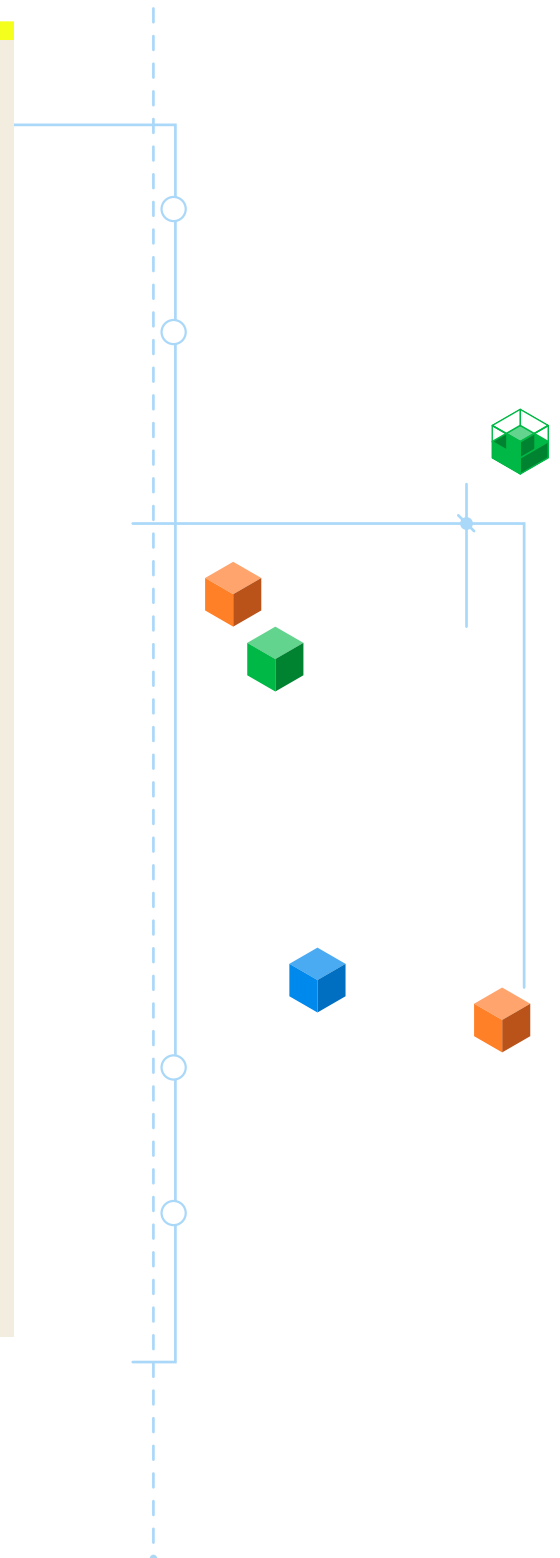
Compliance performance by PCI DSS Key Requirement

Requirement 1 – Install and maintain network security controls

Requirement 2 – Apply secure configurations to all system components

Requirement 3 – Protect stored account data

Requirement 4 – Protect cardholder data with strong cryptography during transmission

Requirement 5 – Protect all systems and networks from malicious software

Requirement 6 – Develop and maintain secure systems and software

Requirement 7 – Restrict access to system components and cardholder data by business "need to know"

Requirement 8 – Identify users and authenticate access to system components

Requirement 9 – Restrict physical access to cardholder data

Requirement 10 – Log and monitor all access to system components and cardholder data

Requirement 11 – Test security of systems and networks regularly

Requirement 12 – Support information security with organizational policies and programs

Full compliance			Control gap			Compensating controls		
Rank	**Key Requirement**	**2023**	**Rank**	**Key Requirement**	**2023**	**Rank**	**Key Requirement**	**2023**
1	Req. 4	90.5%	1	Req. 9	2.3%	1	Req. 2	0.0%
2	Req. 7	87.3%	2	Req. 3	2.4%	1	Req. 4	0.0%
3	Req. 9	85.7%	3	Req. 4	3.3%	1	Req. 7	0.0%
4	Req. 5	79.4%	4	Req. 7	3.4%	1	Req. 9	0.0%
5	Req. 1	74.6%	5	Req. 5	3.6%	1	Req. 12	0.0%
5	Req. 3	74.6%	6	Req. 1	3.7%	6	Req. 1	1.6%
7	Req. 12	63.5%	7	Req. 8	4.3%	6	Req. 3	1.6%
8	Req. 10	60.3%	8	Req. 12	5.0%	6	Req. 5	1.6%
9	Req. 2	58.7%	9	Req. 6	5.3%	9	Req. 10	3.2%
10	Req. 8	57.1%	10	Req. 10	5.4%	10	Req. 11	7.9%
11	Req. 6	52.4%	11	Req. 2	5.8%	11	Req. 8	9.5%
12	Req. 11	47.6%	12	Req. 11	9.1%	12	Req. 6	15.9%

Figure 8. PCI DSS v3.2.1 compliance by key requirement measured in 2023, ranked from most (green) to least (orange) compliant

Figure 8 presents a high-level snapshot of the state of compliance by measuring PCI DSS Key Requirement compliance performance in 2023 against the three key metrics: full compliance, control gap and compensating controls. The key requirements are ranked top to bottom from most to least compliant.

In 2023, PCI DSS Key Requirement 4 was the most sustainable, with 90.5% of organizations scoring 100% PCI DSS compliance at interim validation. Only 47.6% of assessments found Key Requirement 11 to be fully in place. Key Requirement 9 had the smallest control gap—only 2.3% of controls under this requirement were found to be not in place. Requirement 11 had the largest control gap, with 9.1% of controls not in place. 15.9% of organizations applied one or more compensating controls under Key Requirement 6. While higher use of compensating controls should not be viewed as a sign of increased noncompliance, it can increase the workload on design, maintenance and management of controls.

The goals, requirements and constraints of PCI DSS Key Requirements

The overall organizational goal of PCI security compliance can be defined as: 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, reliable and sustainable manner.

To support this overall goal, it's useful to also define the overall individual goal of each of the 12 PCI DSS Key Requirements within its proper operational context. A too-narrow definition and interpretation of the intended function and outcome of any PCI DSS Key Requirement is counterproductive. It can contribute to the failure to structure supporting project tasks and milestones and to secure the investment needed to pursue the achievement of effective, reliable and sustainable security controls.

2022 to 2023 PCI DSS v3.2.1 performance review: The tables on the following pages present the state of PCI DSS v3.2.1 compliance per requirement for each of the 12 Key Requirements for all organizations across the global dataset. The values for each PCI DSS control are expressed either as the percentage ("%": a fraction of 100 used to express a proportion or rate) of compliance or noncompliance or as a percentage point ("pp": the mathematical difference between two percentages) indicating the amount of change between two percentage rates.

The release of PCI DSS v4.0 and the new requirements it introduced has affected organizations across the globe. This state of compliance analysis presents an approximation of the global state of compliance across analyzed industries. Organizations can use this information to improve their goals, objectives and requirements and discover constraints for all in-scope requirements.

Requirement 1: Install and maintain network security controls

This requirement covers the correct use of security controls, such as firewalls and related components, to filter and monitor traffic as it passes between internal and external networks as well as traffic to and from sensitive areas within the organization's internal networks.

Requirement 1 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 1.

The goal: The goal of PCI DSS Key Requirement 1 is to maintain reliable and sustainable operation and management of network security controls across the in-scope environment, delivering consistent and effective network and application access control to and from the cardholder data environment (CDE) by restricting access to authorized users and systems only as well as to support ongoing monitoring and detection of security events and response to incidents. This goal also should include complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope: This goal applies to all people (internal and external) involved in the evaluation, implementation, operation and management of any in-scope network security component, i.e., all logical (IT) and physical security control components required to restrict network access to and from the CDE.

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.

Requirement 1

Full compliance ■ 2022 □ 2023

50%   60%   70%   80%   90% 100%

■ (red bar)	61.8%
□ (yellow bar)	74.6%

50%   60%   70%   80%   90% 100%

% of organizations maintaining full compliance

Full compliance improved from 61.8% in 2022 to 74.6% in 2023—ranking fifth in sustainability across the PCI DSS.

Control gap ■ 2022 □ 2023

0%   5%   10%   15%   20%

■ (red bar)	4.5%
□ (yellow bar)	3.7%

0%   5%   10%   15%   20%

% of controls not in place

The control gap improved from 4.5% in 2022 to 3.7% in 2023—ranking sixth overall across the PCI DSS.

Compensating controls ■ 2022 □ 2023

0%   5%   10%   15%   20%

■ (red bar)	0.0%
□ (yellow bar)	1.6%

0%   5%   10%   15%   20%

% of organizations using compensating controls

Only 1.6% of organizations applied one or more compensating controls under Requirement 1 in 2023. Only Requirement 1.1 was compensated.

Figure 9. Global state of PCI DSS compliance 2022 to 2023: Requirement 1

PCI DSS v3.2.1 Requirement 1 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
1.1	Implement firewall and router configurations.	62.9%	14.1pp	76.9%	5	7.1%	-2.2pp	4.9%	5
1.2	Restrict connections between CDE and untrusted networks.	91.4%	0.9pp	92.3%	3	3.2%	0.4pp	3.7%	4
1.3	Prohibit direct public access between internet and CDE.	91.4%	0.9pp	92.3%	3	1.9%	0.3pp	2.2%	1
1.4	Install personal firewall software.	91.4%	5.5pp	96.9%	1	4.3%	-2.0pp	2.3%	2
1.5	Document policies and procedures for managing firewalls.	97.1%	-0.2pp	96.9%	1	2.9%	0.2pp	3.1%	3

Figure 10. Requirement 1 control performance

Requirement 2: Apply secure configurations to all system components

This requirement covers the controls that reduce the available attack surface on system components by removing unnecessary services, functionality and user accounts as well as by changing nonsecure vendor default settings.

Requirement 2 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 2.

The goal: The goal of PCI DSS Key Requirement 2 is to develop, apply and maintain an effective, secure configuration management capability to all in-scope system components, reducing the means available to threat actors to ensure that the CDE is not susceptible to attack. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope: This goal applies to all in-scope system components, i.e., all applicable hardware and software applications, including wireless network components and components hosted in cloud environments; individuals and teams responsible for implementing and maintaining security configurations; and third parties that support IT system components.

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
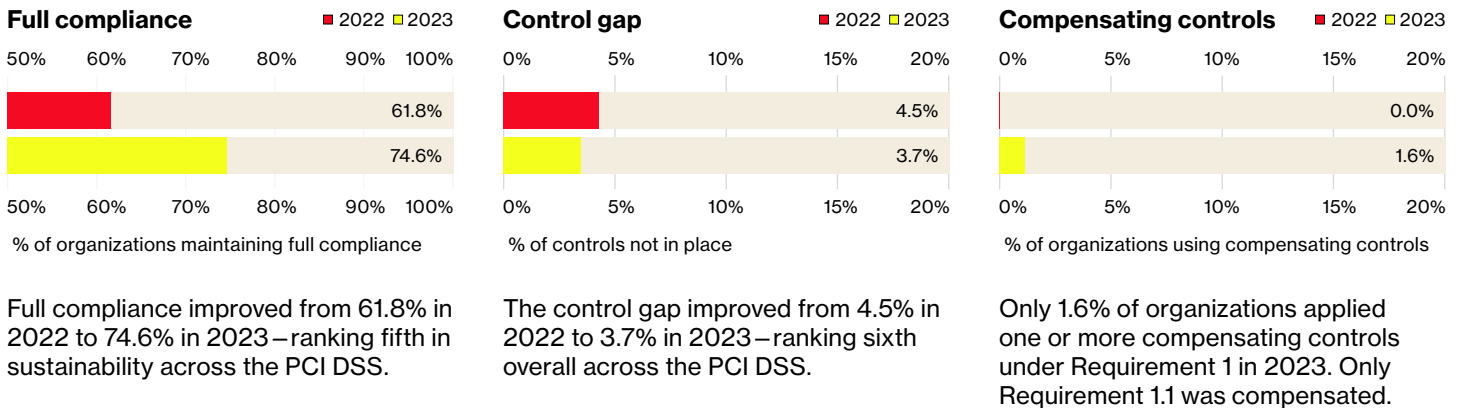
Requirement 2

Full compliance ■ 2022 ■ 2023

50%	60%	70%	80%	90%	100%

64.7%

58.7%

% of organizations maintaining full compliance
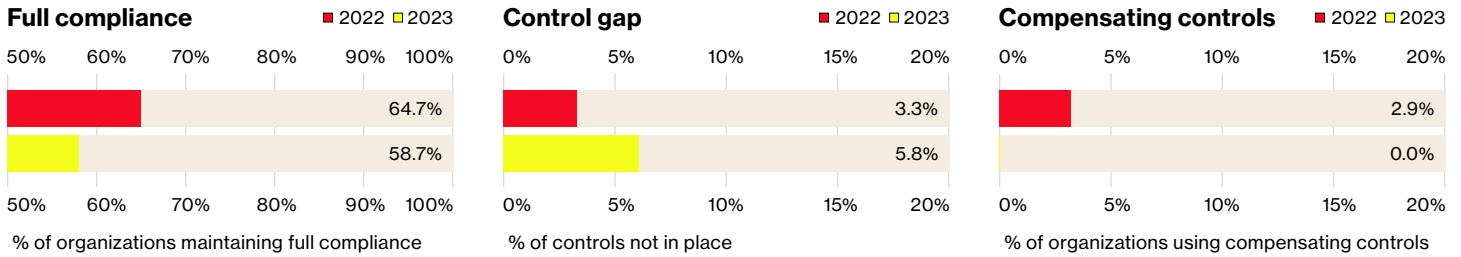
Full compliance declined from 64.7% in 2022 to 58.7% in 2023 – ranking ninth in sustainability across the PCI DSS.

Control gap ■ 2022 ■ 2023

0%	5%	10%	15%	20%

3.3%

5.8%

% of controls not in place

The control gap almost doubled from 3.3% in 2022 to 5.8% in 2023 – ranking 11th overall across the PCI DSS.

Compensating controls ■ 2022 ■ 2023

0%	5%	10%	15%	20%

2.9%

0.0%

% of organizations using compensating controls

No organizations applied any compensating controls under Requirement 2 in 2023.

Figure 11. Global state of PCI DSS compliance 2022 to 2023: Requirement 2

PCI DSS v3.2.1 Requirement 2 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
2.1	Change vendor defaults, disable unnecessary accounts.	100.0%	-12.3pp	87.7%	4	0.0%	4.0pp	4.0%	4
2.2	Develop configuration standards.	74.3%	1.1pp	75.4%	5	4.2%	1.4pp	5.6%	5
2.3	Encrypt nonconsole administrative access.	91.4%	-2.2pp	89.2%	3	2.9%	0.7pp	3.5%	3
2.4	Maintain an inventory of in-scope system components.	82.9%	-10.5pp	72.3%	6	11.4%	14.0pp	25.4%	6
2.5	Maintain policies and procedures for managing vendor defaults.	94.3%	2.6pp	96.9%	2	5.7%	-2.6pp	3.1%	2
2.6	Shared hosting providers must protect environments and data.	100.0%	-1.5pp	98.5%	1	0.0%	1.5pp	1.5%	1

Figure 12. Requirement 2 control performance

Requirement 3: Protect stored account data

This requirement covers the protection of stored cardholder data and sensitive authentication data (SAD). All stored payment account data must be protected using appropriate methods and must be securely deleted after it is no longer needed.

Requirement 3 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 3.

The goal: The goal of PCI DSS Key Requirement 3 is to develop, execute and maintain a sustainable capability for the ongoing effective, reliable and sustainable protection of all stored account data across the control environment; keep the storage of account data to a minimum; and prevent the storage of SAD post-authorization unless needed for card-issuing functions. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope: The goal applies to the storage of all PCI-branded CHD and/or SAD in electronic and hard copy formats and related system components as well as to data at rest in all storage locations (such as file servers, databases, storage arrays or areas, removable disks, and CDs) and includes storage in nonvolatile memory (disks and storage chips). The scope includes the management of responsibilities of any third parties involved in the transmission, storage and processing of account data.

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
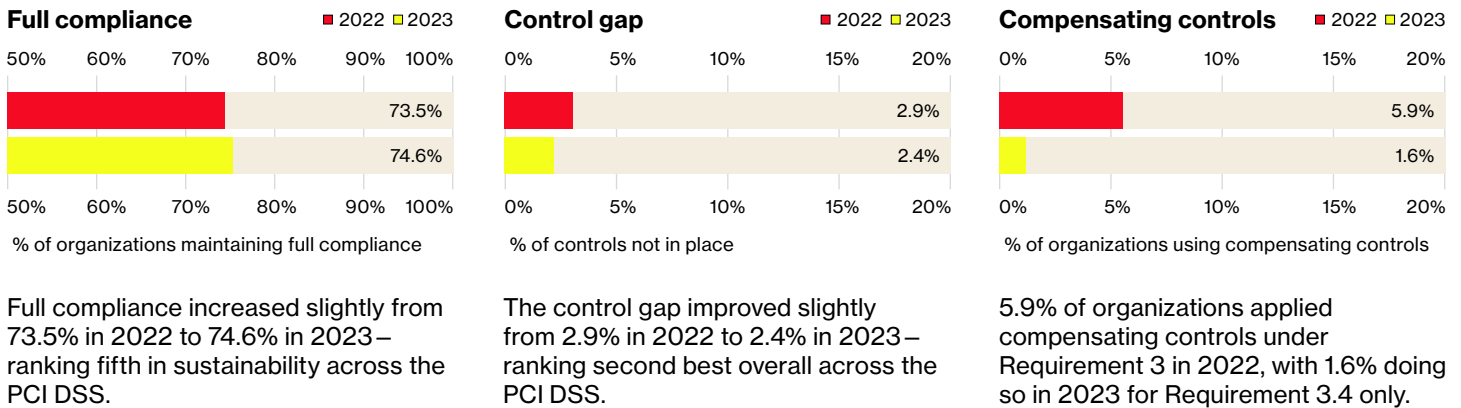
Requirement 3

Full compliance ■ 2022 □ 2023

73.5%
74.6%

% of organizations maintaining full compliance

Full compliance increased slightly from 73.5% in 2022 to 74.6% in 2023 – ranking fifth in sustainability across the PCI DSS.

Control gap ■ 2022 □ 2023

2.9%
2.4%

% of controls not in place

The control gap improved slightly from 2.9% in 2022 to 2.4% in 2023 – ranking second best overall across the PCI DSS.

Compensating controls ■ 2022 □ 2023

5.9%
1.6%

% of organizations using compensating controls

5.9% of organizations applied compensating controls under Requirement 3 in 2022, with 1.6% doing so in 2023 for Requirement 3.4 only.

Figure 13. Global state of PCI DSS compliance 2022 to 2023: Requirement 3

PCI DSS v3.2.1 Requirement 3 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
3.1	Keep data storage to a minimum.	85.7%	6.6pp	92.3%	5	6.7%	-3.1pp	3.6%	5
3.2	Do not store sensitive authentication data after authorization.	97.1%	-7.9pp	89.2%	6	1.6%	3.2pp	4.8%	7
3.3	Mask PANs when displayed.	97.1%	-0.2pp	96.9%	1	2.9%	-0.3pp	2.6%	4
3.4	Render PANs unreadable anywhere they are stored.	97.1%	-3.3pp	93.8%	4	1.8%	-0.1pp	1.7%	2
3.5	Protect keys used to secure stored CHD against disclosure.	82.9%	12.5pp	95.4%	2	3.9%	-2.4pp	1.5%	1
3.6	Document and implement key-management processes.	77.1%	9.0pp	86.2%	7	2.7%	-0.8pp	1.9%	3
3.7	Document policies for protecting stored CHD.	97.1%	-1.8pp	95.4%	2	2.9%	1.8pp	4.6%	6

Figure 14. Requirement 3 control performance

Requirement 4: Protect cardholder data with strong cryptography during transmission

This requirement is designed to protect cardholder data and sensitive authentication data when transmitted over unprotected networks—such as the internet—where it can be vulnerable to interception.

