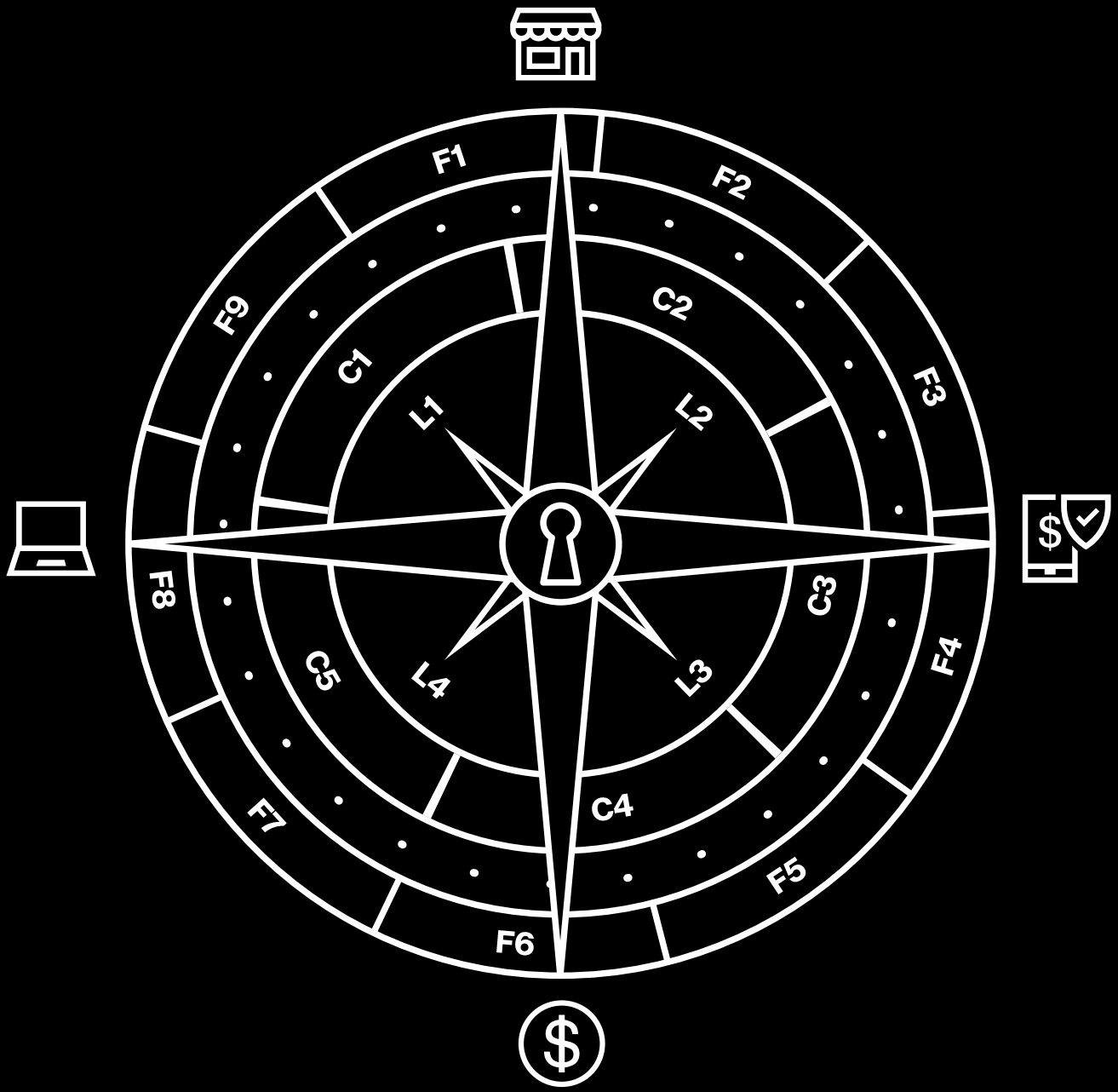
Executive insights

2019 Payment Security Report



verizon

Report timeline

Verizon has published the Payment Security Report (PSR) since 2010. At the time, it was the first-ever study on the value and performance of the Payment Card Industry Data Security Standard (PCI DSS). Fast-forward nine years, and the PSR continues to offer a unique view on the long-term impact of the PCI DSS, measuring a decade of actual PCI assessments conducted across the globe.

