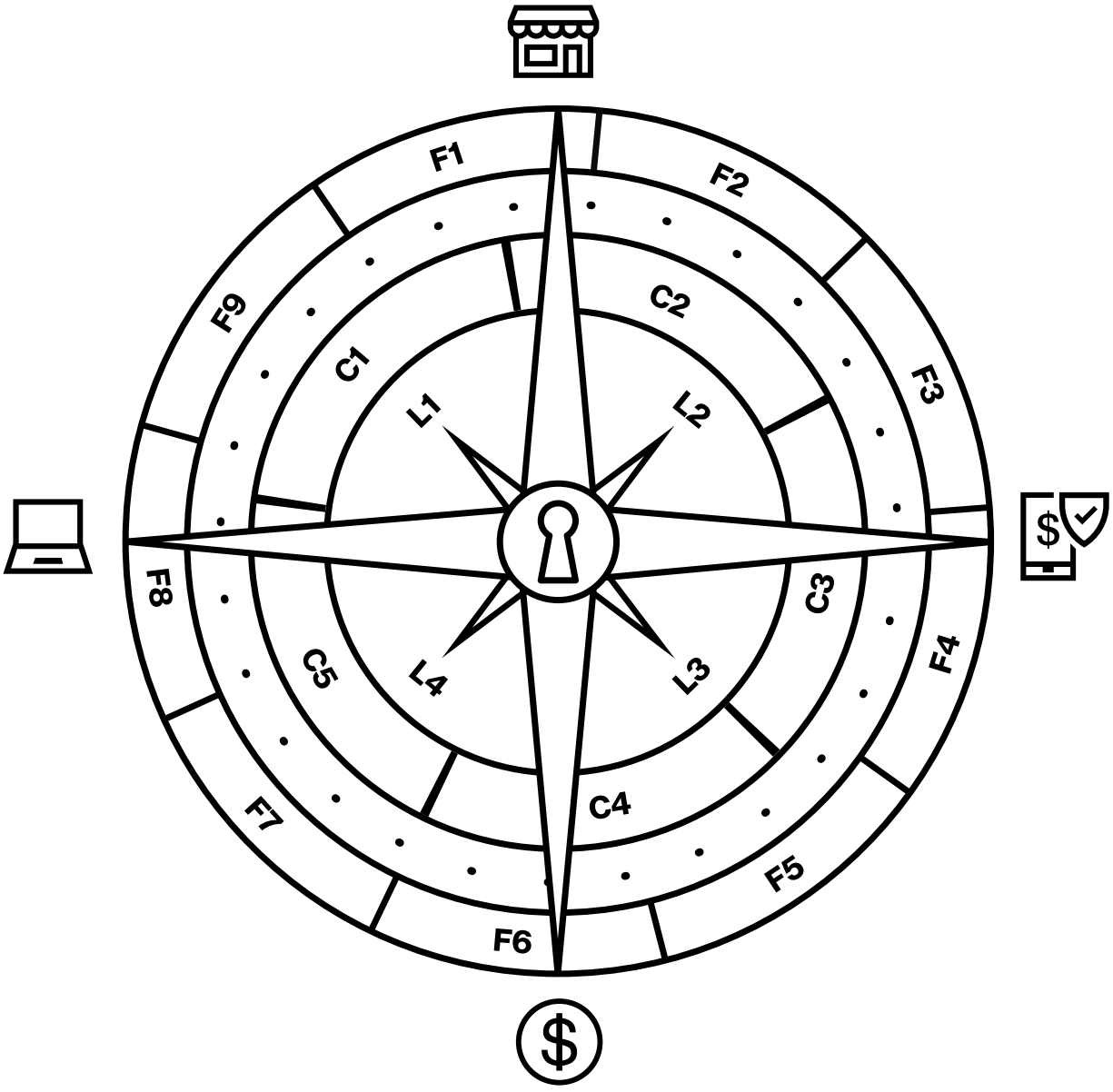
2019 Payment Security Report



verizon business ready

Contents

Verizon has published the Payment Security Report (PSR) since 2010. At the time, it was the first-ever study that provided an in-depth perspective on the regulatory landscape of the payment card industry, as well as 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 data protection successes and failures, and previously undervalued or unknown cause-and-effect factors. The report continues to be highly anticipated within the industry among key players, including the PCI Security Standards Council (SSC), and helps readers address the challenges of protecting payment data and meeting their compliance requirements.