Requirement 4 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 4.

The goal: The goal of PCI DSS Key Requirement 4 is to develop, execute and maintain a sustainable capability for the effective monitoring and protection of CHD across the CDE through the application of strong cryptography to protect primary account numbers (PANs) during their transmission over open, public networks. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems as well as the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope: The goal applies to all system components across the CDE where any PAN is transmitted over open, public networks, such as the internet, messaging systems or wireless technologies (including Wi-Fi, Bluetooth, cellular technologies, satellite communications and General Packet Radio Service [GPRS] components). It also applies to all security system components (technology and people) that support the security controls needed to meet this key requirement, such as systems that support security certificates, cryptographic systems, and logging and monitoring systems.

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.

Requirement 4

Full compliance ■ 2022 □ 2023

% of organizations maintaining full compliance
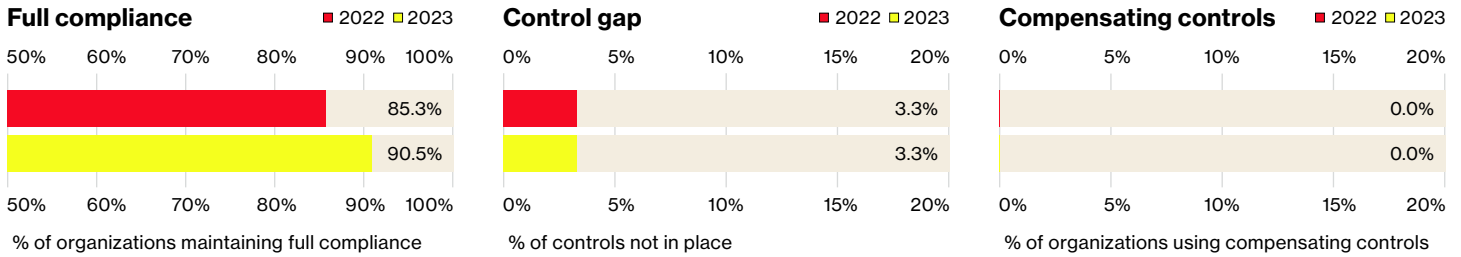
Full compliance improved significantly from 85.3% in 2022 to 90.5% in 2023—earning Key Requirement 4 the top spot as the most sustainable key requirement across the PCI DSS in 2023.

Control gap ■ 2022 □ 2023

% of controls not in place

The control gap remained unchanged at 3.3% from 2022 to 2023—ranking third best overall across the PCI DSS.

Compensating controls ■ 2022 □ 2023

% of organizations using compensating controls

No organizations applied any compensating controls under Requirement 4 in 2022 or 2023.

Figure 15. Global state of PCI DSS compliance 2022 to 2023: Requirement 4

PCI DSS v3.2.1 Requirement 4 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
4.1	Use strong cryptography and protocols.	82.9%	7.9pp	90.8%	3	3.4%	0.6pp	4.0%	3
4.2	Never send unprotected PANs by end user messaging technologies.	97.1%	1.3pp	98.5%	1	2.9%	-2.1pp	0.8%	1
4.3	Maintain procedures for encrypting transmissions of CHD.	97.1%	1.3pp	98.5%	1	2.9%	-1.3pp	1.5%	2

Figure 16. Requirement 4 control performance

Requirement 5: Protect all systems and networks from malicious software

This requirement concerns protecting all in-scope systems commonly affected by malicious software (malware) against viruses, worms and Trojans.

Requirement 5 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 5.

The goal: The goal of PCI DSS Key Requirement 5 is to ensure that all relevant systems across the CDE commonly affected by malicious software remain protected at all times against known and evolving malware threats with an effective antimalware solution and that organizational capability to respond to malware-related incidents is continually in place, and corrective action is taken in a timely manner to prevent or contain malware contamination of the CDE. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope: Technology components: This goal applies to all in-scope system components known to be affected by malware, which may include servers, employee computers, mobile computers, email systems and storage devices as well as related logging, monitoring and incident response systems.

People and teams: The goal also includes the individuals and teams responsible for the deployment, monitoring and response to malware-related incidents, the training and education of end users that access any CDE system components, and third-party vendors that supply or support antimalware and related security system components.

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
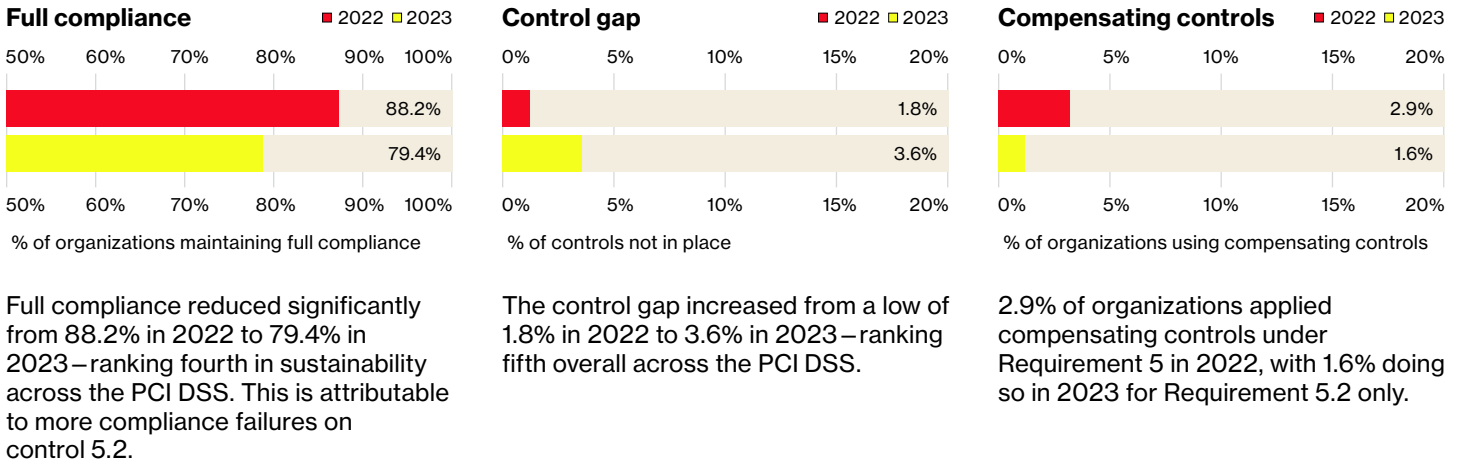
Requirement 5

Full compliance ■ 2022 ☐ 2023

% of organizations maintaining full compliance

Control gap ■ 2022 ☐ 2023

% of controls not in place

Compensating controls ■ 2022 ☐ 2023

% of organizations using compensating controls

Full compliance reduced significantly from 88.2% in 2022 to 79.4% in 2023 — ranking fourth in sustainability across the PCI DSS. This is attributable to more compliance failures on control 5.2.

The control gap increased from a low of 1.8% in 2022 to 3.6% in 2023 — ranking fifth overall across the PCI DSS.

2.9% of organizations applied compensating controls under Requirement 5 in 2022, with 1.6% doing so in 2023 for Requirement 5.2 only.

Figure 17. Global state of PCI DSS compliance 2022 to 2023: Requirement 5

PCI DSS v3.2.1 Requirement 5 controls		Full compliance				Control gap			
Performance year over year		**2022**	**Change**	**2023**	**Rank**	**2022**	**Change**	**2023**	**Rank**
5.1	Deploy antivirus software.	94.3%	-0.4pp	93.8%	3	1.9%	0.7pp	2.6%	3
5.2	Maintain all antivirus mechanisms.	91.4%	-6.8pp	84.6%	4	2.9%	4.0pp	6.9%	4
5.3	Ensure that antivirus mechanisms are actively running and cannot be disabled.	100.0%	-1.5pp	98.5%	1	0.0%	1.0pp	1.0%	1
5.4	Document policies for malware protection.	97.1%	1.3pp	98.5%	1	2.9%	-1.4pp	1.5%	2

Figure 18. Requirement 5 control performance

Requirement 6: Develop and maintain secure systems and software

This requirement covers the security of applications and change management. It governs how systems and applications are developed and maintained, whether by organizations or third parties.

Requirement 6 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 6.

The goal: The goal of PCI DSS Key Requirement 6 is to achieve and sustain mature processes and capabilities for developing and maintaining secure software and systems for all relevant system components across the CDE and to continually improve processes and capabilities for the effective, reliable and sustainable protection of account data. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **IT components:** Applies to all applicable system components across the CDE, such as routers, firewalls, operating systems, application software, databases, point-of-sale (POS) terminals and internet browsers that need to be patched in a timely manner

- **Security tools:** The management of web application firewalls (WAFs) and application security assessment tools

- **People:** All software developers involved with developing and testing of software for CHD-related components, the teams and individuals conducting application assessments and patching, and system-hardening tasks for in-scope systems

- **Documentation:** Software development procedures, secure coding life-cycle management methodologies, detailed application security assessment standards and procedures, and security patch management

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
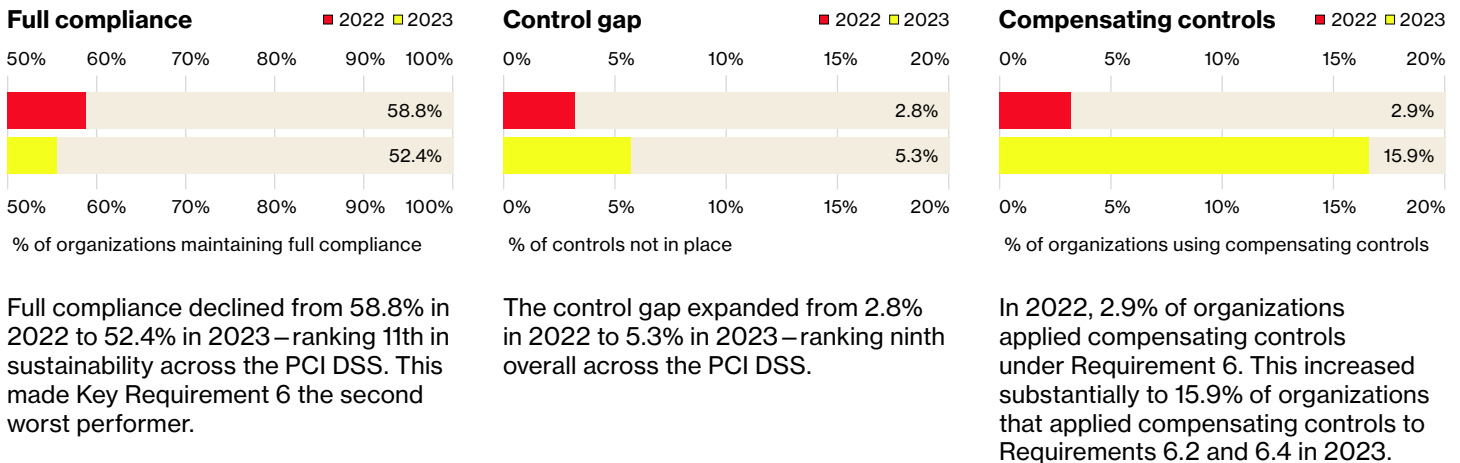
Requirement 6

Full compliance
▪ 2022 ▫ 2023

50% 60% 70% 80% 90% 100%

58.8%

52.4%

50% 60% 70% 80% 90% 100%

% of organizations maintaining full compliance

Full compliance declined from 58.8% in 2022 to 52.4% in 2023 — ranking 11th in sustainability across the PCI DSS. This made Key Requirement 6 the second worst performer.

Control gap
▪ 2022 ▫ 2023

0% 5% 10% 15% 20%

2.8%

5.3%

0% 5% 10% 15% 20%

% of controls not in place

The control gap expanded from 2.8% in 2022 to 5.3% in 2023 — ranking ninth overall across the PCI DSS.

Compensating controls
▪ 2022 ▫ 2023

0% 5% 10% 15% 20%

2.9%

15.9%

0% 5% 10% 15% 20%

% of organizations using compensating controls

In 2022, 2.9% of organizations applied compensating controls under Requirement 6. This increased substantially to 15.9% of organizations that applied compensating controls to Requirements 6.2 and 6.4 in 2023.

Figure 19. Global state of PCI DSS compliance 2022 to 2023: Requirement 6

PCI DSS v3.2.1 Requirement 6 controls		Full compliance				Control gap			
Performance year over year		2022	Change	**2023**	**Rank**	2022	Change	**2023**	**Rank**
6.1	Use reputable outside sources for vulnerability information.	91.4%	0.9pp	92.3%	3	4.3%	2.6pp	6.9%	6
6.2	Protect components and software from known vulnerabilities.	71.4%	4.0pp	75.4%	7	17.1%	-0.2pp	16.9%	7
6.3	Develop secure software applications.	91.4%	-5.3pp	86.2%	4	3.3%	3.3pp	6.6%	5
6.4	Follow change control processes.	85.7%	-7.3pp	78.5%	6	2.1%	2.5pp	4.6%	3
6.5	Address common coding vulnerabilities.	88.6%	-4.0pp	84.6%	5	0.8%	2.9pp	3.7%	2
6.6	Protect public-facing web applications against known attacks.	94.3%	1.1pp	95.4%	2	5.7%	-1.1pp	4.6%	3
6.7	Document policies and procedures for secure systems.	97.1%	-0.2pp	96.9%	1	2.9%	0.2pp	3.1%	1

Figure 20. Requirement 6 control performance

The PCI DSS v4.0.1 reverted to PCI DSS v3.2.1 language for Requirement 6 that installing patches/updates within 30 days applies only for "critical vulnerabilities."[25]

Three underlying factors that influence PCI security program performance

Despite the incremental improvements made to the PCI DSS over the course of the past 20 years and a substantial increase in the amount of supplemental guidance, our research has not indicated any significant widespread improvement in the percentage of organizations within our dataset that maintain sustainable PCI security compliance programs with the capability to rapidly detect and correct controls that are not in place. Why is this so?

This is a perennial question Verizon has explored for more than a decade. It distills down to three key factors:

- Commitment and accountability to achieve the overall program goal must be secured and maintained. (See "Trap 1 – Inadequate leadership" in the 2020 Payment Security Report, page 22.)

- An efficient and effective program design is essential to achieve successful outcomes. (See the 2023 insights white paper "Advanced PCI security program management design.")

- PCI security program management performance needs to be properly measured and evaluated.

Defining management performance

In general, performance management is a continual cycle of planning, tracking, analyzing performance and making adjustments. In the context of PCI DSS, one can broadly define compliance management performance as the capability to benefit from the resources invested in a PCI security program and the rate and consistency with which the program achieves its objectives. Performance is all about knowing what the organization's goals and objectives are for the security compliance program. The performance management cycle begins with defining strategic goals, which are then translated into operational plans and objectives for individual departments within the organization. These departmental plans may include detailed descriptions of targets, timelines and allocation of resources (people, budgets, IT support). By defining and monitoring KPIs and metrics, each department continually assesses whether its contributions to the PCI security program and performance are on track to meet those expectations. Performance measurement analyzes several indicators of the effectiveness of the program—the capacity, capability and commitment of the organization, division or team to achieve the security compliance goals and anticipated outcomes. Analyzing the performance data helps the organization determine whether it needs to adjust its strategy or tactics.

---

25   "Just Published: PCI DSS v4.0.1," PCI Security Standards Council, June 11, 2024. https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1

FACTOR 1: Commitment and accountability to achieve the overall program goal must be secured and maintained.

The reality is that the majority of organizations implement only what are explicitly specified as requirements within the PCI DSS catalog of defined requirements. Organizations choose, for various reasons, to only produce the minimum amount of evidence needed to meet whatever is explicitly stated as an evidence requirement in the PCI DSS validation testing procedures. Often this is for economic reasons—to reduce the number of resources (people, budget and time) allocated to PCI security compliance activities. Organizations, management and PCI security program participants need to have an incentive to do the work necessary to progress toward accomplishing the overall intent of PCI security. That may start with seeking commitment from people to work toward an articulated program goal and objectives that capture the intent of PCI data security. Program objectives should explicitly require that additional steps be taken to ensure that control strength, sustainability and maturity are fully integrated into the design as well as implementation of all PCI DSS requirements. Activities and tasks within projects linked to the PCI security program should include success factors, gatekeepers and milestones associated with the overall program goal to help projects and project managers remain focused on delivering work on objectives that contribute toward the goal—and avoid other work that is merely a distraction.

For most organizations, the overall goal of their PCI security program should be to develop and maintain an economically sustainable capability where the security of payment card data is effective and ongoing every day, year-round, and year after year. The program prioritizes which work needs to be done to effectively reduce and manage the risk of payment card data compromise to protect the interest of the business and clients. The goal should include meeting, and then exceeding,[26] the defined PCI DSS baseline security requirements with clear evidence that all the required PCI DSS security controls are kept in place in an efficient, yet effective and sustainable manner. At the very least, all critical controls should be kept in place by prioritizing their monitoring and the ability to rapidly detect and correct deviations. What is considered to be a critical control is determined on a case-by-case basis. In an ideal world, you would want to do this for all security controls—even the minor supporting controls—but due to economics (the scarcity of resources), this is not a realistic level of performance that can be sustained for many organizations.

It's not possible to realize the intended goals of PCI DSS without an internal performance measurement and evaluation program that actively drives the management performance of the PCI security program. This must encompass the entire life cycle of performance management activities—measuring components and processes, reporting and improving the performance—where continual improvement in terms of quality, frequency and throughput is baked into the performance management system. It should also include the use of maturity models to track the progress of improving processes and capabilities against established criteria.

FACTOR 2: An efficient and effective program design is essential to achieve successful outcomes.

The design of the compliance management program can likely, without exception, directly affect its performance and outcomes. Program performance requires structure to produce and maintain consistency of the input-process-output cycles. The construction, scope and success factors of PCI security program designs evolved significantly during the past 20 years. A basic program design with a scope that focuses mainly on the implementation of the PCI DSS 12 Key Requirements and preparation for compliance validation is significantly outdated. The program structure is of critical importance, i.e., the composition of program components directly determines the workflow and therefore also affects performance—the throughput and quality of output of the work delivered.

Organizations need to apply an integrated set of methods to design the management (planning and implementation) of their PCI security program—program design and management methods that offer clear visibility and perspective to establish and retain control over their payment card security programs and deliverables. The 2023 Payment Security Report insights white paper describes several PCI security program 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.

---

26 Basic examples of exceeding baseline PCI DSS requirements include conducting vulnerability testing every month instead of every quarter and encrypting all connections that transmit PANs—not only over untrusted networks (already a requirement) but also over trusted networks.

FACTOR 3: PCI security program management performance needs to be properly measured and evaluated.

"If you can't measure it, you can't manage it" is an often-quoted business maxim. The measurement and evaluation of PCI security program management performance is an area that needs greater attention. This applies to industries across the world and organizations of all sizes.

Many, if not most, organizations have yet to sufficiently formalize the methods, metrics and tools for measuring and optimizing the management of their PCI security program performance. We emphasize performance management and note that this is distinct from the basic management of PCI security programs in terms of communicating, planning and coordinating the implementation of tasks associated with PCI security compliance.

If you are planning on measuring program performance, you need to understand the underlying data and which metrics and KPIs to apply. (See Appendix B, "A deeper dive into PCI security performance measurement and evaluation," on page 97 of this publication.) Without sensible metrics, it's hard to quantify the performance of a PCI security compliance program and impossible to know its actual value.

A well-designed PCI DSS performance evaluation program is structured to:

- Improve transparency for individuals and their managers on the design and operation of the control environment and the quality of components (such as documents, processes, people, IT systems, projects, and other control environment and program components).