The PSR reveals groundbreaking insights that help payment card professionals better understand their world. The PSR continues to be a highly anticipated report in the industry among key players, including the PCI Security Standards Council (SSC), that addresses the challenges of payment data protection and meeting compliance requirements.

2010: 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

2011: 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

2014: Simplifying complexity

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

2015: Achieving sustainability

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

2016: Developing proficiency

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

2017: Establishing internal control

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

2018: 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 5 Constraints (5 Cs) of Organizational Proficiency

20 years navigating the world of data protection

Twenty years ago, in 1999, the major card brands initiated their cardholder data protection programs and in 2004, the programs were combined into a single data security standard. The PCI DSS celebrates its 15th birthday this year (v1.0 was released in 2004). An effective and sustainable control environment remains as relevant as ever, yet for many organizations, this remains a challenge.

Going through a check-box routine or merely throwing money into data protection does not solve organizations' compliance challenges. Often, these tactics lead to a false sense of security. Too many organizations are stuck in a reactive "wash, rinse, repeat" pattern, focusing only on meeting baseline compliance requirements.

To keep up with threats, data protection compliance programs (DPCPs) must continue to evolve and mature. Organizations must develop visibility, control and predictability in compliance performance. They must become proactive instead of reactive.

What the industry seems to need most is guidance on how to develop and how to measure the effectiveness and maturity of their DPCPs. That is what this edition of the Payment Security Report is about.

Verizon's cumulative experience gained from 25 years of measuring, analyzing and building mature, effective compliance and security programs has helped us position the 2019 PSR as the ideal navigational guide—not only for charting one's course through uncertain and changing waters, but for staying ahead in the race. This year, we build on the insights and recommendations from past years to introduce the practical, integrative Verizon 9-5-4 Compliance Program Performance Evaluation Framework as a navigational tool to improve DPCPs.

What 15 years of compliance trends reveal

Since 2008, Verizon has tracked the percentage of organizations that achieve PCI DSS compliance and keep the numerous required security controls in place throughout their annual compliance cycles. The percentage, as noted in the 2016, 2017 and 2018 editions of the Verizon PSRs, has varied from a low of 11.1% in 2012 to a high of 55.4% in 2016.

When the PCI SSC published the PCI DSS in 2004, it was expected that organizations would achieve effective and sustainable compliance within about five years. Some 15 years later, less than half of organizations maintain programs that prevent PCI DSS security controls from falling out of place within a few months after formal compliance validation. As Figure 1 reveals, sustainability is trending downward.

What our readers are telling us:

"The Verizon PSR provides attention and focus on the exact subjects, at the exact time of its need. It really helps us prioritize and focus on what matters most."

—Chief Information Security Officer (CISO) at a medical organization

"The Verizon Payment Security Report is required reading for our entire program team, managers and all participants. It is a mandate by our Chairman of the Board."

—Compliance Manager at a financial services organization

"The report is clear on what we should measure [and] where we should drive performance. It offers clear, strategic direction to decision-makers. Implementation of its recommendations will increase efficiency and effectiveness of the overall compliance effort. It offers practical guidance on where to apply resources. This translates into reduced workloads, more focused efforts and cost savings, i.e., higher return on investment from the compliance program."

—CISO at a major insurance company

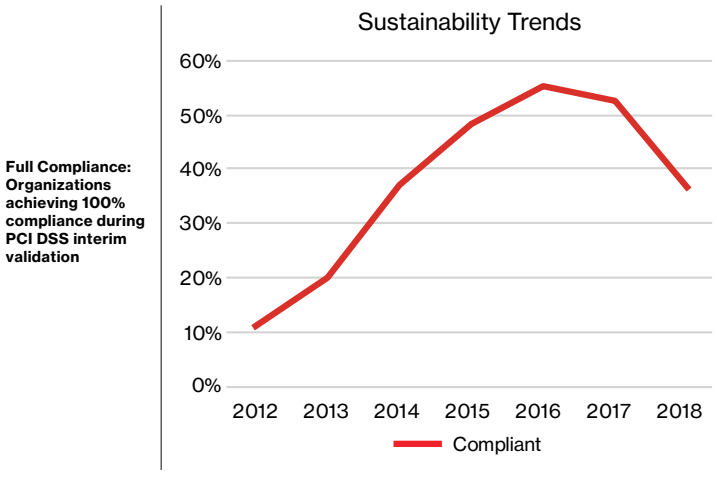


Figure 1. PCI DSS compliance trends, 2012-2018, according to Verizon Payment Security Report research

What's going wrong

Data protection and compliance present daily challenges. Security specialists must be on their toes to assure that controls remain in place and perform consistently. Despite good intentions, more than half of organizations are still struggling to design, implement and maintain a sustainable compliance program.