What our readers are telling us:

"The Verizon Payment Security Report provides attention and focus on the exact subjects, at the exact time it is needed. 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, the managers and all participants, mandated 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

Verizon Payment Security Report history:

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 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

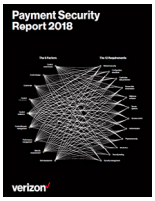
A focused look at improving the sustainability of compliance and a review of the state of scope reduction and payment security innovation and the need to avoid over-reliance on technology

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

Executive summary

The requirement for organizations to comply with payment card industry regulations and to be assessed against payment card data security standards began in 2003. Sixteen years later, many organizations are still stuck in a wash-rinse-repeat cycle of annual validation. The time has come to move data protection and compliance processes and capabilities to higher levels of maturity. To do so, organizations need advanced navigational aids and guidance on how to integrate the applications of maturity models and metrics into their compliance programs.

The PSR has the unique role of measuring the strengths and weaknesses of the PCI DSS and tracking the sustainability of compliance. It also measures and tracks challenges associated with implementing and maintaining security controls required for PCI DSS compliance.

The theme of this 2019 edition of the PSR is performance visibility, control and maturity. The report includes an analysis of how to realign your compliance program to improve these goals and design a sustainable path toward higher data protection maturity. This latest edition builds on previous reports. The 2017 PSR introduced the security control lifecycle framework. The 2018 PSR introduced the 9 Factors of Control Effectiveness and Sustainability and their critical role in a data protection control environment, as well as methods for measuring control effectiveness and maturity.

The 2019 PSR brings these concepts together to explain how to apply and integrate them into data protection compliance programs (DPCPs). The report also addresses requests from CISOs across the industry for guidance on what they need to prioritize to deliver the key objectives that matter most to them: (1) sustainable control effectiveness and (2) predictable program performance and outcomes.

The report includes new tools, including the Verizon 9-5-4 Compliance Program Performance Evaluation Framework, to help you move your compliance management to higher levels of assurance and predictability. The framework builds on the 2018 PSR to provide an integrated method for improving data protection and compliance capabilities by using maturity models as guides.

In addition, the 2019 PSR covers:

- The current 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
- Incident preparedness guidance

The compliance landscape

Introduction

Twenty years ago, in 1999, the major card brands initiated their cardholder data protection programs. The PCI DSS celebrates its 15th birthday this year. An effective and sustainable control environment remains as relevant as ever. Based on the continuing occurrence and severity of data breaches, many organizations appear to still be approaching compliance as a "check box" routine.

Without a sound strategy to measure data protection effectiveness and sustainability, throwing money at data protection does little to prove an organization is getting better at maintaining compliance. This approach may lead to a false sense of security. Many organizations appear stuck in a reactive cyclic pattern, focusing only on meeting baseline compliance requirements.

Compliance programs and organizational capabilities must continue to evolve and mature. Organizations must develop visibility, control and predictability in compliance performance. This structure moves data protection from a state of being reactive to proactive.

We have identified a need across the industry for guidance on how to develop and measure the effectiveness and maturity of data protection. With PCI DSS compliance sustainability in decline worldwide (see Figure 1), organizations must understand how to effectively manage their control environments and achieve a level of assurance and predictability for each core data protection and compliance process.

This edition of the PSR is intended to help readers understand these challenges and integrate maturity models as navigational tools throughout compliance lifecycles. Building on our industry-leading insights and recommendations, this report presents a practical, integrated framework for organizations to improve their data protection and compliance statures.

"Compliance sustainability"[1] 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 and evaluating organizational competence and commitment toward early detection and correction of significant control performance deviations.

1 See Appendix F – Terminology, "Sustainability," page 83

What 15 years of PCI DSS compliance trends reveal

When Visa Inc.[2] initially launched the PCI DSS in 2004, many assumed that organizations would achieve effective and sustainable compliance within five years. A decade ago, Verizon started tracking the percentage of organizations that maintain compliance by measuring PCI DSS compliance during interim assessment—as an indication of full compliance. Full compliance has ranged from 22.0% (2009) to a low of 7.5% (2011) and high of 55.4% (2016).