- Discover any arising problems before they affect the performance of controls and the security of the CDE.

- Track the progress of projects and activities.

- Provide the opportunity to improve core and supporting processes and pinpoint where to improve capabilities.

- Identify which projects are more or less beneficial to the accomplishment of objectives and achievement of the overall program goal.

- Provide access to valuable indicators of challenges and opportunities within the organization.

Performance evaluation

A structured assessment determines how well the organization is implementing the previously developed security compliance strategy and associated plans in daily operations, resulting in effectiveness and efficiency. It's necessary to evaluate the effectiveness of past strategies and formulate future strategies based on the results. A well-designed and executed performance evaluation should bring clarity and reveal what needs to be done to correct performance deficiencies. You need to have a single source of truth that can provide all types of information you may want to measure. You have to compare and analyze the relevant data to get a bigger picture of the operations and identify trends that could affect them.

Assessing your current data security and compliance situation

What is the very first step toward payment card data security and compliance failure?

When organizations do not assess the reality of their current security and compliance situation as is, it may set in motion events that ultimately result in the failure of a PCI security program to meet performance expectations. In other words, when executive leadership, a steering committee or program managers do not grasp what their reality is in terms of the actual strength of their control environment, challenges and failure (including data breaches) can occur. This is what Sun Tzu[27] describes in "The Art of War" as the first step toward failure. In the

When organizations do not assess the reality of their current situation as is, it can set in motion events that ultimately result in the failure of a PCI security program to meet performance expectations.

aftermath of many high-profile payment card data breaches, it became evident that decision-makers made decisions based on incorrect perspectives and false views of the reality of their data security and compliance environments.

Decision-makers who are responsible for the design, execution, management and evaluation of a corporate PCI security strategy and program need to know what to measure, evaluate and report. They need to know how to apply the methods for performing those measurement, evaluation and reporting tasks to gain the

perspective and clarity of their PCI security control environment and the true level of effectiveness in which payment card data and systems are secured. They need to know the efficiency (cost-effectiveness) of their PCI security program—the extent to which resources are wasted by not delivering the right work (focusing on what matters most) in the right manner as well as the ability to accurately determine the reality (the actual strength) of the control environment value and return on their PCI security compliance investment.

Compliance management applications

Many organizations automate performance evaluation reporting by using compliance management software. Every year, an increasing number of compliance management applications are available. Even small organizations benefit from software applications that visually display KPIs and other important data in a performance dashboard that provides a snapshot of the PCI security program and control performance.

Automating as many of the routine tasks and activities within your program as you can is a smart move—to structure and schedule the work that needs to be done as well as to automate reporting and produce insights on program performance to facilitate decision-making on what to change and improve. Off-the-shelf compliance management software often lacks essential features for measuring and reporting the actual strength of control environments.

Management applications are usually capable of presenting complex data in an easy-to-understand format, allowing business leaders to identify areas that need attention and make informed decisions quickly. Yet there is a lot of room for improvement because many applications omit critical metrics and KPIs from their reports and dashboards.

27   Sun Tzu, "The Art of War," translated by Thomas Cleary, Shambhala, 1988. In chapter 6, on "Weak Points and Strong," the author describes the concept of the first step of failure—the importance of perception and understanding reality. To avoid failure, one must emphasize the need for accurate assessment and clear perception of both one's own situation and that of the enemy.

Requirement 7: Restrict access to system components and CHD by business "need to know"

This requirement specifies the processes and controls that should restrict each user's access rights to the minimum they need to perform their duties on a need-to-know basis.

Requirement 7 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 7.

The goal: The goal of PCI DSS Key Requirement 7 is to maintain a reliable and sustainable capability to prevent unauthorized access to account data and systems across the CDE. This is done by effectively restricting access to system components and CHD by business "need to know" and maintaining the capability to detect and respond to access control violations. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.
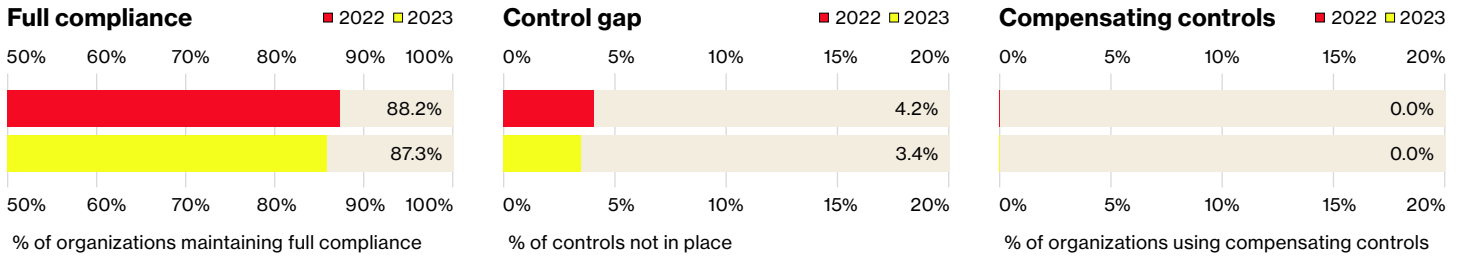
The scope:

- **IT components:** All system components within the CDE, including related security system components that support access control to and from the CDE. The most common role-based access control is Windows Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

- **People:** All employees (such as IT and security staff, accountants, support staff, call center agents, and executives), contractors, consultants, and internal and external vendors and other third parties that provide support or maintenance services as well as any individuals who can access CHD or any system component within the CDE (any component that processes, stores and/or transmits account data and also components that directly connect to or support such components)

- **Documentation:** Detailed documented standards and procedures for the configuration of all administrator and user accounts, including procedures to define, identify and assign different roles and responsibilities; access to data resources; required privilege levels; formal approval of access requests; and periodic internal audits for review and reconciliation between expected access privileges and actual system configurations

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.

Requirement 7

Full compliance ■ 2022 ■ 2023

% of organizations maintaining full compliance

Control gap ■ 2022 ■ 2023

% of controls not in place

Compensating controls ■ 2022 ■ 2023

% of organizations using compensating controls

Full compliance declined slightly from 88.2% in 2022 to 87.3% in 2023 — moving up from third position to rank second in sustainability across the PCI DSS.

The control gap narrowed from 4.2% in 2022 to 3.4% in 2023 — ranking fourth overall across the PCI DSS.

No organizations applied any compensating controls under Requirement 7 in 2022 or 2023.

Figure 21. Global state of PCI DSS compliance 2022 to 2023: Requirement 7

PCI DSS v3.2.1 Requirement 7 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
7.1	Limit access to system components.	85.7%	2.0pp	87.7%	3	7.6%	-2.5pp	5.1%	3
7.2	Establish access control based on need to know; set to deny all.	100.0%	-1.5pp	98.5%	1	0.0%	0.8pp	0.8%	1
7.3	Maintain policies and procedures for restricting access to CHD.	100.0%	-3.1pp	96.9%	2	0.0%	3.1pp	3.1%	2

Figure 22. Requirement 7 control performance

Requirement 8: Identify users and authenticate access to system components

This requirement mandates that access to system components be identified and authenticated and that each user be assigned a unique identification.

Requirement 8 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 8.

The goal: The goal of PCI DSS Key Requirement 8 is to protect payment card account data by maintaining a sustainable capability for the reliable application of strong authentication controls for all in-scope users and systems. It also aims to ensure that only authorized users can access any system component in the CDE and that they are uniquely identifiable, accountable and traceable and are given entitlements based on least privilege and need to know. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **People:** All in-scope users with access to sensitive data, systems and locations, which applies to all personnel, including general users, administrators, vendors and other third parties that access the entity's network from an external or remote network

- **IT components:** The application of automated authentication technology across the CDE, including technologies such as Active Directory, CyberArk, Resource Access Control Facility (RACF), remote authentication and dial-in service (RADIUS) with tokens, terminal access controller access control system (TACACS) with tokens, and other technologies that facilitate MFA

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
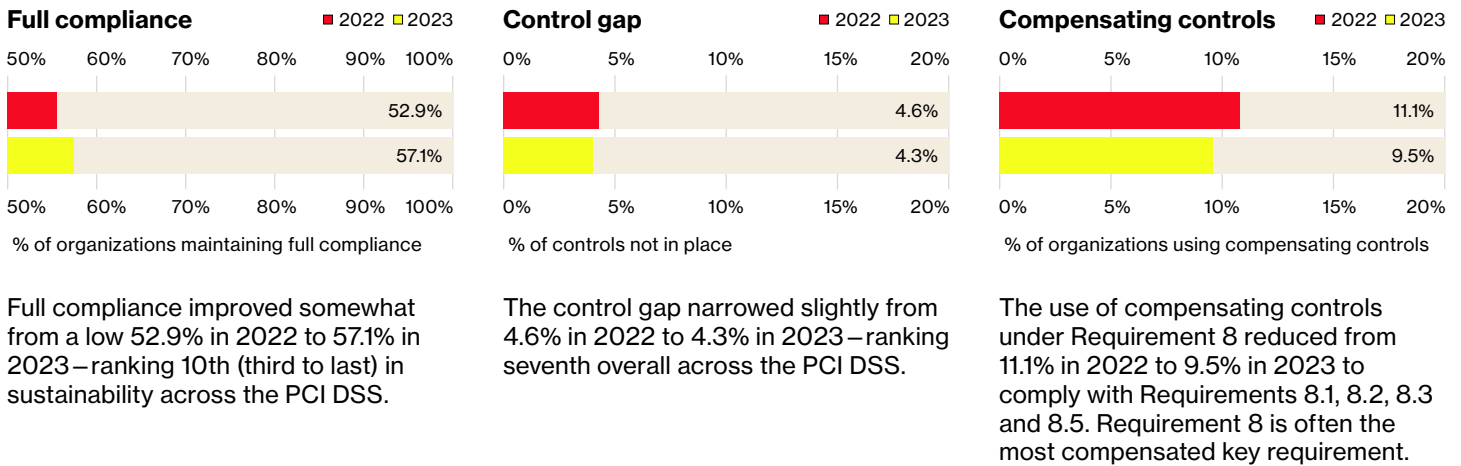
Requirement 8

Full compliance ■ 2022 □ 2023

% of organizations maintaining full compliance

Full compliance improved somewhat from a low 52.9% in 2022 to 57.1% in 2023—ranking 10th (third to last) in sustainability across the PCI DSS.

Control gap ■ 2022 □ 2023

% of controls not in place

The control gap narrowed slightly from 4.6% in 2022 to 4.3% in 2023—ranking seventh overall across the PCI DSS.

Compensating controls ■ 2022 □ 2023

% of organizations using compensating controls

The use of compensating controls under Requirement 8 reduced from 11.1% in 2022 to 9.5% in 2023 to comply with Requirements 8.1, 8.2, 8.3 and 8.5. Requirement 8 is often the most compensated key requirement.

Figure 23. Global state of PCI DSS compliance 2022 to 2023: Requirement 8

PCI DSS v3.2.1 Requirement 8 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
8.1	Define policies and procedures for user identification.	74.3%	-0.4pp	73.8%	8	5.7%	-0.5pp	5.2%	6
8.2	Ensure proper user authentication management.	68.6%	6.8pp	75.4%	7	4.5%	0.8pp	5.3%	7
8.3	Use MFA for all remote access to the CDE.	85.7%	5.1pp	90.8%	5	5.2%	-0.9pp	4.4%	5
8.4	Communicate authentication policies to all users.	97.1%	1.3pp	98.5%	2	2.9%	-2.3pp	0.5%	3
8.5	Do not use group/shared IDs.	82.9%	6.4pp	89.2%	6	5.7%	2.0pp	7.7%	8
8.6	Uniquely identify and secure authentication mechanisms.	100.0%	0.0pp	100.0%	1	0.0%	0.0pp	0.0%	1
8.7	Restrict all access to any database containing CHD.	94.3%	4.2pp	98.5%	2	4.3%	-3.9pp	0.4%	2
8.8	Maintain policies and procedures for identification.	97.1%	-0.2pp	96.9%	4	2.9%	0.2pp	3.1%	4

Figure 24. Requirement 8 control performance

Requirement 9: Restrict physical access to cardholder data

This requirement stipulates that organizations must restrict physical access to all systems within the PCI DSS scope and all hard copies of CHD.

Requirement 9 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 9.
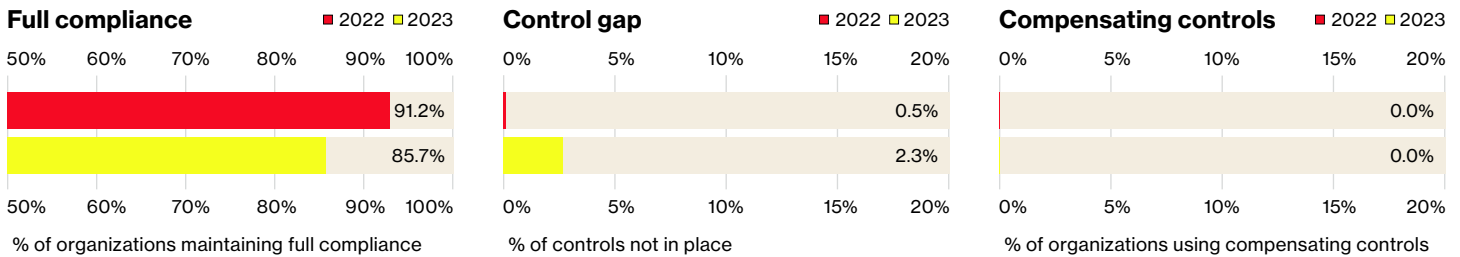
The goal: The goal of PCI DSS Key Requirement 9 is to protect payment card account data by maintaining a sustainable capability for the effective and reliable restriction of physical access to sensitive facilities, systems and any component (such as hard copies) that contain CHD across the CDE to authorized individuals only and to prevent, detect and respond to access attempts by any unauthorized individuals. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **CHD components:** All IT components, desktop and mobile computers, storage devices (such as external hard drives and backups), paper records, POS devices, and electronic audio recordings that contain payment card account data as well as components that can access such systems and the facilities in which they reside

- **Security components:** Network security components (routers, firewalls, logging and monitoring, access control, and authentication systems), wireless access points, network jacks, telecommunication lines, badge readers, key entry locks, closed-circuit television (CCTV) cameras and recording systems

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.

Requirement 9

Full compliance ■ 2022 ■ 2023

| 50% | 60% | 70% | 80% | 90% | 100% |

91.2%
85.7%

| 50% | 60% | 70% | 80% | 90% | 100% |

% of organizations maintaining full compliance

Control gap ■ 2022 ■ 2023

| 0% | 5% | 10% | 15% | 20% |

0.5%
2.3%

| 0% | 5% | 10% | 15% | 20% |

% of controls not in place

Compensating controls ■ 2022 ■ 2023

| 0% | 5% | 10% | 15% | 20% |

0.0%
0.0%

| 0% | 5% | 10% | 15% | 20% |

% of organizations using compensating controls

Key Requirement 9 experienced a significant reduction in compliance, from 91.2% in 2022 to 85.7% in 2023 — falling from its top spot in 2022 to third in sustainability across the PCI DSS.

The control gap widened from a low 0.5% in 2022 to 2.3% in 2023. Requirement 9 retained its top spot as the key requirement with the lowest gap across the PCI DSS.

No organizations applied any compensating controls under Requirement 9 in 2022 or 2023.

Figure 25. Global state of PCI DSS compliance 2022 to 2023: Requirement 9

PCI DSS v3.2.1 Requirement 9 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
9.1	Use appropriate facility entry controls to monitor access of CDE.	94.3%	-2.0pp	92.3%	8	0.8%	1.8pp	2.6%	7
9.2	Distinguish between on-site personnel and visitors.	100.0%	-4.6pp	95.4%	5	0.0%	3.6pp	3.6%	9
9.3	Control physical access for on-site personnel to sensitive areas.	97.1%	2.9pp	100.0%	1	1.0%	-1.0pp	0.0%	1
9.4	Implement procedures to identify and authorize visitors.	100.0%	-4.6pp	95.4%	5	0.0%	1.5pp	1.5%	4
9.5	Physically secure all media.	100.0%	-1.5pp	98.5%	2	0.0%	0.4pp	0.4%	3
9.6	Control internal and external distribution of media.	100.0%	-1.5pp	98.5%	2	0.0%	0.3pp	0.3%	2
9.7	Control storage and accessibility of media.	100.0%	-4.6pp	95.4%	5	0.0%	2.3pp	2.3%	6
9.8	Destroy media when it is no longer needed.	97.1%	-0.2pp	96.9%	4	0.7%	0.8pp	1.5%	4
9.9	Protect data capture devices from tampering/ substitution.	97.1%	-6.4pp	90.8%	10	1.1%	4.3pp	5.4%	10
9.10	Document policies restricting physical access to CHD.	94.3%	-2.0pp	92.3%	8	0.8%	1.8pp	2.6%	7

Figure 26. Requirement 9 control performance

Requirement 10:
Log and monitor all access to system components and cardholder data

This requirement covers the creation and protection of information that can be used for the tracking and monitoring of access to all systems in the PCI DSS scope and synchronization of all system clocks.

Requirement 10 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 10.

The goal: The goal of PCI DSS Key Requirement 10 is to develop and maintain a sustainable capability to effectively record and track user activities for preventing, detecting or minimizing the effect of a data compromise through reliable logging and monitoring of all access to system components and CHD. This ensures that all required logs are collected for all system components across the CDE and that they are correlated and reviewed daily, enabling the ability to effectively detect and respond to incidents in a timely manner. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **IT components:** A centralized, automated logging and monitoring system that collects and correlates logs from all related CDE system components, which includes all system components that store, process or transmit CHD and/or SAD and all critical system components, including those that perform security functions such as file-integrity monitoring or change-detection software, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), routers, firewalls, antimalware, database logging systems and application and physical access logs

- **People:** All internal staff and third parties involved in the implementation, management, monitoring and support of system components (such as those listed above) required to meet the goal of this key requirement

- **Standard of performance:** A complete, integrated security monitoring strategy, policy and procedure document with defined scope, roles and responsibilities for the production, protection and retention of audit trails, and expected standard of performance of people and systems supporting the achievement of this goal

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
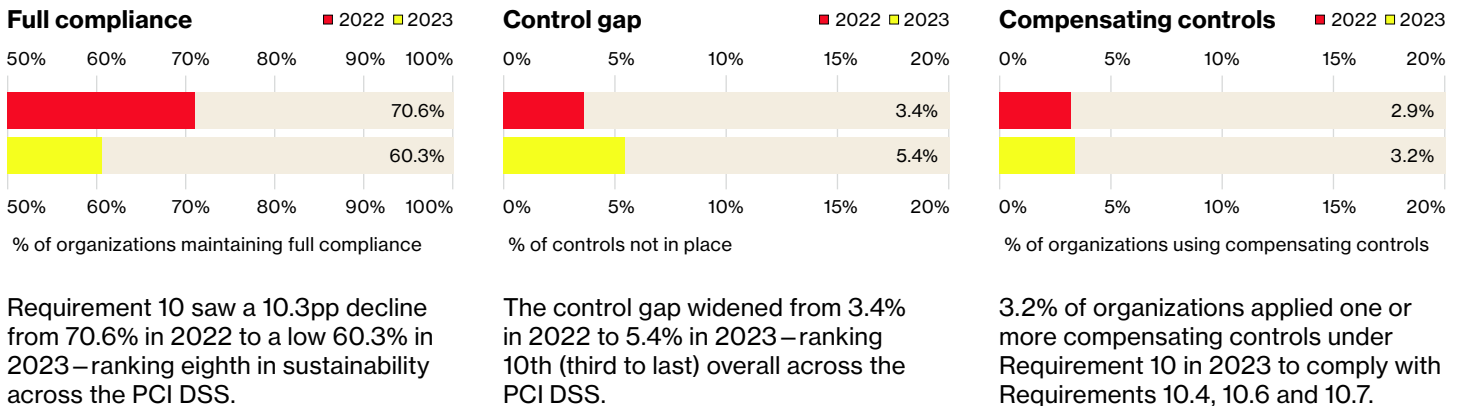
Requirement 10

Full compliance ■ 2022 □ 2023

% of organizations maintaining full compliance

Requirement 10 saw a 10.3pp decline from 70.6% in 2022 to a low 60.3% in 2023—ranking eighth in sustainability across the PCI DSS.