One challenge is that many security professionals believe they can protect data by following a script, as if doing A, B and C in the correct order will achieve effective and sustainable data protection. In the real world, things are messy.

Organizations might be spending a lot of time and money creating their DPCPs, but many are ineffective and fail to advance beyond a program that looks good on paper but does not withstand the scrutiny of a professional security assessment. The DPCPs lack the design, implementation, review process and revisions to become effective and sustainable.

Additionally, organizations have inadequate or overly complex strategies, which originate from a lack of proficiency in designing, implementing, monitoring and evaluating a DPCP.

Program maturity:

Nearly one-quarter of organizations (18%) have no defined compliance program. Only 20% of organizations rate their DPCP maturity as advanced. No organizations (0%) rate their program maturity as optimized.

Use of metrics:

Only 18% measure their PCI DSS controls more frequently than what PCI DSS requires across their entire environment. About one-third (32%) use control effectiveness and operational performance metrics. Only 7% use program impact metrics to measure program performance.

—Verizon 2018 survey results of approximately 55 organizations worldwide

Data protection should be approached like a chess game, with a sound strategy that includes assessing risks and planning several steps ahead. Each move should be evaluated and executed strategically, taking the pieces on the board into thoughtful consideration.

All too often, CISOs focus on keeping only baseline control activities in place instead of growing data protection competency and maturity. They need a clear and easy-to-understand navigational guide to help them deliver measurable results and predictable outcomes.

In the 2018 PSR, we outlined the key factors that affect control effectiveness and sustainability. The response was overwhelmingly positive, with numerous requests for practical recommendations on how to implement the 9 Factors of Control Effectiveness and Sustainability Framework to strengthen and improve DPCPs. That is what the Verizon 9-5-4 Compliance Program Performance Evaluation Framework is all about.

The Verizon 9-5-4 Compliance Program Performance Evaluation Framework

Compliance challenges do not exist in isolation. In the 2018 PSR, we explained PCI DSS control dependencies and the influence of the control environment. We introduced the 9 Factors of Control Effectiveness and Sustainability. If any of the 9 Factors are deficient or missing from a DPCP, the program will likely fail to achieve a sustainable level of process maturity. We also pinpointed the typical constraints that limit the performance and achievement of control objectives across the 4 Lines of Assurance.

In the 2019 PSR, we provide the Verizon 9-5-4 Compliance Program Performance Evaluation Framework that combines the 9 Factors of Control Effectiveness and Sustainability with the 5 Constraints of Organizational Proficiency and 4 Lines of Assurance.

This integrated framework can be the navigational aid that organizations need to enhance the clarity of their DPCPs. The framework provides a new level of visibility and control that helps businesses achieve repeatability, consistency and highly predictable outcomes.

The 9-5-4 Framework addresses elements to help develop and improve capability and process maturity across an entire DPCP. Continuously maturing your security framework with the Verizon 9-5-4 Compliance Program Performance Evaluation Framework is a proactive and progressive step that will help keep compliance at full capacity. We delve deeper into the framework later in this summary, preceded by an overview of this year's statistical analysis of global compliance.

Global state of PCI DSS compliance

This year's PSR has exciting aspects in its findings. For the first time, the PSR contains assessment data compiled from additional qualified security assessor (QSA) companies. This expands the view and perspective provided in past PSRs.

The 2019 PSR includes data from 302 engagements around the world. We expect this number to increase as QSA companies globally continue to collaborate and share their insights to provide a holistic view of PCI DSS compliance. This data takes on a new level of importance as the entire payment card industry moves to the new standard, PCI DSS v4.0, in 2021.

The 2018 PSR reported that full compliance with the PCI DSS decreased, and this year we see the same negative trend globally. Assessments from other QSA companies also show lower full compliance.

Organizations are required not only to achieve 100% compliance with the PCI DSS but also to maintain it. This means having all applicable security controls continuously in place and functioning as intended. Verizon measured organizations during interim assessments to determine the percentage that achieved full compliance for each PCI DSS key requirement in 2018.

An interim assessment—or initial report on compliance (iRoC)—provides a valuable opportunity for organizations to validate the effectiveness of PCI DSS control management. For some time, these interim assessments found full compliance with PCI DSS to be increasing. But in 2017, that upward trend reversed when full compliance declined by 2.9 percentage points.