Control gap ■ 2022 □ 2023

% of controls not in place

The control gap widened from 3.4% in 2022 to 5.4% in 2023—ranking 10th (third to last) overall across the PCI DSS.

Compensating controls ■ 2022 □ 2023

% of organizations using compensating controls

3.2% of organizations applied one or more compensating controls under Requirement 10 in 2023 to comply with Requirements 10.4, 10.6 and 10.7.

Figure 27. Global state of PCI DSS compliance 2022 to 2023: Requirement 10

PCI DSS v3.2.1 Requirement 10 controls		Full compliance				Control gap			
Performance year over year		**2022**	**Change**	**2023**	**Rank**	**2022**	**Change**	**2023**	**Rank**
10.1	Implement audit trails linking access to individual users.	94.3%	-0.4pp	93.8%	3	5.7%	0.4pp	6.2%	7
10.2	Implement automated audit trails to reconstruct events.	77.1%	5.9pp	83.1%	8	4.0%	2.8pp	6.8%	8
10.3	Record user ID, date and time events.	94.3%	1.1pp	95.4%	2	0.8%	3.6pp	4.4%	3
10.4	Use time-synchronization technology.	82.9%	1.8pp	84.6%	6	6.2%	-3.1pp	3.1%	2
10.5	Secure audit trails so they cannot be altered.	88.6%	-5.5pp	83.1%	8	1.9%	3.5pp	5.4%	6
10.6	Review logs to identify anomalies or suspicious activity.	88.6%	0.7pp	89.2%	5	4.1%	1.2pp	5.3%	5
10.7	Retain audit trail history for at least one year.	97.1%	-12.5pp	84.6%	6	2.9%	7.4pp	10.3%	9
10.8	Report failures of critical security control systems.	97.1%	-6.4pp	90.8%	4	2.9%	2.1pp	4.9%	4
10.9	Maintain policies and procedures for monitoring all access.	94.3%	4.2pp	98.5%	1	5.7%	-4.2pp	1.5%	1

Figure 28. Requirement 10 control performance

Requirement 11:
Test security of systems and networks regularly

This requirement covers the use of vulnerability scanning, penetration testing, file integrity monitoring and intrusion detection to ensure that weaknesses are identified and addressed.

Requirement 11 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 11.

The goal: The goal of PCI DSS Key Requirement 11 is to develop and maintain a sustainable capability to effectively verify the security posture of all system components across the CDE using automated network scanning and penetration testing tools as well as manual methods, all designed to detect network and application vulnerabilities operating inside the network, and to rectify vulnerabilities based on a formal risk-assessment framework. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **Testing scope:** Security testing of all in-scope networks and IT system components across the CDE, including wireless access points, internal and external vulnerability scanning, internal and external penetration testing, segmentation testing, cloud environments, and service providers

- **Security tools:** Configuration, use and maintenance of network scan applications, penetration testing tools, change-detection tools (file-integrity monitoring), automated monitoring tools (IDS/IPS, network access control [NAC], wireless)

- **Process:** Documented vulnerability management program, including network and application vulnerability management procedures, penetration testing methodology, wireless access point assessments, security alert configuration standard, incident response process

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.
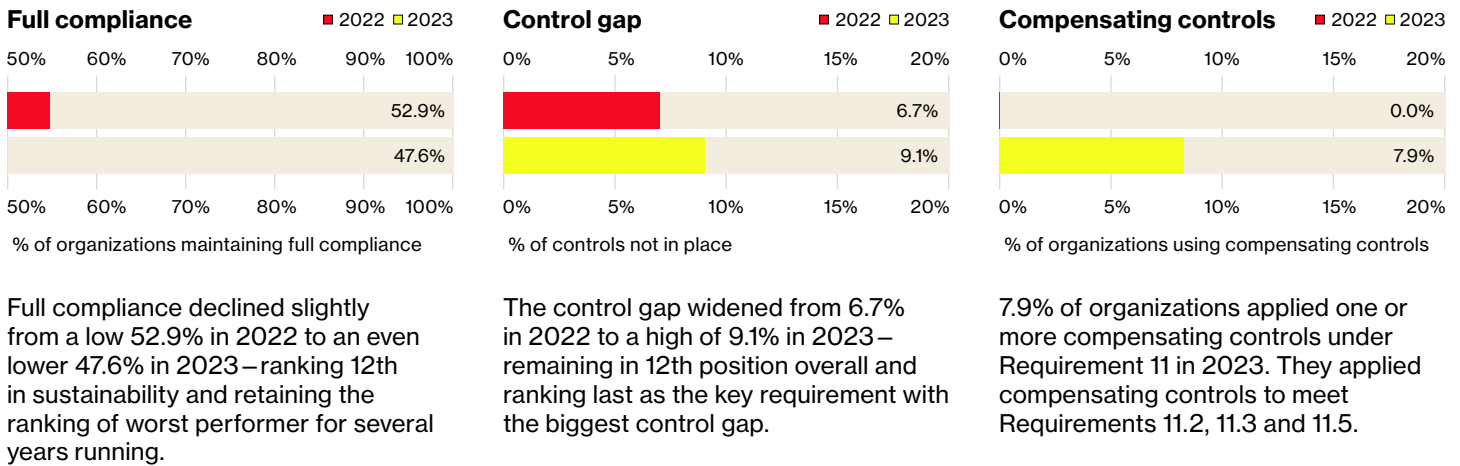
Requirement 11

Full compliance   ■ 2022 ■ 2023

% of organizations maintaining full compliance

Control gap   ■ 2022 ■ 2023

% of controls not in place

Compensating controls   ■ 2022 ■ 2023

% of organizations using compensating controls

Full compliance declined slightly from a low 52.9% in 2022 to an even lower 47.6% in 2023—ranking 12th in sustainability and retaining the ranking of worst performer for several years running.

The control gap widened from 6.7% in 2022 to a high of 9.1% in 2023— remaining in 12th position overall and ranking last as the key requirement with the biggest control gap.

7.9% of organizations applied one or more compensating controls under Requirement 11 in 2023. They applied compensating controls to meet Requirements 11.2, 11.3 and 11.5.

Figure 29. Global state of PCI DSS compliance 2022 to 2023: Requirement 11

PCI DSS v3.2.1 Requirement 11 controls		Full compliance				Control gap			
Performance year over year		2022	Change	2023	Rank	2022	Change	2023	Rank
11.1	Test for the presence of wireless access points.	94.3%	2.6pp	96.9%	1	1.2%	-0.6pp	0.7%	1
11.2	Run network vulnerability scans.	71.4%	-9.9pp	61.5%	6	11.4%	2.9pp	14.3%	6
11.3	Implement penetration testing.	65.7%	2.0pp	67.7%	5	7.5%	3.4pp	10.9%	5
11.4	Use intrusion detection systems.	97.1%	-4.8pp	92.3%	3	1.0%	4.7pp	5.6%	3
11.5	Deploy change detection mechanisms.	91.4%	-5.3pp	86.2%	4	7.6%	3.2pp	10.8%	4
11.6	Document procedures for monitoring and testing.	97.1%	-0.2pp	96.9%	1	2.9%	0.2pp	3.1%	2

Figure 30. Requirement 11 control performance

PCI DSS requirement process capability maturity evaluation

Results from our PCI DSS v3.2.1 state of compliance analysis indicate that organizations have much to do to reliably and sustainably produce required PCI security outcomes. See pages 40 and 41 for an overview of the use and limitations of capability maturity models. Maturity capabilities are the essential elements of effective processes, and they are useful to help describe how well an organization can control its various PCI security program processes.

PCI security management has a logical order. For many organizations, it begins with the need to correctly interpret and understand the PCI DSS requirements. The next steps are to determine the applicability of requirements and specify the control designs to prepare for implementation of the in-scope requirements, controlled execution of the control implementation, operation of the controls and evaluation of the control environment performance.

To briefly describe each of the six steps in terms of maturity capability:

1. **The interpretation of PCI DSS requirements:** The process capability to correctly interpret each PCI DSS requirement and the expectations on performance (required inputs/outputs, throughput) and meeting the intent of the requirement and control objective

2. **Determining requirement applicability:** The process capability to correctly determine which system components (people, processes, documents and technology) are included in the compliance environment and which PCI DSS requirements are either in scope of implementation and validation or not applicable and to be excluded from implementation

3. **PCI DSS requirement/control designs:** The process capability to prepare for the implementation of requirements with the use of documented security control design specifications and profile templates to achieve manageable and predictable control design, configuration and performance

4. **PCI DSS requirement implementation:** The process capability of putting requirements into effect (such as IT system configurations, documentation, training, awareness and reviews) within the control and compliance environments—with a controlled process (a staged/incremental implementation, or big-bang approach)

5. **PCI DSS requirement operation:** The process capability to establish or adjust operational processes (interaction between people, systems and documentation) and ensure alignment and adherence to policies, standards and procedures as well as controlled, predictable and sustainable control operation

6. **PCI DSS requirement performance evaluation:** The process capability to evaluate, report on and improve the operational performance of PCI DSS requirements using analytical applications, dashboards, scorecards and data-based decisions

Figure 31 on pages 80 and 81 outlines a capability maturity matrix for PCI DSS requirement measurement and evaluation. The maturity levels classify organizations' capabilities according to their performance and the quality of their management systems. It presents structured levels for how well the behaviors, practices and processes of an organization can reliably and sustainably produce outcomes on life-cycle management of PCI DSS requirements.

Process capability and maturity definitions

These basic definitions of process capability and maturity describe the fundamental concepts associated with the management of PCI security program and control requirements.

Defined process
A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs and exit criteria of a particular process.

Process capability
A process is "capable" if it satisfies its specified product quality, service quality and process performance objectives. A capable process consistently produces output that is within specifications. Execution of a capable process always gives predictable results.

Maturity
The degree of formality and optimization—from low maturity where processes and capabilities are ad hoc, unstructured and disorganized, with unpredictable performance and outputs, to highly mature practices that produce optimized outcomes. Mature processes are streamlined, fully standardized and documented, and tested for efficiency and effectiveness, and they deliver repeatable performance and can be consistently replicated.

Process maturity
A process is mature when work is performed in a well-structured, documented and controlled way and where everyone knows what is expected of them and performs accordingly.

PCI DSS process capability maturity matrix

Capability	1	Low/initial/ unpredictable	2	Managed/ reactive	3	Defined/ proactive/ predictable	4	Measured/ quantitatively managed	5	Optimized/high performance
Interpretation PCI DSS requirements interpretation capability		A process for the interpretation of PCI DSS requirements is only partially or not in place. There is only basic interpretation of requirements and minimal reference to supplemental guidance material. The processes and outcomes cannot be consistently replicated.		Interpretation of requirements are planned and executed according to policy using ordered methods that are well-documented. Management processes are still reactive and inconsistent.		A well-defined specification and process for how to interpret PCI DSS requirements and scope is documented and in place. Management is proactive with tailored processes and predictable performance.		The requirements interpretation process is consistently measured and controlled. Performance is tracked and reported. An integrated and searchable library of PCI DSS material is maintained.		Quality processes for the consistent guidance/ interpretation of PCI DSS requirements are maintained with ongoing process improvements. PCI DSS requirement interpretation work is performed in a well-structured, documented and controlled way, and outcomes can be consistently replicated.
Applicability Determining and reviewing PCI DSS requirements applicability		A process to determine the applicability of PCI DSS requirements is only partially or not documented. The process is not consistent and is unpredictable.		Management is reactive, with only a basic process for determining applicability of PCI DSS requirements. Baseline reports are used. Decision-flow diagrams are not used.		A complete specification contains clear guidance for how to determine applicability of PCI DSS requirements. Decision-flow diagrams and custom reports are used.		PCI DSS requirement applicability and scope evaluation are process-driven, consistently measured, reported, evaluated and controlled. There is quantitative reporting and management of PCI DSS scope.		Determining the applicability of PCI DSS requirements is a predictable process performed in a well-structured, documented and controlled manner. There is proactive maintenance of scope control and evidence of continual process improvement.
Control design PCI DSS requirement control design capability		The control design is open for interpretation. The control design specification is only partially or not documented. Control design processes are ad hoc and unpredictable.		A management process exists. Basic control design templates and guidance are in use and applied for some/ most controls. Control systems are only partially integrated.		Clearly defined control design standards, templates and procedures are maintained and consistently applied. The control design is proactive, predictable and fully replicable.		The design of PCI DSS controls is fully documented, controlled, quantitatively measured, reported, and evaluated. The design process is statistically tracked and monitored with automation.		The control design process is fully functional, automated and integrated. Improvement of the security control design process and integration between control design elements is ongoing.

(Figure continues on next page)

PCI DSS process capability maturity matrix (continued)

Capability	1	Low/initial/ unpredictable	2	Managed/ reactive	3	Defined/ proactive/ predictable	4	Measured/ quantitatively managed	5	Optimized/high performance
Implementation PCI DSS requirement implementation capability		Control implementation standards and procedures have only partial or no specifications. There is unpredictable implementation of key requirements.		A basic process for PCI DSS control implementation, with documented guidance, is in place. Baseline management reports are used.		Clearly defined, comprehensive control implementation procedures are described more rigorously and in use. Custom management reports are used.		Control implementation is quantitatively measured, with analytical reporting, historical trends and forecasting. Processes are tracked and monitored with IT automation.		High-quality requirement implementation outcomes can be consistently replicated. Ongoing improvement of tailored implementation processes and standards exists.
Operation PCI DSS requirement operation capability		Specifications for control operations are only partially or not documented. The operation of security controls is unpredictable and poorly controlled.		Control operation processes are established but not executed and managed in a standardized manner.		PCI security operation processes are clearly defined and predictable. Processes are audited. Metrics for evaluation and reporting are in place.		Operational PCI security processes, procedures and standards are statistically measured, reported and proactively controlled.		All PCI DSS operations are performed in a well-structured, documented and controlled way with outcomes that are consistently replicated. There is ongoing improvement of operational performance.
Evaluation Internal PCI DSS requirement evaluation capability		Specifications for PCI DSS control evaluation are only partially or not documented. Evaluation processes are disorganized, unpredictable, poorly controlled.		PCI DSS requirement evaluation processes are planned, documented and manageable but often reactive. Only basic reporting on evaluation results exists.		Evaluation processes are clearly defined, standardized and understood. Custom evaluation reports and tools are used to support automation.		Life-cycle evaluation of PCI DSS requirements are quantitatively measured, statistically reported, consistently monitored and controlled.		Dashboard scorecards and analytical applications are used to make data-based decisions. Evaluation processes are high quality and continually improved.

Figure 31. A process capability maturity matrix for PCI DSS v4.0x requirement measurement and evaluation

Requirement 12: Support information security with organizational policies and programs

Actively manage security team data protection responsibilities by establishing, updating and communicating security policies and procedures aligned with the results of regular risk assessments.

Requirement 12 performance evaluation

Develop and maintain an internal performance measurement and evaluation program to report and improve the overall maturity of processes and capabilities associated with PCI DSS Requirement 12.

The goal: The goal of PCI DSS Key Requirement 12 is to develop and maintain a sustainable and secure control environment for the effective protection of payment card data by maintaining a comprehensive program—supported by an integrated set of documented organizational information security, risk management and compliance standards, policies and procedures—with oversight from a governance structure and supporting processes for effective execution and continual improvement.

This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training.

The scope:

- **Documentation:** Security policies, standards, procedures and guidance documents that cover all PCI DSS requirements, third-party vendor agreements, incident response plans and security awareness program plans

- **People:** Applies to all employees (such as IT and security staff, accountants, support staff, call center agents, and executives), contractors, consultants, and internal and external vendors and other third parties that provide support or maintenance services to in-scope components, as well as any individuals who can access account data or any system component within the CDE

Action: Frequently evaluate and report the extent to which each activity contributes toward the overall goal of this requirement.

Requirement 12

Full compliance   ■ 2022 ■ 2023

% of organizations maintaining full compliance

Full compliance declined significantly from 73.5% in 2022 to a low 63.5% in 2023 — ranking seventh in sustainability across the PCI DSS.

Control gap   ■ 2022 ■ 2023

% of controls not in place

The control gap doubled from a relatively low 2.3% in 2022 to a fairly high 5.0% in 2023 — ranking eighth overall across the PCI DSS.

Compensating controls   ■ 2022 ■ 2023

% of organizations using compensating controls

No organizations applied any compensating controls under Requirement 12 in 2022 or 2023.

Figure 32. Global state of PCI DSS compliance 2022 to 2023: Requirement 12

PCI DSS v3.2.1 Requirement 12 controls		Full compliance				Control gap			
Performance year over year		**2022**	**Change**	**2023**	**Rank**	**2022**	**Change**	**2023**	**Rank**
12.1	Publish, maintain and disseminate a security policy.	88.6%	-7.0pp	81.5%	9	2.9%	1.1pp	4.0%	6
12.2	Implement a risk-assessment process.	100.0%	-10.8pp	89.2%	7	0.0%	10.8pp	10.8%	10
12.3	Develop usage policies for critical technologies.	97.1%	-3.3pp	93.8%	4	0.2%	1.9pp	2.1%	1
12.4	Define information security responsibilities for all personnel.	94.3%	-0.4pp	93.8%	4	4.3%	-1.2pp	3.1%	3
12.5	Assign information security management responsibilities.	97.1%	-1.8pp	95.4%	3	1.0%	1.1pp	2.1%	1
12.6	Implement a formal security awareness program.	91.4%	-5.3pp	86.2%	8	3.3%	6.2pp	9.5%	9
12.7	Screen potential personnel prior to hire.	100.0%	-3.1pp	96.9%	1	0.0%	3.1pp	3.1%	3
12.8	Manage service providers with policies and procedures.	88.6%	-8.6pp	80.0%	11	2.9%	8.7pp	11.5%	11
12.9	Ensure that service providers acknowledge responsibility.	100.0%	-3.1pp	96.9%	1	0.0%	3.1pp	3.1%	3
12.10	Implement an incident response plan.	88.6%	-7.0pp	81.5%	9	2.9%	1.1pp	4.0%	6
12.11	Additional requirements for service providers on policies and procedures.	91.4%	-0.7pp	90.8%	6	6.7%	1.0pp	7.7%	8

Figure 33. Requirement 12 control performance

Bottom-20 list

The 20 biggest control gaps

The control gap indicates the number of failed controls divided by the total number of controls expected. This is an averaged figure that provides a measure of how far the assessed organizations were from full compliance. A recurring pattern year after year, Requirement 11 requirements for penetration testing and security vulnerability scans continue to have the highest control gap.