Compared to the previous years, global compliance fell a further 15.8% in 2018 to 36.7%, and is following the decreasing trend in sustainability seen across the past three years (2016-2018), according to the 2017 and 2018 editions of the Verizon PSR.

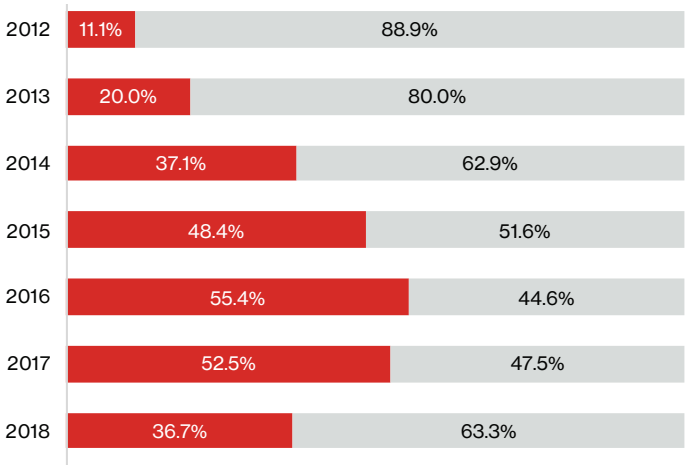


Figure 2. Full compliance history

This is a significant drop in compliance rates. There are many potential factors for the decrease. For example, changes in personnel and mergers can throw a proverbial wrench into the works of DPCPs. Changes in the operating environment can also leave the ship adrift without guidance.

Full compliance

The share of organizations achieving 100% PCI DSS compliance at interim validation. All organizations studied passed a previous validation assessment, so this indicates how well they managed to sustain compliance.

Control gap

The number of failed controls divided by the total number of controls expected. This is an average figure that gives a measure of how far the assessed entities were from full compliance.

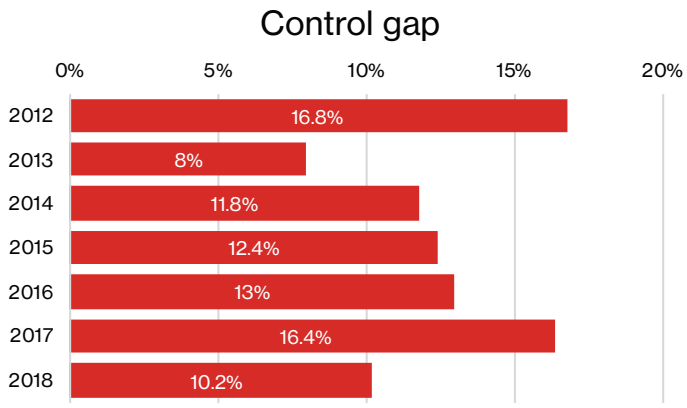


Figure 3. Control gap

The compliance story

While overall compliance has fallen, the control gap representing how far organizations were from full compliance remained consistent with the previous year at 7.2% for the total population of organizations in the data set, according to the most recent Verizon PCI Security Practice data.

Requirements 5 and 7 of the standards continue to be the most consistently maintained, as we have seen across the past three years.

The largest compliance drop was seen against Requirement 6, as organizations struggle to maintain effective vulnerability management, software development and change processes. Requirement 11 remains the poorest performing in both overall compliance and control gap, as organizations cannot sustain compliance with security testing requirements year-on-year.

Organizations in the Asia-Pacific (APAC) region show stronger ability to maintain full compliance: 69.6% maintained conformance to the security standard. Fewer than one-quarter of all organizations in the Americas maintained full compliance, at 20.4%.

This is 49.1% fewer than the APAC average. If you are an organization in the Americas, there is more than a 75% chance that you need support to get your security and compliance programs on track.

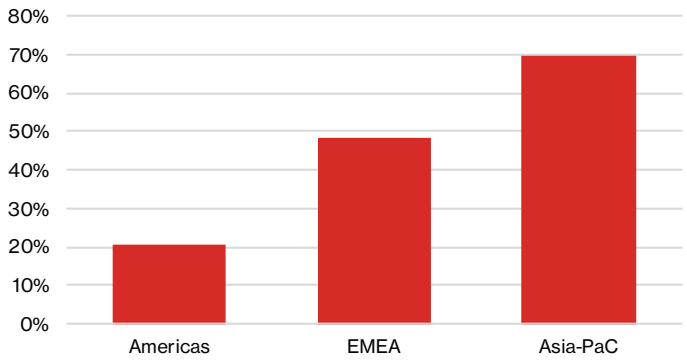


Figure 4. Full compliance by region

The finance industry has done a tremendous job with raising the bar on full compliance in comparison to peer industries, but it is only 2.4% above the global average. As with other industries, we saw a significant decrease in the ability to maintain full compliance. Hospitality would strongly benefit from the advice provided in the Verizon PSR to build a sustainable security program.