#	Gap (2023)	PCI DSS control	PCI DSS control and testing procedures descriptions
1	38.5%	11.2	Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed.
2	27.7%	2.4.a	Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.
3	27.7%	2.4	Maintain an inventory of system components that are in scope for PCI DSS.
4	26.2%	8.1	Define and implement policies and procedures to ensure proper user identification management for nonconsumer users and administrators.
5	24.6%	6.2.b	Select a sample of system components and related software, and compare the list of security patches.
6	24.6%	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor patches, and install critical patches within one month.
7	23.1%	2.4.b	Interview personnel to verify that the documented inventory is kept current.
8	23.1%	1.1	Inspect the firewall and router configuration standards and other documentation to verify that standards are complete and implemented.
9	23.1%	8.1.b	Verify that procedures are implemented for user identification management.
10	20.0%	11.2.2.a	Review output from the four most recent quarters of external vulnerability scans, and verify that four occurred in the most recent 12 months.
11	20.0%	11.2.1.a	Review internal vulnerability scan reports, and verify that four passing quarterly scans were obtained in the most recent 12 months.
12	16.9%	11.2.1.b	Review internal vulnerability scan reports, and verify that all high-risk vulnerabilities are addressed and that the scan process includes rescans to verify remediation.
13	15.4%	11.3.3	Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed remediation.
14	15.4%	5.2	Ensure that all antivirus mechanisms are periodically maintained.
15	15.4%	6.5	Address common coding vulnerabilities in software-development processes.
16	15.4%	12.8.1	Verify that a list of service providers is maintained and includes a description of the service provided.
17	15.4%	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.
18	13.8%	10.7.b	Interview personnel and examine audit logs to verify that audit logs are available for at least one year.
19	13.8%	11.3.2.a	Examine the scope of work and results from the most recent internal penetration test.
20	13.8%	3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

Methodology

State of compliance

Dataset

Producing a PCI DSS assessment report may involve numerous assessments. In several cases, an assessment report is the product of assessments conducted globally or across a specific region. Individual PCI DSS compliance reports consist of between one and, in some cases, more than 120 assessments per report, covering multiple in-scope locations.

Assessments

PCI DSS version: The data from all assessments are based on PCI DSS v3.2.1, which consists of 12 PCI DSS Key Requirements, 79 controls, 252 control requirements and 417 test procedures, excluding a few additional requirements in the PCI DSS appendices.

This edition of the Payment Security Report is likely the last research analysis of PCI DSS v3.2.1. From 2024 onward, validation assessments are against PCI DSS v4.0 and updated versions of the v4.0x series.

Reports: The comparative analysis of PCI DSS requirements is based on an aggregate of PCI DSS ROC validation reports across the Americas; Europe, Middle East and Africa (EMEA); and Asia and the Pacific (APAC) regions. All ROCs included in the dataset were completed with a control status for each control. There are no partial ROCs included in the dataset.

Data sources: This PCI DSS state of compliance research is based on the analysis of quantitative data gathered by QSAs from multiple Qualified Security Assessor Company (QSAC) organizations across the world. The dataset for this edition is based on information from six sources. In alphabetical order, they are:

- Control Gap (controlgap.com)
- GM Sectec Corporation (gmsectec.com)
- Integrity360 (integrity360.com)
- MegaplanIT Holdings, LLC (megaplanit.com)
- Online Business Systems (obsglobal.com)
- Verizon (verizon.com/business)

Verizon appreciates the contributions of anonymized PCI DSS validation data from third-party contributors and welcomes other QSACs to participate in the collective research for the PCI DSS state of compliance.

Data volume: In 2023, the compliance status of a total of 29,120 PCI DSS v3.2.1 requirements was validated against 15,680 requirements assessed in 2022. It's noteworthy that a comparatively significant decline in the number of PCI DSS reports recorded for interim assessments occurred during the COVID-19 pandemic—particularly for the 2021 dataset. This reduction in volume negatively affects the statistical strength and validity for the 2021 dataset and has a marginal effect on the 2022 results.

"

Anything can be measured. If a thing can be observed in any way at all, it lends itself to some type of measurement method. No matter how 'fuzzy' the measurement is, it's still a measurement if it tells you more than you knew before."[28]

Douglas W. Hubbard

---

28   Douglas W. Hubbard, "How to Measure Anything," Third ed., Wiley, 2014.

The data analysis process

Our overall Payment Security Report data collection and analysis process remains intact and unchanged from previous years. All assessment data included in this report was individually reviewed and converted to create a common, anonymous aggregate dataset. The collection method and conversion are the same between contributors. In general, three steps were used to accomplish the dataset:

1. Enroll contributors and collect eligible PCI DSS v3.2.1 assessment reports.

2. Fully anonymize and convert the reports by the contributors into normalized data. All contributors received and followed instruction to omit any information that might identify organizations or individuals involved.

3. Secure submission of the anonymized data to the Verizon Payment Security Report data science team for aggregated analysis.

Data eligibility

For a potential entry (interim/draft ROC) to be eligible for the PCI DSS compliance validation corpus, it must meet several requirements. The entry must be data from a confirmed PCI DSS validation assessment conducted by a QSA who completed a ROC for an interim validation assessment. In addition to meeting the baseline definition of a draft or interim ROC, the entry is assessed for quality. A subset of compliance report data is then created that passes our quality filter.

In addition to having the level of details necessary to pass the quality filter, the assessment reports must be within the time frame of analysis.

What percentage of total PCI DSS compliance validation assessments that are conducted worldwide each year is covered in the survey? We do not know. We only have access to the data for the validation assessments that were conducted by Verizon and contributing QSACs.

Noncommittal disclaimer

We would like to reiterate that we make no claim that the findings of this report are representative of all PCI DSS compliance assessments for all organizations at all times. Even though the combined records from all our contributors more closely reflect reality than any of them in isolation, this dataset is still a sample. Although we believe many of the findings presented in this report are appropriate for generalization (and our confidence in this grows as we gather more data and compare it to that of other security organizations), bias undoubtedly exists.

The findings are based on aggregated demographic information. While aggregations are made up of individual organizations, individual organizations are not made up of aggregations. It's not a two-way street. There are limitations to the extent that these aggregations can be useful in making decisions. Therefore, when reading the findings of this report, do not make assumptions about their applicability to individual organizations. Some findings and conclusions require additional context and data to add more value on the individual level.

4 | Appendices
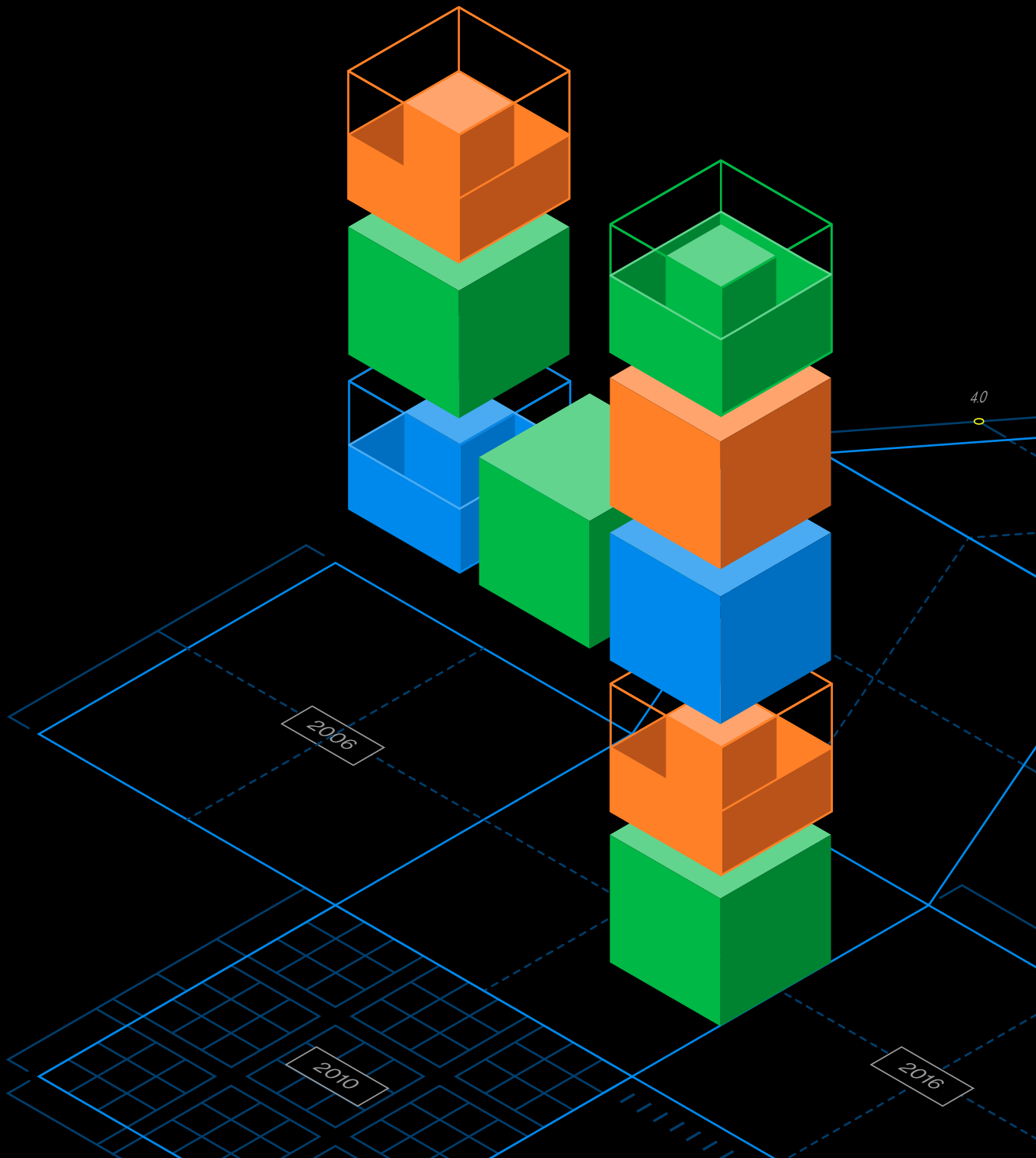
Appendix A:
The rise and risk of third-party scripts in modern websites

By Stephen Ward
Chief Marketing Officer
Source Defense

Cyber adversaries increasingly are targeting third-party scripts to steal data at the point of input. This term spotlights the shift in focus from traditional data targets—data in transit or at rest—to the point where users first input their data. Attackers exploit vulnerabilities in third-party scripts to inject malicious code, which enables them to capture data as soon as it's entered into the online forms that power e-commerce. These attacks are referred to as Magecart, e-skimming, digital skimming, clickjacking, credential harvesting and other terms, but they are all synonymous with a major threat confronting consumer personally identifiable information (PII), credentials and payment card data.

The ability of cybercriminals to target this data in real time, exposing potentially billions of online consumer sessions to their illicit activities, stems from the evolution of the modern website and a fundamental weakness in website design, security and third-party risk management. JavaScript powers the vast majority of the world's websites. The JavaScript powering these sites increasingly comes from third-party digital supply chain partners, whose code is neither vetted by website owners nor controlled by them with any regularity.

The modern website now has its own third-party supply chain. Source Defense's comprehensive analysis of more than 7,000 of the world's largest merchant websites reveals a disconcerting landscape dominated by third- and fourth-party scripts, with a staggering 129,897 scripts identified. These scripts, often embedded within payment pages and directly interacting with PII and payment data, underscore a significant cybersecurity and payment security vulnerability.

Specifically, 51,968 scripts were found on payment pages (40% of the total observed), 17,002 were accessing PII, and thousands more were handling sensitive payment and credentials data. The findings highlight a pervasive oversight.

They show an average of more than 18 scripts per page—with a distinction between third- and fourth-party contributions—further highlighting the extent of potential exposure. This represents a 50% increase in script use compared to our previous findings, which underscores the urgent need for enhanced scrutiny and strategic oversight within digital security frameworks.

Requirements 6 and 11 and scripts

New updates to Requirements 6 and 11 in the Payment Card Industry Data Security Standard (PCI DSS) include a requirement to inventory, authorize, monitor and secure scripts running on payment pages and within payment flows. Monitoring the script behavior and preventing unauthorized access to this sensitive data is key to meeting PCI DSS v4.0x[29] compliance. In addition, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 has clear directives to inventory third-party services, understand data access and flows between those third parties, and guide organizations to mitigate and manage data loss incidents. Both frameworks highlight the critical blind spot third- and fourth-party scripts represent in safeguarding online transactions and user data against cyberthreats.

29 The "x" designates any incremental or future versions of the PCI Data Security Standard.

New updates to PCI DSS include a requirement to inventory, authorize, monitor and secure scripts running on payment pages and within payment flows. Monitoring the script behavior and preventing unauthorized access to this sensitive data is key to meeting PCI DSS v4.0x compliance. In addition, NIST CSF 2.0 has clear directives to inventory third-party services, understand data access and flows between those third parties, and guide organizations to mitigate and manage data loss incidents. Both frameworks highlight the critical blind spot third- and fourth-party scripts represent in safeguarding online transactions and user data against cyberthreats.

The evolution of third-party scripts

The inception of third-party scripts dates back to the early days of web development, when the need for dynamic content and functionality led to widespread adoption. Initially, these scripts were simple tools for enhancing website aesthetics or tracking basic user interactions. As the internet matured, so did the complexity and capabilities of these scripts, evolving into sophisticated tools integral to e-commerce, social media and data analytics.

Today, third-party scripts are indispensable, powering everything from chatbots and payment gateways to analytics and advertising tools. Scripts can help businesses better understand their customers and tailor their offerings accordingly. However, this reliance poses significant security challenges. These scripts, by nature, can access, modify and transmit sensitive user data, making them prime targets for cyber adversaries. The data compiled and analyzed by Source

Defense shows the alarming prevalence of unsecured third- and fourth-party scripts across various industries.

Several high-profile breaches over the years highlight the critical need for robust security measures for third-party scripts, particularly those handling sensitive user data, such as a:

- **Large children's apparel retailer (2019):** Threat actors compromised the merchant website by inserting malicious code that skimmed customer financial details directly from the payment process. The breach potentially exposed customer names, shipping and billing addresses, payment card numbers, card verification value (CVV) codes, and expiration dates.

- **Global airline (2018):** A breach occurred through malicious third-party scripts on the airline's website. Attackers injected code to capture customer data during payment, affecting 380,000 transactions. This breach highlighted the vulnerabilities in scripts managing sensitive data, leading to significant financial penalties and reputational damage.

- **Ticket sales and distribution company (2018):** The company website was compromised through a third-party chatbot script. The breach exposed the personal and payment information of thousands of customers.

Percentage of scripts on payment pages, accessing PII data, accessing payment data or accessing credentials

Scripts accessing credentials
4.2%

Scripts accessing payment data
4.8%

Scripts accessing PII data
22.4%

Other
68.5%
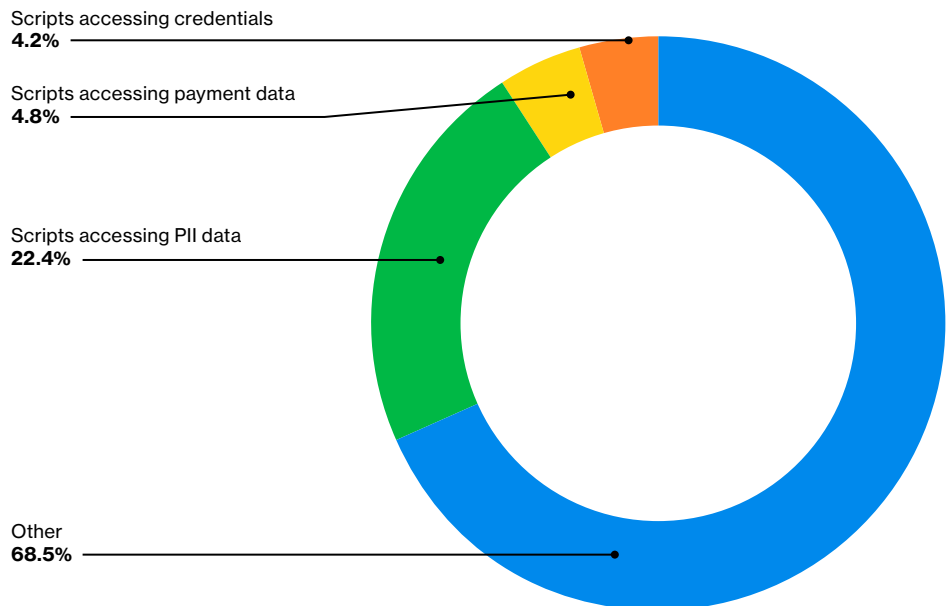
Figure 34. 7,075 unique websites from 6,342 companies

Visa's biannual report continues to highlight the threat of e-skimming, reporting that, "The targeting of eCommerce platforms and third-party code integrations are among the most common tactics utilized by threat actors ... threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information."[30] The security firm Recorded Future found that 1,520 unique malicious domains were involved in the infections of 9,290 unique e-commerce domains at any point in 2022.[31] And as late as January 2024, Europol disrupted an organized e-skimming operation that was impacting hundreds of European Union merchants and millions of consumers.[32]

> 💡 **Recommended reading:** "Biannual Threats Report," Visa, December 2023. https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/pfd-biannual-threats-report-december-2023.pdf

Changes to safeguard scripts

The new requirements in the PCI DSS recognize this evolving threat and the critical role of script management in safeguarding payment data. Compliance now requires a proactive approach to script security to protect against data breaches. This includes implementing robust monitoring and control measures to ensure that scripts do not become a weak link in payment card data security.

Different approaches can be taken to mitigate the risks associated with third-party scripts. Subresource integrity (SRI) checks can help prevent tampering with a script, while content security policies (CSPs) can restrict which scripts run on a webpage. Proprietary script management solutions, such as the pioneering Source Defense platform, offer another option by providing a comprehensive framework for managing and securing scripts.

Script mitigation strategies

Script security will likely expand as the digital landscape evolves. Future changes may include a greater emphasis on behavioral-based assessment and authorization of scripts. This could involve analyzing the behavior of scripts in real time to detect and block potentially malicious activity.

The rise of third-party scripts has brought with it new challenges and risks. However, by understanding these risks and implementing effective mitigation strategies, organizations can harness the benefits of third-party scripts without compromising security or privacy.

The most effective approach to third-party script management and security involves real-time monitoring and control. This method includes proactively identifying and mitigating threats and ensuring that script vulnerabilities are addressed promptly. This approach bolsters web application security by focusing on preemptive defenses and aligns with data protection standards, safeguarding sensitive customer data against potential cyberthreats.

Third-party scripts are a game-changer in web development, offering unparalleled functionality. But the security challenges are massive. Protecting data at the point of input is a critical step in addressing these challenges.

30 "Biannual Threats Report," Visa, June 2022. https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/biannual-threats-report.pdf
31 "Annual Payment Fraud Intelligence Report: 2022," Recorded Future, January 17, 2023. https://www.recordedfuture.com/annual-payment-fraud-intelligence-report-2022
32 "Action against digital skimming reveals 443 compromised online merchants," Europol, December 22, 2023. https://www.europol.europa.eu/media-press/newsroom/news/action-against-digital-skimming-reveals-443-compromised-online-merchants

Data findings summary report

Generally, a strong correlation exists between how customizable a product or service offering may be and the utilization of scripts on the websites that sell them. This makes sense because many scripts in use today relate to customization, suggestions to consumers on additional products, and shopping cart value enhancement and conversion.

High volume of scripts in certain industries: The apparel and fashion industry leads with a significantly higher volume of scripts than other industries, indicating a heavy reliance on third-party services for analytics, marketing, customer engagement and e-commerce functionalities. This suggests that industries with a strong online retail presence tend to integrate more third-party scripts to enhance user experience and drive sales, but at the potential cost of increased exposure to security vulnerabilities.

Widespread use of third-party services: The presence of third-party scripts across various industries highlights the reliance on external services for a wide range of functionalities, including analytics, payment processing, marketing and customer support. While these services can provide valuable insights and capabilities, they also introduce potential risks because each script represents a vector through which data breaches or leaks can occur if not properly managed.

Potential security risks: The accessing of PII, payment data and credentials through scripts poses significant security risks, especially if the scripts are from third-party sources. Each script with access to sensitive data increases the attack surface for potential exploitation by malicious actors. Industries with high numbers of such scripts need to implement robust security measures to protect against data breaches, cross-site scripting (XSS) attacks and other vulnerabilities.