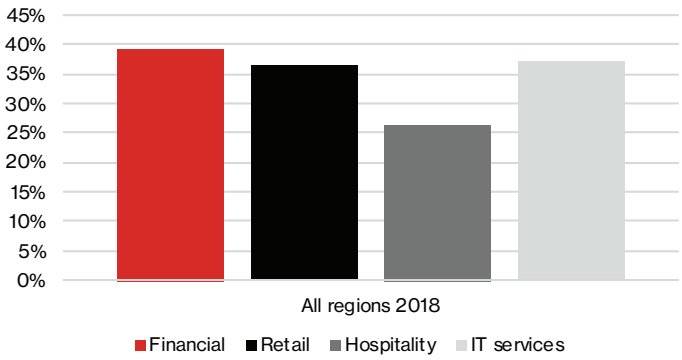


Figure 5. Global PCI DSS compliance by industry

Interesting notes about the control gap

Because PSR research has found that many organizations do not maintain compliance, it is important to understand how well they protect sensitive payment card data. Organizations that are fully compliant have a control gap of zero. For others, the control gap decreased to 10.2%, which is 6.2% better than what was documented in the 2018 PSR. This translates to just under 90% compliance for most organizations. If 90% is an "A," then the average control gap would result in a "B."

If we look at the controls organizations sustain least, we see 7 of 12 requirements have controls in the bottom 20 list. Requirement 11 has consistently ranked last, with seven of its controls in the bottom 20 list.

These controls are fundamental steps to establishing a compliance program to protect data. If you haven't implemented these controls, Verizon Threat Research Advisory Center (VTRAC) data indicates there is a more than 95% probability that your organization has not truly committed to a sustainable DPCP.

While a smaller control gap means businesses are moving in the right direction, the controls with the most substantial gap to full compliance are 16 to 33 percentage points away from the lowest possible compliance—indicating potentially serious security risks.

Data breach correlation

In this year's report, we've included more detailed data breach investigation correlations. These are based on data breach metrics from PCI Forensic Investigations (PFIs) performed by VTRAC from 2016-2018.

It is not always possible to pinpoint the specific cause that resulted in the data breach or the contributory factors that helped propagate it. In 28.7% of investigations, identifying a specific requirement as causing a breach was not possible. In 27.4% of investigations, the extent to which a requirement could be identified as contributing to a data breach is unknown. This is mainly due to the lack of evidence available to investigators because of poor log management practices, weak incident response (IR) procedures, and limited capabilities within organizations to preserve evidence in the wake of a cybersecurity incident.

Incident preparedness summary

12 requirements

No organization suffering a data breach was compliant across all 12 requirements across the 2016-2018 dataset.

0%

No organizations—at the time of breach—were compliant with Requirements 3, 8, 10, 11 and 12.

75%

Requirement 9 had the highest compliance rates of all PCI DSS requirements among breached entities, but failures were still observed in 75% of organizations.

10.2

Most organizations had difficulty meeting Requirement 10.2, the ability to reconstruct events by implementing proper audit trails. Retail organizations experienced the lowest level of compliance with PCI DSS incident preparedness requirements, followed by the financial services industry. IT services do much better, with only 1% of organizations failing to meet Requirement 10.2.[1]

These PCI DSS controls directly address incident preparedness: the ability of an organization to identify and respond effectively to a cybersecurity incident.