Need for rigorous security policies and practices: The data underscores the importance of implementing rigorous security policies and practices—including regular audits of third-party scripts, ensuring compliance with data protection regulations (such as the General Data Protection Regulation [GDPR] and the California Consumer Privacy Act [CCPA]), and adopting secure coding practices. Industries must prioritize data privacy and security by vetting third-party vendors, using CSPs to restrict script sources and employing data encryption in transit and at rest.

Client-side security solutions: There's a clear need for advanced client-side security solutions, such as real-time monitoring tools, that can detect and mitigate threats posed by third-party scripts.

Consumer awareness and transparency: The extensive use of scripts that access sensitive information calls for greater consumer awareness and transparency from companies about how data is collected, processed and stored. Providing clear, accessible privacy policies and offering users control over their data can help build trust and ensure compliance with privacy standards.

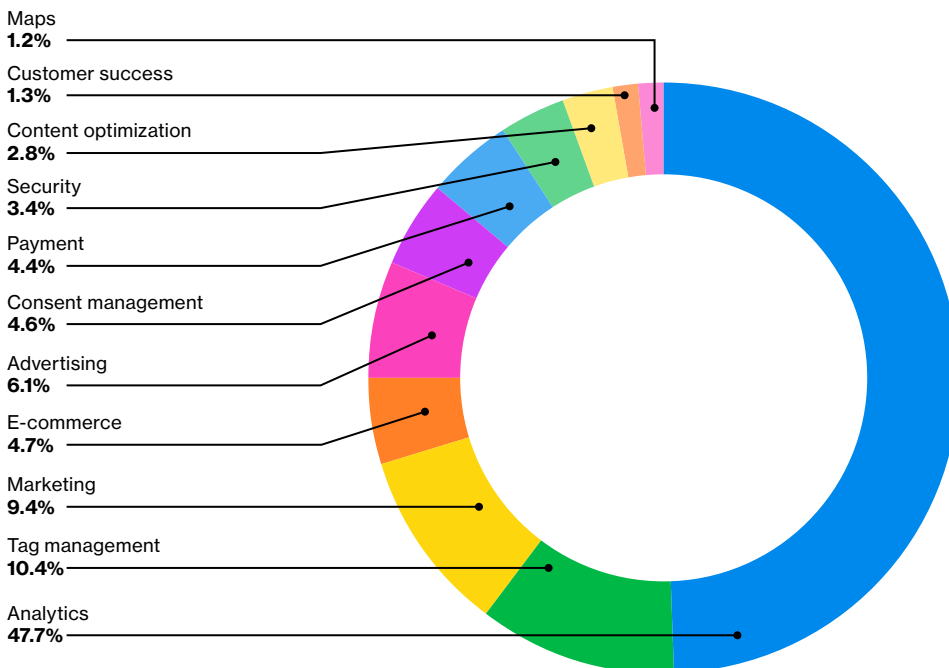## Most prevalent script categories

Maps
1.2%

Customer success
1.3%

Content optimization
2.8%

Security
3.4%

Payment
4.4%

Consent management
4.6%

Advertising
6.1%

E-commerce
4.7%

Marketing
9.4%

Tag management
10.4%

Analytics
47.7%

Figure 35. 7,075 unique websites from 6,342 companies

PCI DSS v4.0 implications of findings

The PCI DSS ensures that all companies that accept, process, store or transmit payment card information maintain a secure environment. The introduction of PCI DSS v4.0 brings more robust security measures and flexible compliance strategies to adapt to the evolving payment security landscape. Given the analysis of script usage across various industries, particularly those accessing PII, payment data and credentials, several implications are worth highlighting.

Increased scrutiny on third-party service providers

The reliance on third-party scripts, especially in industries such as apparel and fashion, which showed the highest volume of scripts accessing sensitive data, underscores the need for rigorous vendor management policies under PCI DSS v4.0. The PCI standard requires that entities maintain and manage a list of service providers with access to cardholder data (CHD), including the nature of the services provided and the responsibility for securing CHD. Given the analysis, businesses must ensure that their third-party scripts and service providers adhere to PCI DSS requirements to prevent data breaches and ensure compliance.

Enhanced focus on security of payment page scripts

The significant number of scripts accessing payment data indicates a potential risk area for PCI DSS compliance. Under PCI DSS v4.0, there is an enhanced focus on protecting the cardholder data environment (CDE) against unauthorized access, including client-side attacks such as formjacking and e-skimming. Companies must implement strong controls over scripts running on payment pages and within payment flows, with additional requirements to inventory, authorize, ensure integrity, turn on alerts and block all malicious activity related to these scripts.

Requirement for advanced monitoring and detection

With the high volume of scripts accessing sensitive data, the need for advanced monitoring and detection mechanisms is imperative to identify and mitigate threats in real time. PCI DSS v4.0 emphasizes the importance of promptly detecting and responding to security incidents. Businesses must deploy solutions capable of monitoring script behavior on client-side web applications, detecting anomalies and preventing data exfiltration attempts by malicious scripts.

Data protection and encryption

The analysis revealed that scripts are accessing a wide range of sensitive data, including PII, payment data and credentials. PCI DSS v4.0 mandates the encryption of transmission of CHD across open, public networks.

This extends to ensuring that any script or service that handles CHD must also employ strong encryption methods to protect data in transit and at rest, aligning with the PCI standard's requirements for robust encryption and key management practices.

Impact on risk assessment and mitigation strategies

Given the widespread use of scripts across industries, PCI DSS v4.0 requires entities to perform regular risk assessments to identify vulnerabilities within their payment processing systems, including those introduced by third-party scripts. The data highlights the need for a comprehensive risk management strategy that considers the variety of scripts accessing sensitive data, evaluating their necessity and implementing appropriate controls to mitigate identified risks.

Conclusion

In conclusion, the extensive use of third-party scripts across various industries, particularly those handling sensitive payment information, has significant implications for PCI DSS v4.0 compliance. Businesses must adopt a proactive approach to managing third-party risks, securing payment pages and payment flows, implementing advanced monitoring and detection capabilities, ensuring data protection, and conducting thorough risk assessments to maintain compliance with PCI DSS v4.0. Failure to address these issues not only poses a risk to data security but also jeopardizes an organization's compliance status, potentially leading to fines, reputational damage and loss of customer trust.

Source Defense data analysis findings

In the first quarter of 2024, Source Defense conducted its analysis and found:

- 7,075 unique websites from 6,342 companies

- Total number of third- and fourth-party scripts: 129,897

- Total number of scripts found on payment pages: 51,968

- Total number of scripts accessing PII: 17,002

- Scripts accessing payment data: 3,636

- Scripts accessing credentials data: 3,222

  - Average number of scripts per page: 18.37 (representing a 50% increase in script utilization since our 2023 analysis)

  - Average number of third-party scripts per page: 13.08

  - Average number of fourth-party scripts per page: 8.32 (previous data indicated two fourth parties—we are now seeing a fourfold increase)

  - Average number of scripts accessing PII: 2.40

  - Average number of scripts accessing payment data: 0.51

Most prevalent script types

The total number of script type occurrences is 36,356. The following script types, along with their percentage of the total, are arranged from highest to lowest:

1. Facebook Connect: 15.82%

2. Google Global Site Tag: 15.48%

3. Google Tag Manager: 15.47%

4. Google Analytics: 10.61%

5. Optanon: 6.32%

6. Pinterest Conversion Tracker: 5.98%

7. Universal Event Tracking (Bing): 5.32%

8. Klaviyo: 4.61%

9. Google Analytics—E-commerce: 4.51%

These script types are the most common in the dataset, indicating their widespread use across the analyzed websites. The presence of multiple analytics and tracking scripts (e.g., from Google, Facebook and Pinterest) suggests a strong focus on data collection and analysis in online platforms.

■ Scripts accessing payment data   □ Scripts accessing credentials data   ■ Scripts accessing PII data
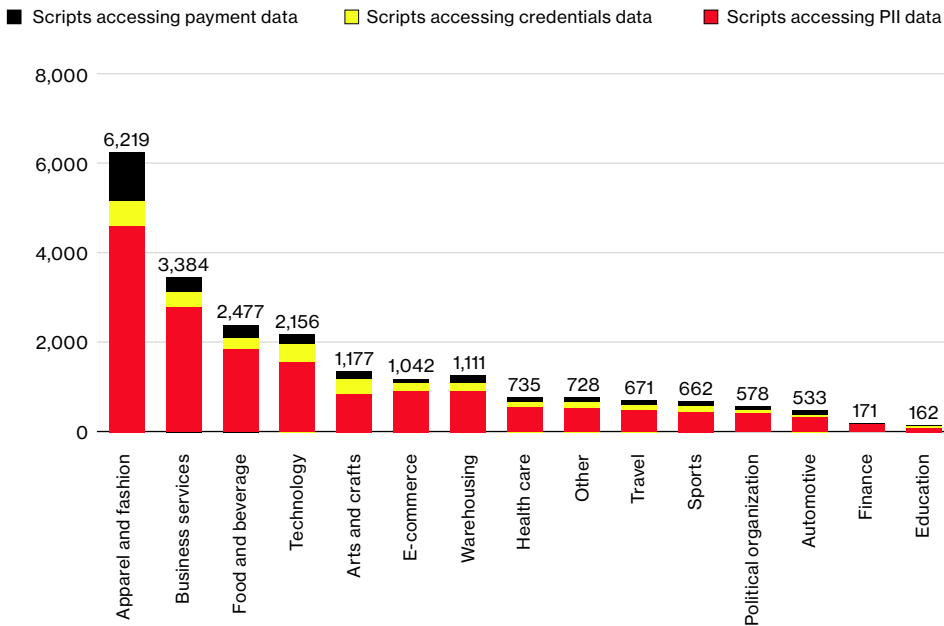
Figure 36. Number of web pages with scripts accessing PII, credentials and payment data

Top 15 industries overview ranked by total number of such scripts

1. Apparel and fashion | Total scripts: 81,850 (63% of the total, yet represented only 29% of the industry dataset); script origins include various analytics, marketing and customer engagement tools

2. Technology | Total scripts: 30,827 (24% of the total, yet represented only 14% of the industry dataset); script origins feature a mix of analytics, development tools and security services

3. Food and beverage | Total scripts: 27,518 (21% of the total, yet represented only 9% of the industry dataset); script origins include content delivery networks, marketing platforms and social media integrations

4. Business services | Total scripts: 23,629 (18% of the total, yet represented only 11% of the industry dataset); script origins range from customer relationship management to business analytics tools

5. Arts and crafts | Total scripts: 16,944 (13% of the total, yet represented only 7% of the industry dataset); script origins feature e-commerce platforms, analytics and marketing automation tools

6. E-commerce | Total scripts: 12,945 (10% of the total, yet represented only 6% of the industry dataset); script origins include payment processors, marketing tools and analytics services

7. Sports | Total scripts: 10,907 (8% of the total, yet represented only 5% of the industry dataset); script origins feature a mix of analytics, marketing and customer service tools

8. Warehousing | Total scripts: 9,420 (7% of the total, yet represented only 3% of the industry dataset); script origins include logistics and supply chain management tools, along with analytics

9. Travel | Total scripts: 8,191 (6% of the total, representing 3% of the industry dataset); script origins range from booking engines to customer feedback and analytics tools

10. Automotive | Total scripts: 7,030 (5% of the total, representing 3% of the industry dataset); script origins include dealer management systems, analytics and customer engagement platforms

11. Other | Total scripts: 6,678 (5% of the total); script origins feature a diverse range of tools tailored to specific industry needs

12. Health care | Total scripts: 4,431 (3% of the total, representing 2% of the industry dataset); script origins include patient management systems, analytics and health care compliance tools

13. Political organization | Total scripts: 4,217 (3% of the total, representing 2% of the industry dataset); script origins range from campaign management to voter engagement and analytics tools

14. Education | Total scripts: 2,243 (2% of the total, representing 1% of the industry dataset); script origins feature educational platforms, learning management systems and analytics

15. Finance | Total scripts: 1,246 (1% of the total, representing 1% of the industry dataset); script origins include banking systems, financial analytics and security tools

> 💡 **Script totals exceed 100% because many scripts are seen and used across multiple industries.**

Behaviors

Using first-party cookies:
28,715

Transferring data:
22,721

Using browser storage:
20,722

Executing risky actions:
4,586

Accessing PII data:
3,932

Accessing data:
3,538

Accessing PCI data:
987

Accessing credentials data:
830

Accessing GPS:
13

Loaded from blacklisted
domain: **5**

Sending data to blacklisted
domain: **3**

These behaviors range from common web functionalities, such as using cookies and browser storage, to more disconcerting actions such as executing risky actions and accessing sensitive data. The frequencies provide insight into how prevalent each behavior is within the dataset's context.

Client-side security risks associated with the most prevalent script types and PCI DSS v4.0 remedies

1. **Facebook Connect (5,838)**
   Risk: Data leakage through improper permissions or compromised application programming interface (API). Risk of oversharing user data or unauthorized access.

   PCI DSS v4.0: Limit data exposure to only what's necessary, monitor data access and usage, and ensure strict access controls and auditing.

2. **Google Global Site Tag (5,173)**
   Risk: Potential for sensitive information leakage or data exfiltration if misconfigured.

   PCI DSS v4.0: Ensure no capture or transmission of CHD, review and validate configurations regularly, and monitor for unauthorized data access.

3. **Google Tag Manager (5,709)**
   Risk: Can inject third-party scripts, leading to potential vulnerabilities if not secured or if third-party scripts are compromised.

   PCI DSS v4.0: Use strong user access controls, regularly monitor script changes, validate all third-party code and ensure that only authorized users can modify configurations.

4. **Google Analytics (3,914)**
   Risk: Could inadvertently capture personal or sensitive information if not configured correctly.

   PCI DSS v4.0: Ensure proper configuration to exclude any CHD from being captured, monitor data collection practices and regularly audit settings.

5. **Optanon (2,333)**
   Risk: Generally low risk, but misconfiguration can lead to compliance issues or unintentional data exposure.

   PCI DSS v4.0: Ensure that the script does not interfere with the secure handling of payment data and that consent preferences are respected and documented.

6. **Pinterest Conversion Tracker (2,205)**
   Risk: Tracks user interactions for marketing purposes, which could lead to data leakage if not configured correctly.

   PCI DSS v4.0: Ensure that no payment data is captured or processed by the tracker, regularly review data access and permissions, and monitor for unauthorized access.

7. **Universal Event Tracking (Bing) (1,963)**
   Risk: Similar to Google Analytics, tracking user behavior could lead to sensitive data exposure if misconfigured.

   PCI DSS v4.0: Verify that no CHD is captured, access only necessary information, and ensure regular monitoring and auditing of the tracking implementation.

8. **Klaviyo (1,700)**
   Risk: Manages and analyzes customer data for targeted campaigns, which involves data storage and processing, potentially introducing risks of unauthorized access or data leakage.

   PCI DSS v4.0: Ensure that Klaviyo does not store, process or transmit CHD unless it's absolutely necessary and secure. Implement strict data access controls and regular audits.

9. **Google Analytics – E-commerce (1,663)**
   Risk: Specifically designed for e-commerce analytics, but if misconfigured, could lead to sensitive data exposure.

   PCI DSS v4.0: Regularly audit and monitor data collection to ensure that no CHD is being captured or transmitted, and maintain strict access controls.

Top 10 domains based on various script categories, highlighting key trends in the dataset

- **Total scripts on page:** Shows domains with the highest total number of scripts (third- and fourth-party scripts combined). This indicates the overall load and potential complexity of interactions on these domain pages.

- **Third-party scripts:** Highlights domains with the highest number of third-party scripts. These scripts are typically used for various functionalities, including analytics, advertising and customer support tools.

- **Fourth-party scripts:** Focuses on domains with the highest number of fourth-party scripts, which are scripts called by third-party services. Their presence can indicate deeper levels of dependencies and potential security concerns.

- **Scripts accessing payment data:** Shows the domains with the most scripts accessing payment data, pointing to potential areas of vulnerability or increased security measures for handling sensitive financial information.

- **Scripts accessing PII:** Identifies the domains with the highest number of scripts accessing PII, highlighting privacy implications and the need for robust data protection practices.

These trends offer insights into the security, privacy and operational practices of the domains in question, revealing potential areas for further investigation, optimization or security enhancements.

Appendix B:
A deeper dive into PCI security performance measurement and evaluation

By Ciske van Oosten
Head of Global Business Intelligence
Verizon Cyber Security Consulting

Measuring the performance and evaluating the effectiveness of your organization's PCI data security and compliance efforts are essential to their long-term success. The importance and value of measuring management performance is indisputable. By assessing various PCI security operations metrics, you can make informed decisions and find ways to establish and improve visibility, accountability and a clear path forward. Despite these benefits, many businesses experience difficulty determining what and how to measure and report for internal decision-making. If you want to help your organization achieve its PCI security and compliance objectives and overall goal, this appendix presents additional guidance on how to construct a performance measurement and evaluation program.

For an overview on how metrics can facilitate better awareness and decision-making, it's recommended that readers read the 2019 Payment Security Report, pages 21 through 29. It explains how a comprehensive metrics-driven evaluation program can provide a consistent and repeatable framework for the analysis of complex situations and a mechanism for identifying broken PCI security compliance management processes or unusual activity. This allows executives and managers to monitor performance and identify corrective actions.

Since the release of PCI DSS v4.0, the requirements place greater emphasis on objective-based, evidence-backed continual compliance. To meet the new and updated requirements, organizations will need to make changes to improve their data security and compliance processes and capabilities—including the scope of what they measure, document and report. Some requirements are minor and require incremental changes; others require substantial effort depending on the existing maturity of the compliance management capabilities.

Although many organizations have improved their capabilities over time, relatively few have progressed to sufficiently mature PCI compliance management capabilities and processes.

Essential PCI DSS v4.0 program evaluation

- What is the reality of evaluating PCI security programs? Are organizations getting it right?

- What should organizations do to improve program evaluation since PCI DSS v4.0 became mandatory?

- How can organizations develop their PCI security evaluation programs and formalize them?

PCI DSS v4.0x performance measurement and improvement

Performance measurement and improvement are systematic processes by which an organization continually and consistently tracks and applies important program and operations metrics. The data is an essential input to optimize the organization's capability to efficiently and effectively advance sustainable payment card data security. These processes enable continual learning and improvement. They provide substantial support to help organizations achieve better PCI security program results.

By measuring, evaluating and reporting security program performance (as an internal capability), organizations can:

- Ensure that programs or initiatives are implemented as designed. Often the reality of a security control environment differs vastly from design and implementation expectations.

- Track progress toward, and be held accountable for, meeting and maintaining compliance with PCI DSS requirements.

- Communicate progress and successes internally and externally. The process and output of a PCI security performance measurement and evaluation program brings evidence to bear in decision-making and is a critical component of effective and efficient security governance.

- Learn to achieve even better results by analyzing insights. Organizations that formalize the process of evaluating PCI security program performance gain substantial benefits over time and valuable insights about program effectiveness, improving economic return on their PCI security compliance investments.

Improving performance through measurement: The Hawthorne effect

When people become aware that they are subjects being evaluated, the attention they receive from the evaluation often causes them to change their conduct. The mere experience of being observed and feeling valued significantly affects worker performance independent from physical work conditions. This tendency is based on the so-called Hawthorne effect, which is also observed in security compliance management.