- **Requirements 12.10, 12.10.1, 12.10.2**
  Implementing a plan to respond immediately to a cardholder data security incident, defining procedures for reporting incidents, responding to alerts and effective management of the process
- **Requirements 11.1.2, 12.5.3**
  Establishing incident response (IR) procedures for security monitoring and responding to alerts, including rogue wireless monitoring, security event logs, intrusion detection and change detection solutions
- **Requirements 10.2, 12.10.4**
  Communicating the plan and response procedures, ensuring personnel know of and are trained in the IR plan and procedures, and maintaining a 24/7 capability to respond to cybersecurity alerts
- **Requirement 12.8.3**
  Appropriate due diligence for third parties must include evaluation of IR capabilities and a requirement to notify about all security incidents

1 2017 data PCI DSS set. For details, see page 13 of the 2019 Verizon Incident Preparedness and Response Report, https://enterprise.verizon.com/resources/reports/2019/vipr/2019-vipr-full-report.pdf

Introducing our VTRAC investigator view from the field

For years, we've heard the claim by industry experts that "no truly PCI DSS-compliant merchant has ever been breached." We don't have access to investigative data from every breach of a payment card processing environment since the first plastic card with a magnetic stripe was processed and compromised. Nor do we have direct access to every adversary who decided to electronically evade an organization's security controls. But here's what we do know:

The State of Compliance section of the 2019 PSR includes more detailed breach correlation data than ever before. Alongside, we also present real-world, first-hand observations from our field investigators, who have conducted PCI data breach investigations.

When we revisit payment card security breaches investigated by VTRAC, we can definitively state we have never reviewed an environment or investigated a PCI data breach involving an affected entity that was truly PCI DSS compliant—even if it had a signed Attestation of Compliance (AOC).

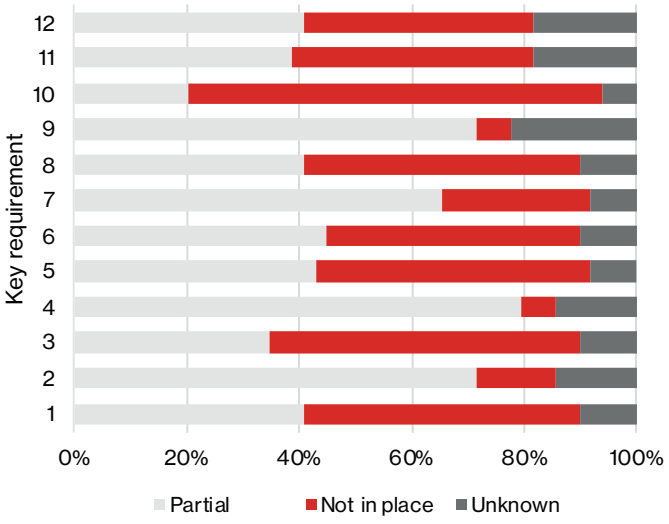


Figure 6. PCI DSS control status of breached organizations

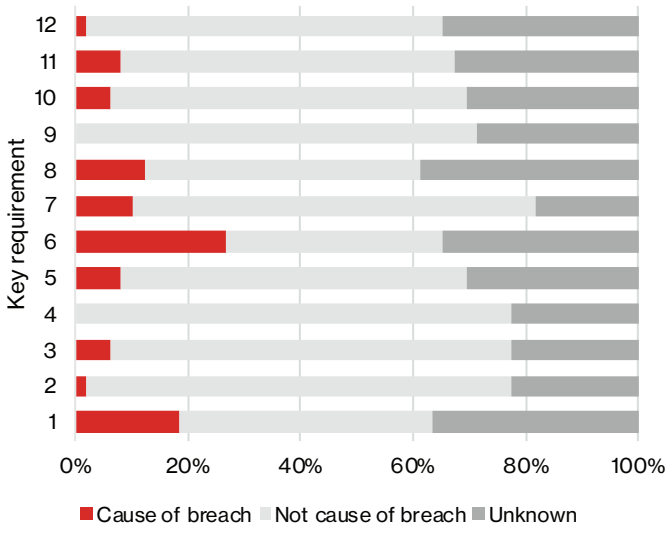


Figure 7. Requirements identified as the cause of data breach in PFI investigations

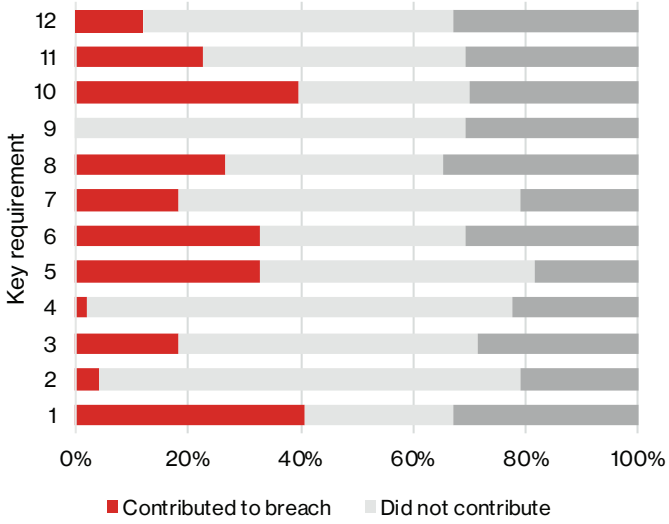


Figure 8. Requirements identified as contributing to a data breach in PFI investigationsw