The Hawthorne effect
The phenomenon is named after a set of studies conducted between 1924 and 1932 at Western Electric's Hawthorne Works located outside of Chicago in the United S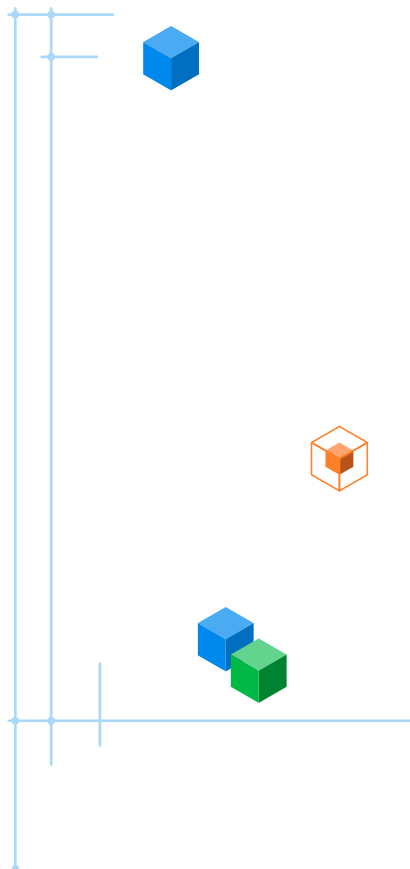tates. To examine its effect on worker productivity, work conditions were altered—such as variations in office lighting. The researchers noticed that employee productivity increased not only in improved conditions but also in inferior conditions. Productivity only decreased when the study ended, leading researchers to conclude that the productivity gain was a result of workers thinking they were being monitored individually.

Similarly, in the context of PCI security compliance management, teams and individuals tend to alter their behavior in response to an awareness of being observed and their performance being evaluated, resulting in higher levels of performance and compliance with PCI security requirements.

Performance measurement vs. evaluation

Performance measurement and evaluation help stakeholders (such as board members, executives, CISOs, risk managers, and compliance program managers) understand how well the PCI security strategy and program are working, develop systematic evidence, and identify possible improvements. They serve as methods for systematic assessment to facilitate learning about, and improving the results of, security compliance activities. Both evaluation and performance measurement generate the required evidence. Yet important differences exist between these methods.

Performance measurement	Evaluation
Definition Ongoing collection, monitoring, reviewing and reporting of PCI security program and compliance data on preselected measures and activity outcomes. Measurement weighs and examines elements against an explicit or implicit yardstick with a comparison against an explicit standard. The measurement process requires systematic collection of data about program activities, characteristics and outcomes. These are needed for input to make judgments about the program, improve program effectiveness and/or inform decisions about future changes.	**Definition** Evaluation is the systematic process to examine how well all or part of the PCI security compliance program is working and to determine its merit, worth, value and significance. Evaluation applies the methods to action programs to obtain objective and valid measures of what such programs are accomplishing, the kinds of change desired, the means by which this change is to be brought about and the signs by which such changes are recognized.
Purpose • Measuring progress toward preestablished goals and targets: including scope of PCI DSS control implementation, maintenance, control effectiveness and sustainability • Determining whether an activity is achieving its stated output/outcome objectives; making adjustments if it isn't • Serving as an early alert system in case of significant changes in operations	**Purpose** • Assessing the efficiency and effectiveness of a program, or an individual project within the program, as compared to its absence—or to one or more alternative approaches • Establishing a causal relationship between an activity and the outcomes experienced by those affected by it • Addressing questions about contextual factors, variations in effectiveness across different settings or populations, and implementation
Data and analysis • Data is largely quantitative, typically expressed as a percentage. • Data points are assessed against targets or compared to previous data for the same measure in order to detect trends over time.	**Data and analysis** • Data and analytical techniques are guided by the evaluation questions. • They generally include both quantitative and qualitative data. • In the case of causal studies, they require complex methods to isolate impacts from other influences.

Limitations of PCI DSS v4.0

The PCI DSS has always been and remains a security control framework. It's neither a program, risk management nor governance framework. Figure 37 indicates some aspects of compliance management that receive little or no coverage in PCI DSS v4.0. Organizations must implement additional complementary external or internal frameworks and standards.

Measuring PCI DSS controls alone is not enough

The 2019 Payment Security Report, pages 21 through 25, briefly explains how to use metrics for measuring control performance. We mentioned that many organizations only measure the number of implemented PCI DSS requirements (control coverage) and their control status (such as in place, not in place and compensated).

We recommended broadening PCI security program metrics to also include repeat measurements of the following governance, management, operational and technical control processes:

- **Business (governance) processes:** Business and compliance goals and objectives, high-level business and security strategy and alignment, communication processes, business governance, resource allocation and expenditure

- **Management control processes:** Data security and compliance management strategy; security and compliance policies; standards;

PCI DSS v4.0	Yes	No	Depends
Stricter requirements and numerous new and updated requirements	X		
Enhanced validation reporting requirements	X		
Improved risk management requirements	X		
More flexibility on control design and implementation			X
Increased evidence of compliance validation	X		
Compliance program management performance reporting		X	
Explicit requirements for security control effectiveness evaluation and reporting			X
Explicit performance metrics/key performance indicator requirements—including control strength		X	
Comprehensive compliance program design requirements		X	

Figure 37. Limitations of PCI DSS v4.0

procedures; improvement plans; management communication and reviews; and risk treatment processes, incident preparedness and response

- **Operational control processes:** Operational procedures, control environment design, control environment implementation and review, capacity management, change control, supply chain, recruitment, risk assessment

- **Technical control processes**: IT support processes, configuration management, system hardening, vulnerability management, software patch management, access control, antivirus controls, intrusion detection systems, firewalls, content filtering processes

What else should be measured, reported and improved?

In the content below, we suggest a series of additional metrics to track control performance at a process level to measure and report on various performance areas, such as resource utilization, quality, efficiency, throughput, variance and effectiveness of PCI security compliance activities.

Control performance metrics

Control performance metrics can and should be broadened to include control effectiveness, performance and impact metrics.

- Control coverage measures the deployment status of a control requirement across a total population of in-scope components and requirements.

- Control effectiveness measures the extent to which controls are designed, implemented and supported by processes to achieve their intended outcomes (such as robustness and resilience).

- Operational performance measures the number and severity of deviations from performance standards and the speed at which teams correct them (control reliability and sustainability).

- Program impact metrics convey the impact of the compliance program on the organization's mission (e.g., program milestone reporting that provides ongoing progress toward objectives and a strategic goal).

What other types of metrics and KPIs can be used to measure processes?

Security and compliance process metrics can be broadly categorized into five types:

- Process efficiency metrics measure the resources used in completing a security compliance process to reduce waste of resources (people, time, attention, effort, budget).

- Process variance metrics measure variation in standard processes over time.

- Process effectiveness metrics measure the success of a process in achieving its desired outcome.

- Process control metrics evaluate conformance to business rules and regulatory standards.

- Continual improvement metrics measure the effect of process improvements over a longer time period or against agreed-on objectives.

Measurements vs. metrics vs. KPIs

While often used interchangeably, key performance indicators (KPIs), process metrics and measurements are slightly different. Measurement refers to a specific, single, point-in-time snapshot of raw data. Metrics are typically much broader and include various data points used for analysis. Metrics compare predetermined baselines against a series of measurements taken over time and provide objective interpretations of the data collected through the measurement process. Metrics may not always directly align with key objectives.

Process metrics, for example, are specific measures that focus on the performance of particular business processes. They monitor and evaluate the efficiency, effectiveness and flexibility of a process, helping identify where improvements are needed. KPIs can be seen as a subset of metrics, often tied directly to the organization's strategic objectives and typically within a defined time frame, such as monthly or quarterly targets. KPIs are directly tied to strategic goals, and they're used for measuring performance against set objectives.

Evaluating efficiency

Organizations should develop and apply efficiency metrics to measure the performance and productivity of all critical security program and compliance processes. It's essential to evaluate how well a process uses resources—including time, money and people—to deliver economical outputs.

Leading vs. lagging indicators

Tracking performance measurement trends can provide indicators for future performance—when past performance provides an indication of future performance or the measures used are leading rather than lagging.

Lagging measures also are referred to as tombstone measures, which indicate only what has happened in the past. Leading measures provide some indication of future performance—but of course without the certainty that hindsight provides.

PCI security program process efficiency metrics

By evaluating these metrics, organizations should identify areas where waste can be reduced and process speed can be increased. Examples of efficiency metrics include:

- **Cycle time:** This is the total time taken to complete a security compliance process from start to finish—a shorter cycle time may signify a more efficient process.

- **Resource utilization:** This measures the percentage of available resources used in a security compliance process—higher utilization generally signifies more efficient use of resources.

- **Cost per activity:** This measures the total cost to carry out a process for each activity (related project tasks). By reducing this cost, organizations can increase the profitability of each project.

Evaluating processes

Compliance program managers should consider incorporating the following four categories of metrics for evaluating PCI security program management and operational processes: process control, process variance, process effectiveness and improvement metrics.

PCI security process control metrics

Control metrics are used to monitor compliance and conformance within a business process.

They help ensure that processes are operating within acceptable parameters and complying with relevant regulations and standards. Examples of control metrics include:

- **Compliance rate:** Measures the extent to which a security compliance process complies with a set of standard rules or regulations. A higher compliance rate indicates a more controlled process.

- **Risk incidents:** Measures the number of times risks identified in a security compliance process occurred. Fewer risk incidents imply a better-controlled process.

PCI security process variance metrics

Variance metrics evaluate the consistency of a process. They measure the difference between the actual process performance and the expected or standard performance. By analyzing variance metrics, businesses can understand the degree of unpredictability or risk in a process. Examples of variance metrics include:

- **Standard deviation:** Measures the amount of variation or dispersion in a set of values. A low standard deviation indicates that the values are close to the mean, implying a more consistent process.

- **Range:** The difference between the highest and lowest values in a set. A smaller range suggests less variance and more consistency in the process. The Pareto principle can visualize range in process performance, where typically 80% of outcomes are resulting from 20% of causes.

PCI security process effectiveness metrics

Effectiveness metrics measure the ability of a process to achieve its intended results. They focus on the quality and outcomes of a process rather than its efficiency. Examples of effectiveness metrics include:

- **Error rate:** Measures the number of errors or defects produced during a process. A lower error rate suggests a more effective process.

- **Quality rate:** The proportion of output that meets a specified quality standard. A higher quality rate suggests a more effective process.

Continual improvement metrics

Improvement metrics assess the effect of changes made to multiple security compliance processes. They help quantify the benefits of process improvements, which can include cost savings, improved efficiency, better quality or higher customer satisfaction. Examples of continual improvement metrics include:

- **Cost:** Measures the cost efficiency or effective savings realized from implementing process improvements. Total cost of ownership calculations or should-cost modeling can help analyze and drive the cost benefits of continual improvement.

- **Improvement in cycle time:** Measures the decrease in cycle time after implementing improvements. A larger decrease in cycle time indicates more effective improvements.

- **Reduction in error rate:** Measures the decrease in error rate after implementing improvements. A larger reduction indicates more effective improvements. In services, error rate can also be measured by the amount of rework.

Setting direction and tracking performance — using a logical process

It is important to have the right people engaged and assign appropriate responsibilities to individuals and teams that design and govern PCI security compliance management evaluation programs. In smaller organizations, it's common for executive leadership to be involved in setting strategy as well as the direct, hands-on management and measurement of the operation performance of PCI security compliance programs.

In general, for midsize and large organizations, it shouldn't be the organization's executive leadership (such as the company board) that establishes process metrics because they are responsible for setting the overall strategy. Executives communicate the security strategy and test whether it's being measured and effectively delivered in operations. Therefore, successful organizations know how to abstract performance indicators with a clearly defined set of metrics that help ensure that strategy is being delivered. The lower-level operational metrics need to align with the data security strategy built across the organization to help ensure that all participants are focused on the right objectives and tasks.[33]

Performance measurement communication should remain focused on tracking actual progress made toward achieving the overall goal of PCI security compliance. It's far too common for PCI security management reports, and verbal communication during meetings and presentations, to quickly get lost in the weeds by spending too much time on lower-level compliance metrics. Instead, remain focused on the bigger picture: reporting strategic KPIs that evaluate management performance, i.e., how well the PCI security program is actually progressing as a direct result of the logical design and execution (follow-through) of strategic governance and management plans and actions.

---

33   The section "What other types of metrics and KPIs can be used to measure processes?" that starts in this report on page 101 is adapted from "How to effectively use process metrics in business process analysis," Workfellow (now ProcessMaker). https://www.workfellow.ai/blog/how-to-use-process-metrics-in-business-process-analysis

The Logical Thinking Process

How do you determine the order of steps to plan, design and execute a formal PCI security program evaluation? The construction of PCI security program evaluation and performance measurement plans can benefit from the application of The Logical Thinking Process (LTP). The method is based on the Theory of Constraints (TOC) developed by Dr. Eliyahu Goldratt[34] and was later enhanced by H. William Dettmer.[35] The framework comprises five separate logic trees. Each one has a specific purpose designed to help organizational teams make better decisions. The LTP adheres to logical principles that apply to each step of the process. We introduced this process in the 2022 Payment Security Report— see page 74.

This Five Trees approach has multiple uses and can help guide performance evaluation. It presents a step-by-step, workable course of action by finding a fully implemented solution for an ill-defined problem. It analyzes what is needed to achieve the assigned goal of the PCI security program, assessing the situation versus required conditions and communicating what needs to be done, in which order and why.

"

The maturity of a compliance program[36] provides a window into how serious an organization is about protecting data. How an organization invests in the improvement of data protection capabilities and progress toward optimized processes can be a barometer for security success."

2019 Payment Security Report, page 19

We explain this method and each of the five trees extensively in the 2022 Payment Security Report, pages 74 through 79.

Conclusion

Many organizations need to and would like to improve the performance and outcomes of their PCI security programs and the capabilities of the program participants. They need to maintain visibility of the actual efforts and impact that individuals, teams, processes and IT systems components make toward the achievement of their PCI security management performance objectives and the overall program goal. Organizations can benefit significantly from learning and applying the methods and practices we previously reviewed

to know what to include in performance measurement and evaluation projects and how to construct and execute them.

Most of these data collection and measurement activities can and should be automated with the use of compliance management application software. This can help ensure that the correct measurements are frequently performed using the most relevant metrics. Management software helps make the process as consistent, timely and repeatable as possible. It facilitates and simplifies clear, actionable reporting to inform decision-makers what the next five moves should be during each step of the security compliance management journey.

Step 1	Step 2	Step 3	Step 4	Step 5
The Goal Tree	**The Current Reality (Problem) Tree**	**Conflict Resolution (Evaporation Cloud) Diagram**	**The Future Reality (Solution) Tree**	**The Prerequisite (Implementation) Tree**
What is the goal?	What is the problem?	Which assumptions are invalid?	What is the solution?	How to implement it?

Figure 38. Application of the Five Logical Trees

34 Eliyahu M. Goldratt and Jeff Cox, "The Goal: A Process of Ongoing Improvement," North River Press, 2004.
35 H. William Dettmer, "Goldratt's Theory of Constraints: A Systems Approach to Continuous Improvement," American Society for Quality (ASQ) Press, 1997.
36 See pages 40 and 41 in this publication to understand the limitations of using maturity models for improving PCI security performance.

Appendix C: PCI DSS compliance schedule

By Sung Chae and Yan Bao Jackson Wee
Qualified Security Assessors
Verizon Cyber Security Consulting

The Payment Card Industry Data Security Standard (PCI DSS) v4.0[37] contains 250 requirements and 464 testing procedures. Thirteen new requirements went into effect on April 1, 2024; 51 requirements will go into effect in April 2025.

Key Requirements	Requirements	Test procedures
Requirement 1	19	35
Requirement 2	11	27
Requirement 3	29	55
Requirement 4	6	12
Requirement 5	13	25
Requirement 6	19	35
Requirement 7	12	22
Requirement 8	29	52
Requirement 9	27	56
Requirement 10	27	38
Requirement 11	21	51
Requirement 12	37	56
Total	**250**	**464**

Factoid: A typical assessment of a PCI DSS control environment to determine the state of compliance for all PCI DSS requirements requires approximately 836 validation steps (such as documentation reviews, interviews, configuration analyses, physical inspections and requirement evaluations).

This PCI DSS compliance schedule that begins on page 107 outlines a structure of activities to conduct throughout the year to support ongoing compliance. This table maps out key tasks (such as quarterly vulnerability scans and annual penetration testing) with their minimum frequency, action items, resource needs and justifications. By adhering to the PCI DSS recommended compliance schedule for applicable controls that must be performed at various times throughout the year, organizations systematically address many PCI requirements and enhance their security practice. This enhances organizations' preparation for their annual PCI DSS assessment. However, additional continual efforts and proactive measures are necessary to address the PCI security requirements and maintain a mature security practice. This proactive approach helps mitigate risks, safeguard cardholder data (CHD) and maintain customer trust.

37   "Payment Card Industry Data Security Standard: Requirements and testing procedures Version 4.0," PCI Security Standards Council, March 2022.
     https://www.pcisecuritystandards.org/document_library

PCI DSS version	1.1	2.0	3.2	3.2.1	4.0
Released (year)	2006	2010	2016	2018	2022
Number of pages	17	75	139	139	360
Control objectives	6	6	6	6	6
Key requirements	12	12	12	12	12
Total base controls	64	62	79	79	63
Total requirements	207	211	251	252	250
Test procedures	-	338	415	417	464

Time frames in PCI DSS Requirements	Descriptions and examples
Daily	Every day of the year (not only on business days)
Weekly	At least once every 7 days
Monthly	At least once every 30 to 31 days, or on the nth day of the month
Every 3 months (quarterly)	At least once every 90 to 92 days, or on the nth day of each third month
Every 6 months	At least once every 180 to 184 days, or on the nth day of each sixth month
Every 12 months (annually)	At least once every 365 (or 366 for leap years) days or on the same date every year
Periodically	Frequency of occurrence is at the entity's discretion and is documented and supported by the entity's risk analysis. The entity must demonstrate that the frequency is appropriate for the activity to be effective and to meet the intent of the requirement.
Immediately	Without delay; in real time or near real time
Promptly	As soon as reasonably possible

Figure 39. As appears on page 25 of the PCI DSS v4.0

Frequency/ Requirement	Action items	Resources	Justifications
Every 12 months 6.2.2	Train software development personnel on software security.	**Human resources** Low: Ample training materials are available; numerous industry training providers offer such programs.	Having staff knowledgeable in secure coding methods helps minimize the number of security vulnerabilities introduced through poor coding practices.
		Financial resources Medium: This may require additional budget, resources and management approval because employees may be absent from regular work for training duration.	
Every 12 months 9.4.1.2	Review the security of offline media backup locations with CHD.	**Human resources** High: The review process may require a significant amount of time based on the number of off-site storage locations; trained personnel should do the reviews.	Conducting regular reviews of storage facilities enables organizations to promptly identify and address security issues.
		Financial resources Medium: Travel and required remediation costs will likely be incurred; outsourcing the review or using a third-party location may result in extra costs but may reduce the overall resource requirements.	
Every 12 months 9.4.5.1	Conduct inventories of electronic media with CHD.	**Human resources** Medium: IT staff is required to locate, track and conduct inventories of electronic media.	Conducting reviews of electronic media inventory reduces the risk of stolen or missing electronic media going unnoticed.
		Financial resources Low: May require minor documentation of costs and recordkeeping unless inventory management software is purchased.	
Every 12 months 11.4.2 11.4.3 11.4.5	Conduct internal and external penetration tests as well as network segmentation tests.	**Human resources** Medium: Personnel with specialized expertise in ethical hacking and penetration testing are required.	Testing helps discover vulnerabilities and misconfigurations that could be used by an attacker.
		Financial resources Medium: Costs may be incurred if a security firm is engaged to perform activities; there are also potential remediation or security upgrade costs.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Every 12 months 12.1.2	Review the information security policy.	**Human resources** Low: Additional personnel from management, legal, IT security and other teams may be needed to review and discuss industry updates, regulations and compliance requirements. Efforts to update, document and communicate policy changes may also be needed. **Financial resources** Low: Usually little to no additional costs are required in this process. Investment may be needed for policies to remain aligned with changes to the control environment and other changes across the organization.	This review helps ensure that relevant changes or new measures to defend against emerging threats are addressed.
Every 12 months 12.3.1	Perform a review of each targeted risk analysis at least once every 12 months to determine whether results are still valid or updated risk analysis is needed.	**Human resources** Low: Some collaboration effort is required across various IT teams but only for controls with a targeted risk analysis. **Financial resources** Low: The review has little to no financial cost other than a minimal potential cost for risk management tools or software.	The review helps define how frequently an activity is performed based on the risk to the environment and helps ensure validity and consistency with policies and procedures.
Every 12 months 12.3.2	Perform a targeted analysis of risk at least once every 12 months.	**Human resources** Low: The analysis requires collaboration effort across various IT teams but only for those controls that require a targeted risk analysis. **Financial resources** Low: The review has low to no financial cost other than a minimal potential cost for risk management tools or software.	This analysis helps ensure that controls meet or exceed the security provided.
Every 12 months 12.3.3	Review documented cryptographic cipher suites and protocols in use.	**Human resources** Medium: Dedicated staff with expertise in IT security are needed to monitor any changes; various IT teams will need to thoroughly analyze, test and implement new or updated cryptographic cipher suites and protocols. **Financial resources** Medium: Additional consulting costs to analyze, test and implement new or updated cryptographic cipher suites and protocols may be incurred.	The review helps organizations detect security weaknesses associated with deprecated protocols/encryption or design flaws.