Developing program maturity

Organizations do not willfully and deliberately fail to design effective and sustainable control environments. Developing program maturity is difficult. It requires capacity (resources), capability, competence, commitment and communication. We refer to this as the 5 Constraints of Organizational Proficiency, or 5 Cs. By asking yourself tough questions, taking the steps below and guiding your progress with the Verizon 9-5-4 Compliance Program Performance Evaluation Framework, you can navigate your organization toward a more mature and effective DPCP.

- **Prioritize**
  Security professionals with the right skills and experience should know how to prioritize program objectives. There will always be more issues than an organization can simultaneously address. It is crucial to know what to focus on and how to prioritize.
- **Document detailed performance standards**
  This process is essential to identify problems and define acceptable vs. unacceptable deviations from internal data protection and compliance performance standards.
- **Apply risk management techniques**
  The root cause of issues is typically not a single component of the control environment. Applying a systematic evaluation with risk management techniques can help differentiate one-time events from recurring problems critical to remediate.

Learning where your organization needs to focus, and how to make the necessary changes, is easier with the Verizon 9-5-4 Compliance Program Performance Evaluation Framework.

10 tough questions to advance your DPCP

As film director and author Werner Herzog sagely put it, “Sometimes a deep question is better than a straight answer.”

1. What data do you have, where is it and how does it flow?
2. Are you secure enough? How confident are you about the protection of your data?
3. How much confidence do you have that the right controls are effective and in the right places?
4. How predictable is your DPCP performance?
5. How do you ensure the quality and durability of your key data protection and compliance processes? Do you know what those processes consist of?
6. How quickly can you detect and respond to policy, standard and procedure deviations?
7. Do you have controls in place to measure the effectiveness of your DPCP implementation and maturity strategy?
8. How do you know that you are prioritizing the right DPCP activities at the right time?
9. How well are you managing the 5 Constraints of Organizational Proficiency: capacity, capability, competence, commitment and communication?
10. How well do you understand the 9 Factors of Control Effectiveness and Sustainability? What target maturity levels are you working to achieve in the long term?

An integrated evaluation framework for sustainability and effectiveness

Based on our findings, only 36.7% of organizations maintain sustainable control environments. Clearly, too many organizations do not know how to effectively measure the strength of their DPCPs.

The framework presented here allows organizations to map, monitor and report the status of sustainability and effectiveness for each of the 9 Factors across each of the essential 4 Lines of Assurance by evaluating the 5 Constraints. This mapping presents 45 control points across each of the lines of assurance and 180 control points in total.

Key questions

- Is your organization's compliance program well-designed?
- Does your compliance program work in practice?
- Is your program being managed effectively?
- How sustainable is your control environment?
- Do you know how to pinpoint your program's constraints and deficient proficiencies?

The 9-5-4 Compliance Program Performance Evaluation Framework

Evaluate and report the 9 Factors and each of the 5 Constraints across all 4 Lines of Assurance

Lines of Assurance:

1. **Individual accountability**
2. Risk management and compliance teams
3. Internal audit
4. External audit, regulators

Factor	Capacity	Capability	Competence	Commitment	Communication
1. Control environment	■	■	■	■	■
2. Control design	■	■	?	■	■
3. Control risk	■	■	■	■	■
4. Control robustness	■	■	?	?	■
5. Control resilience	■	■	?	?	■
6. Control lifecycle management	■	■	■	■	■
7. Performance management	■	■	■	■	?
8. Maturity measurement	■	■	■	■	?
9. Self-assessment	?	■	?	?	■

Figure 9. Compliance Program Performance Evaluation Framework

Figure 9 contains sample data and is a high-level presentation of the 5 Cs of Organizational Proficiency that can affect the design, implementation and operation of the 9 Factors for each of the 4 Lines of Assurance. Each of the 180 control points can be integrated into a DPCP as an outcome. For example, you can start with evaluating all 9 Factors and each of the 5 Cs for the first line of assurance to determine the effectiveness and sustainability of data protection and compliance at the individual accountability level.