🟩 Low   🟨 Medium   🟧 High

Frequency/ Requirement	Action items	Resources		Justifications
Every 12 months 12.3.4	Review hardware and software technologies in use.	**Human resources** Low: Minimal efforts should be required because existing resources can review vendor updates, technology changes and emerging threats for leveraged technologies.		This review helps ensure awareness of changes to technologies in use and evolving threats to those technologies.
		Financial resources Low: The review requires little to no cost because meetings can be scheduled periodically with vendors of acquired technologies to stay current with emerging technology and threats.		
Every 12 months 12.5.2	Review the documented PCI DSS scope.	**Human resources** Low: The review process generally uses existing human resources, but IT security professionals with PCI DSS know-how must ensure an accurate evaluation of the documented scope.		This review helps validate PCI DSS scope and helps ensure that it remains up to date and aligned with infrastructure and business changes.
		Financial resources Low: The review requires little to no additional financial cost; the task is essential for maintaining compliance and ensuring CHD security.		
Every 12 months 12.6.2	Review the security awareness program to address any new threats and vulnerabilities.	**Human resources** Low: This requires minimal IT security team head count and is generally restricted to making updates and refinements to existing training materials.		This review helps ensure that training received by personnel is up to date and references the current threat environment.
		Financial resources Low: No significant consulting or expertise cost is generally incurred; existing resources can update training materials.		
Every 12 months 12.6.3	Conduct security awareness training for personnel; document personnel acknowledgment that security policies and procedures are understood.	**Human resources** Low: This activity requires minimal dedicated staff; existing training materials and resources can be used, including personnel acknowledgment documentation.		Personnel training helps reinforce the importance of information security and staff's role in protecting the organization.
		Financial resources Low: Apart from the initial investment in digital security training platforms, this should require little to no additional cost for external consulting.		

🟩 Low　🟨 Medium　🟧 High

Frequency/ Requirement	Action items	Resources	Justifications
Every 12 months 12.8.4	Monitor third-party service provider (TPSP) PCI DSS compliance status.	**Human resources** Low: This requires minimal effort, but it may require staff with PCI DSS knowledge. It also requires time to review compliance documentation and coordinate with providers to gather information and resolve issues.	Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness regarding compliance with applicable requirements for services they perform on behalf of an organization.
		Financial resources Medium: Potential costs may be incurred to remediate noncompliant service providers, extend the PCI scope to include service providers or change to a PCI DSS-compliant provider.	
Every 12 months 12.10.2	Review and test the security incident response to ensure that processes remain viable and personnel are familiar with the plan.	**Human resources** Medium: Time may be required to review and update plans, coordinate testing and conduct training; it may require additional head count for collaboration with teams and stakeholders.	Reviews will identify weak processes and missing steps that could result in delays in containment and increase exposure during incidents; reviews help ensure that relevant personnel are familiar with incident response plans.
		Financial resources Medium: Additional costs may be incurred for training and external consulting to ensure that relevant personnel are familiar with the incident response plan and industry best practices to handle different scenarios.	
Every 6 months 1.2.7	Review configurations of network security controls (NSCs) to confirm that they are relevant and effective.	**Human resources** Low: The review requires minimal head count, using existing resources to review configurations; it may require support from IT staff with network security knowledge.	This review helps clean up unneeded, outdated or incorrect rules or configurations that could be exploited; it helps ensure that rules and configurations only allow authorized services, protocols and ports that match a documented business justification.
		Financial resources Low: There is little to no cost because existing resources are used to review configurations; added costs may be incurred if reviews use tools and software.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Every 6 months 7.2.4	Review all user accounts and related access privileges, including third-party/ vendor accounts.	**Human resources** Low: This requires various teams within IT to document all user accounts and access levels as well as update and revoke access as needed. **Financial resources** Low: The review requires little to no cost because it uses existing resources; minor expenses might include tools and software to support the review process.	This review helps detect excessive access rights remaining after user job responsibilities change, system functions change or other modifications are made; it helps ensure that accounts for all terminated users and third parties that no longer need access are revoked.
Every 6 months 11.4.6	Conduct a network segmentation test (service providers only).	**Human resources** Medium: Personnel with specialized expertise and advanced training in ethical hacking and penetration testing are required. **Financial resources** Medium: This activity may require costs to engage an external security company to perform activities; potential costs also may be incurred for remediation or security upgrades.	This testing can help detect poorly designed segmentation controls before they can be exploited by threat actors attempting to pivot laterally from an out-of-scope, untrusted network into the cardholder data environment (CDE).
Every 6 months 12.5.2.1	Service providers should review the documented PCI DSS scope every 6 months.	**Human resources** Low: The review process generally uses existing personnel resources, but IT security professionals with knowledge of PCI DSS are required to ensure accurate evaluation of the documented scope. **Financial resources** Low: Little to no significant additional financial cost is required; this task is essential for maintaining compliance and ensuring the security of CHD.	Service providers typically access greater volumes of CHD and have larger and more complex networks than merchants, resulting in a much larger impact if compromised; reviews help validate PCI DSS scope accuracy and help ensure that the scope remains up to date and aids in the discovery of overlooked changes.
Every 3 months 3.2.1	Verify that stored account data exceeding the defined retention period is securely deleted or rendered unrecoverable.	**Human resources** Medium: Head count is required to locate and document stored account data location, account data exceeding the retention period and associated secure deletion methods and procedures. **Financial resources** Low: There is a potential cost for data erasing tools.	This activity helps ensure that storage of CHD and sensitive authentication data prior to the completion of the authorization process is kept to a minimum and is only retained for a defined amount of time.

🟩 Low   🟨 Medium   🟧 High

Frequency/ Requirement	Action items	Resources	Justifications
Every 3 months 11.2.1	Test, detect and identify authorized and unauthorized wireless access points.	**Human resources** Low: This requires IT network professionals with knowledge of the network to perform scans and immediately respond to the introduction of rogue wireless access points.	Detecting and removing unauthorized access points reduces the duration of an attack and the likelihood of rogue devices being leveraged for an attack.
		Financial resources Medium: Costs may be incurred for wireless scanning tools or security services as well as potential remediation or security upgrades.	
Every 3 months 11.3.1 11.3.2	Conduct internal and external vulnerability scans; external scans must be performed by an Approved Scanning Vendor (ASV).	**Human resources** Medium: This requires IT security professionals with experience in vulnerability scanning tools and techniques. External service providers may be needed to perform scanning services using authorized scanning solutions.	Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or CHD.
		Financial resources Medium: Costs may be incurred for vulnerability scanning tools and for the labor of IT security professionals; potential costs for remediation or security upgrades are also possible.	
Every 3 months 12.4.2	Service providers conduct independent reviews to confirm that personnel are performing their tasks in accordance with security policies and procedures.	**Human resources** Medium: Independent head count with PCI DSS/ IT audit methodologies experience may be required to conduct reviews, analyze data and report document findings.	These reviews provide assurance that expected controls are active and working as intended.
		Financial resources High: May incur labor costs for internal auditors, compliance professionals and independent security professionals; potential remediation or security upgrade costs are also possible.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Within one month 6.3.3	Install critical or high security patches/ updates within one month of release.	**Human resources** Medium: IT professionals with necessary skills and expertise are required as the effort could span different technologies; this routine maintenance activity can be managed with existing staff.	Organizations can quickly address vulnerabilities, enhancing their security posture and reducing the likelihood of successful cyberattacks.
		Financial resources Low: This activity may require some financial investment, including software licenses or subscription fees, potential hardware upgrades or replacement, and consulting fees for some technology specialized expertise (if needed).	
Weekly 11.5.2	Perform critical file comparisons and alert personnel for any unauthorized modifications.	**Human resources** Medium: IT security professionals with experience in file integrity monitoring (FIM) may be required to configure and maintain file comparison tools, analyze results and identify potential security incidents.	Comparisons will detect and evaluate changes to critical files and generate alerts indicating a threat actor may have compromised a system in the CDE.
		Financial resources High: This activity may require costs for security incident and event management (SIEM) systems, log management tools, incident response, or remediation; could incur potential costs if it's necessary to outsource to a managed security service provider (MSSP) if lacking head count or expertise.	
Daily 10.4.1	Review audit logs to identify suspicious or anomalous activities.	**Human resources** High: This activity requires IT security professionals with experience in SIEM systems to identify and investigate potential security incidents.	Many breaches occur months before being detected. Regular log reviews mean that incidents can be quickly identified and proactively addressed.
		Financial resources High: This may require costs for SIEM systems, log management tools, incident response or remediation; potentially could outsource to an MSSP if head count or expertise are lacking.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Immediately 2.2.1	Properly configure and harden all system components before or immediately after they connect to production environments.	**Human resources** Medium: This requires dedicated staff (specialized IT security and system administration expertise); other time-consuming tasks include configuration review, vulnerability scanning and penetration testing; ongoing monitoring is required to ensure that security and compliance continue. **Financial resources** High: A high cost is associated with this process; it requires security tools or security services, such as vulnerability scans and penetration tests.	Configuring and hardening system components before they are introduced into the production environment helps ensure that they are secure from the outset, reducing vulnerabilities and protecting against potential cyberattacks and data breaches.
Immediately 6.4.1 6.4.2	Use an automated technical solution (e.g., a web application firewall [WAF]) to protect public-facing web applications configured to block web-based attacks or to generate alerts that must be immediately investigated.	**Human resources** Medium: This requires IT security staff with specialized expertise to configure a WAF and analyze threats coming from security logs and alerts. The process is usually time-consuming for initial setup and fine-tuning WAF rules. Ongoing monitoring and analysis of WAF logs and alerts also requires dedicated resources. **Financial resources** Medium: A potential financial cost may be required for software or cloud service; external consulting; and maintenance, updates and support.	Web-based attacks must be investigated immediately to quickly identify and mitigate damages and protect sensitive data from potential theft or compromise.
Immediately 8.2.5	Revoke access for terminated users immediately.	**Human resources** Low: This requires IT staff with access control responsibilities (such as system administrators); some effort may be required for timely human resources (HR) coordination. **Financial resources** Low: This activity requires little to no cost; it primarily relies on existing resources such as an access control system.	Revoking user access immediately on termination is a proactive measure to enhance security and prevent sabotage.

🟩 Low   🟨 Medium   🟧 High

Frequency/ Requirement	Action items	Resources	Justifications
Immediately 8.3.5	Passwords must be changed immediately after the first use.	**Human resources** Low: This process requires minimal head count; it's generally managed by existing IT staff or via automated password reset tools.	Changing passwords immediately after first use helps mitigate the risk of unauthorized access due to potential exposure or interception during initial login.
		Financial resources Low: This activity requires little to no cost; minimal financial cost may be incurred for password management software or tools.	
Immediately 9.3.1.1	Physical access to sensitive areas must be immediately revoked on termination.	**Human resources** Medium: This requires dedicated staff with physical access control responsibilities (such as security officers and facility managers); some effort may be required for timely HR coordination.	Revoking access immediately helps prevent unauthorized entry, thereby protecting company assets.
		Financial resources Low: This activity has little to no cost; it primarily relies on existing resources such as an access control system.	
Immediately 12.10	Respond to any security incidents that affect the CDE immediately.	**Human resources** Medium: This requires immediate attention from dedicated staff with specialized incident response expertise. Staff must rapidly assess events to identify and contain issues and take swift action to restore systems or implement mitigating controls.	Responding to security incidents immediately is crucial to minimize damage, contain threats, identify vulnerabilities and restore normal operations swiftly.
		Financial resources Medium: Additional costs for external expertise are possible such as forensic analysis, reporting, or hardware or software replacement or repair.	
Promptly 5.3.1	Antimalware must be kept current and promptly deployed.	**Human resources** Low: This requires minimal head count; establish and communicate documented checklists or system onboarding procedures to relevant IT teams.	Deploying antimalware promptly can prevent malicious software infections and maintain the integrity of critical components.
		Financial resources Low: This process is largely administrative and usually automated; costs are likely already included in the existing security infrastructure.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources		Justifications
Promptly 10.3.3	Audit log files are promptly backed up to central log servers (e.g., SIEM).	**Human resources** Low: Minimal head count is required; establish and communicate documented checklists or system onboarding procedures to relevant IT teams.		Backing up audit log files promptly ensures the preservation of crucial evidence for security investigations and maintains the integrity of system activity records.
		Financial resources High: This activity may require costs for a SIEM system or log management tools; it could be outsourced to an MSSP if human resources are lacking.		
Promptly 10.7	Failure of critical security systems must be responded to promptly.	**Human resources** Medium: This requires prompt attention from dedicated staff with specialized expertise for critical systems; it requires staff to rapidly assess events to identify and contain issues and take swift action to restore the system or implement mitigating controls.		Promptly responding to security system failures can help minimize downtime and any potential breaches or vulnerabilities.
		Financial resources Medium: This may incur added costs for external forensic analysis, reporting, or hardware or software replacement or repair support.		
Promptly 12.3.4	Ensure that in-scope hardware/software continues to promptly receive security updates from vendors.	**Human resources** Medium: This process requires minimal head count, leveraging routine vendor security update monitoring procedures; the service may be covered as part of third-party service contracts.		Receiving security updates promptly is vital because they often contain patches for known vulnerabilities.
		Financial resources Low: This process relies primarily on existing resources and infrastructure; software maintenance contracts and subscriptions often include updates. Tools may be acquired. A minimal one-time cost or ongoing cost may be required.		

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Periodically 5.2.3	Ensure that system components that do not have antimalware installed are evaluated periodically.	**Human resources** Low: This review focuses on systems that traditionally aren't affected by malware but could be as new threat vectors are identified.	Systems that don't traditionally have antimalware installed need periodic evaluation to identify potential security gaps and mitigate the risk of malware infiltration.
		Financial resources Low: The financial cost associated with this evaluation is low; software required is only antimalware.	
Periodically 7.2.5.1	Review access privileges for all system accounts based on targeted risk analysis (TRA) defined frequency.	**Human resources** Low: This requires IT teams to document all system accounts along with associated access levels and update and revoke access as needed.	Organizations need to ensure that privileges for system accounts remain appropriate for their intended function to minimize risk of unauthorized access.
		Financial resources Low: The review uses existing resources that require little to no cost; minor expenses might include tools and software to support reviews.	
Periodically 8.6.3	Change the passwords for system accounts based on TRA defined frequency.	**Human resources** High: This requires a minimal level of head count but could potentially require a significant amount of planning to minimize disruption to critical services.	Changing passwords for system accounts is crucial to mitigate the risk of potential password compromise through means such as brute-force attacks, phishing or insider threats.
		Financial resources Low: This activity requires no significant financial investment using existing resources; minor expenses might include password management software.	

■ Low   ■ Medium   ■ High

Frequency/ Requirement	Action items	Resources	Justifications
Periodically 9.5.1	Inspect point-of-interaction (POI) device surfaces for tampering or unauthorized substitution periodically.	**Human resources** Low: This process can primarily be handled by existing head count to inspect POI devices and record inspection activities.	Inspecting the surface of POI devices is essential to detect physical tampering, skimming devices or other unauthorized modifications.
		Financial resources Low: Little to no financial resources are required, but this task is essential for maintaining compliance and ensuring CHD security.	
Periodically 10.4.2	Review logs of all other system components periodically.	**Human resources** High: Reviewing logs from all other system components requires IT and security professionals to analyze, identify and investigate potential incidents. Review is recommended daily or weekly — less often might delay incident response efforts.	Logs of all other components not specified in 10.4.1 must be reviewed periodically to identify any potential issues.
		Financial resources High: The review may require costs for SIEM systems, log management tools, incident response or remediation. It could potentially be outsourced to an MSSP if head count or expertise is lacking, which would involve additional costs.	
Periodically 12.10.4	Train personnel responsible for responding to security incidents periodically.	**Human resources** Medium: Subject matter experts on incident handling are required to design and deliver training. This task may also require IT and security professional participation.	Incident responders must remain proficient in handling evolving threats, technologies and procedures.
		Financial resources Medium: A moderate level of financial investment may be required: All team members need training. External trainers or subject matter experts may be required.	

🟩 Low   🟨 Medium   🟧 High

Sung Chae
South Korea-based consultant specializing in various GRC frameworks, such as PCI DSS, SWIFT CSP and ISO27001

Jackson Wee
PCI DSS QSA, CISSP, CISA, CISM
Singapore-based consultant specializing in various GRC frameworks, such as PCI DSS and ISO27001

Verizon 2024 Payment Security Report

Editorial team

Lead author
Ciske van Oosten

Co-authors
Sung Chae
Stephen Ward (Source Defense)
Jackson Wee

Lead editor
Cynthia B. Hanson

Co-editors
Jennifer M. Rudrow
Patti Tom Watt

Project managers
Caitlin Menendez
Jennifer M. Rudrow

Data analysts
Matt Arntsen
Mikhail Banguerski
Sebastien Mazas
Anne Turner
Ciske van Oosten

Contributors
Matt Arntsen
Ferdinand Delos Santos
John Galt
Claire Lavelle
Vincent Lucas
Sebastien Mazas

Legal review
Rishard Cooper
Eric Nouri-Mesbahi

Payment security consulting practice

Verizon Cyber Security Consulting
Senior Director, Security:
Kristof Philipsen
Director: Sam Junkin

PCI and payment security consulting practice
Global lead: Sebastien Mazas
Global intelligence: Ciske van Oosten
Americas region: Matt Arntsen
APAC region: Ferdinand Delos Santos
EMEA region: Loic Breat

Team email
paymentsecurity@verizon.com

Third-party contributors

We thank the following organizations for the valuable contribution of anonymized PCI DSS ROC data:

Control Gap: Laura McAllister
GM Sectec: Carlos Convit, Russell Latimer, Héctor G. Martinez, Oswaldo Silva
Integrity360: Marco Borza, Martin Petrov
MegaplanIT: Jennifer Boyd, Caleb Coggins, Anthony Petruso, Michael Vitolo
Online Business Systems: Sherri Collis, Rob Harvey, Steve Levinson

The Verizon Payment Security Report author team extends an open invitation to any Qualified Security Assessor organization to join our research team and contribute compliance data to the publication.

PCI DSS data contributors

About Verizon Cyber Security Consulting

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

Verizon is the longest-running global PCI security consulting and assessment services provider in the world, offering services since 2002. Our payment security practice provides PCI and Society for Worldwide Interbank Financial Telecommunication (SWIFT) consulting, assessments and program maturity improvement services. Across its Cyber Security Consulting portfolio, Verizon offers services that help clients identify, protect against, detect, respond to and recover from cyberthreats while helping to comply with applicable regulations and standards.

This publication is available online at: verizon.com/paymentsecurityreport