The example (Figure 9) indicates that:

- There are no significant concerns (■) about capacity, capability, competence, commitment or communication for Factor 1, the control environment, at the individual level within the organization.
- There is uncertainty (**?**) whether the needed competence exists internally at the individual level for Factor 2, control design. Further investigation is necessary.
- The competence for Factor 3, control risk, does not exist (■), indicating a need to obtain the necessary knowledge, skills and experience for designated individuals to measure control risk.

You repeat the evaluation, starting with a new table for each line of assurance, filling in the status for each organizational proficiency (i.e., constraint) as it applies to each of the 9 Factors within the chosen line of assurance. The lines of assurance can be expanded as needed, such as by explicitly adding executive management and board oversight.

This framework allows for a highly structured, repeatable and consistent method to:

- Clearly define the internal and external control environment
- Identify and define the controls needed to mitigate risks
- Identify and define the constraints that affect control performance and data protection effectiveness and sustainability
- Define and communicate performance requirements and standards for the design and operation of the control environment

This integrated evaluation approach provides the benefits of:

- **Transparency**
  This approach provides full visibility into the value of compliance investments, by tying processes, constraints and outcomes together.
- **Precision**
  This framework provides a detailed and exact focus on each of the core components to address specific constraints. It allows for precise tailoring of the controls and upfront measurement of control effectiveness.
- **Scalability**
  This approach allows for the incremental development of maturity. Capability and process maturity can increase as the capacity and other resources become available.
- **Flexibility**
  The Verizon 9-5-4 Compliance Program Performance Evaluation Framework complements existing standards, such as National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Control Objectives for Information and Related Technology (COBIT), and Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- **Measurement**
  Organizations can measure control effectiveness and use this data to precisely tailor controls across the environment.

Overview of the 2019 Payment Security Report

It is high time for compliance programs and organizational capabilities to evolve. Organizations need to develop the visibility, control and predictability in compliance performance that powers proactive, rather than reactive, data protection.

Our full 2019 PSR provides guidance to accomplish these tasks and explains how new tools, such as the Verizon 9-5-4 Compliance Program Performance Evaluation Framework, can help you move your compliance management to new levels.

The 2019 PSR explains how, with new methods, organizations can effectively manage control environments and achieve higher levels of assurance and predictability in their DPCPs. The report builds on the 2018 PSR, presenting an integrated framework to incrementally improve organizations' data protection and compliance capabilities by using maturity models as a guide. Specifically, the 2019 Payment Security Report covers:

- The global state of compliance; how organizations are maintaining (and not maintaining) PCI DSS compliance
- Important compliance program design considerations
- Insights into data breach correlation and incident preparedness
- Mobile payment security trends
- A PCI DSS compliance reference calendar

About the cover

The cover presents an 18-point navigational compass rose used for orientation. In this case, the compass symbolizes the 9-5-4 Compliance Program Performance Evaluation Framework introduced in the 2019 Payment Security Report to illustrate that the report can help you navigate toward mature data protection management with 360° visibility and control. The four cardinal directions (where you would normally see north, east, south and west) symbolize four key industries: hospitality, retail, financial and IT services. Instead of eight principal winds, which are commonly found on compasses, we've illustrated the 9 Factors of Control Effectiveness and Sustainability, along with the 5 Constraints of Organizational Proficiency as half-winds surrounding the 4 Lines of Assurance nearest to the core. The core of the compass holds the key to unlocking effective and sustainable data compliance program management.

Verizon 2019 Payment Security Report – Executive insights

Published September 17, 2019

Editorial team

Lead author:
Ciske van Oosten

Co-authors and editors:
Anne Turner, Clarence Hill, Cynthia B. Hanson, Dyana Pearson, John Grim, Neal Maguire

Data analysts:
Anne Turner, Noel Richards, Saravanan Thangam, Sundeep Paderu, Ron Tosto

Security assurance practice

Managing director:
Rodolphe Simonetti

PCI and Payment Security consulting practice

Global lead:
Ron Tosto

Americas region:
Franklin Tallah

APAC region:
Sebastien Mazas

EMEA region:
Gabriel Leperlier

Business intelligence:
Ciske van Oosten

Team email: paymentsecurity@verizon.com

Download the Payment Security Report at:

https://enterprise.verizon.com/resources/reports/payment-security/

Contributing organizations:

ControlScan FOREGENIX MEGAPLANIT schellman