However, now, 15 years after the launch of the PCI DSS, our assessments highlight that just over a third (36.7%) of organizations were actively maintaining PCI DSS programs in 2018. As Figure 1 indicates, the downward trend continues—which is a major cause for concern.

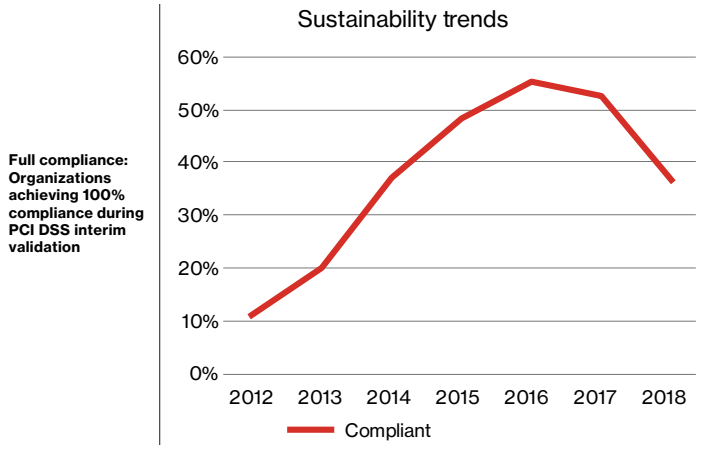


Figure 1. PCI DSS interim validation compliance trends, 2012–2018, according to Verizon PSR research

What's going wrong

Data protection and compliance present daily challenges. Organizations must be on their toes to ensure that controls remain in place and perform consistently. Despite good intentions, more than half of companies still struggle to design, implement and maintain a sustainable compliance program.[3]

Our research suggests that many organizations 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, solutions are not simple, requiring complex paths with non-linear progression.

Program maturity

Nearly one-fifth of organizations (18%) had no defined compliance program, according to approximately 55 organizations we surveyed for the 2018 PSR. Only 20% of organizations rated their DPCP as advanced. None of those organizations (0%) rated their program maturity as optimized.

Use of metrics

Only 18% measured 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.

Organizations might be spending a lot of time and money creating data protection compliance programs (DPCPs), but many can be ineffective and fail to advance beyond programs that look good on paper but do not withstand the scrutiny of a professional security assessment. Such DPCPs lack the design, implementation, review processes and revisions to be both effective and sustainable.

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

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.

verizon business ready

2 Visa Inc. published PCI DSS 1.0 in 2004; the PCI SSC's first publication was PCI DSS 1.1—published in 2006

3 Verizon global PCI customer survey 2018, page 27 (section on metrics and maturity)

Navigating predictable outcomes

In describing the challenges of securing card payment processes, we find an apt analogy of yacht racing, as explained in J. Rodney Turner's book on project management.

The one with the best strategic plan is the one who wins.

When yachts are sailing in a race, they sail around in a triangle, the longest leg of which is arranged to be sailing upwind. If, while sailing that leg, the crew aims the boat directly at the next buoy, they will be blown backward. What they have to do is to sail across the wind, called tacking, and slowly make their way upwind by tacking back and forth. Hence, they achieve the next objective not by sailing directly toward it, but by sailing for something they can achieve, and then something else they can achieve, eventually making the objective.

There is a joke about asking an Irishman the way to Dublin station. He says, "I wouldn't start here, if I were you." You would prefer not to start at this buoy to get to the next one upwind, but you have to, and you do it by taking it in steps you can achieve. All life is like that; all management is like that.

While tacking the current leg, you will choose a sail and rudder setting and will plan to sail so far, say 100 yards, before tacking about. While sailing that leg, you do not say, "This is my sail setting, this is my rudder setting, good project management is adhering to my plan, come what may." You continually adjust your sail and rudder setting as the wind fluctuates. You monitor the actual conditions and respond accordingly. And if the wind comes around far enough, it may be better to tack in the other direction, and you will change course.

You should treat your project plan as flexible. It was your best view of how to achieve the project when you developed the plan, but you must be willing to adapt it as you get new information and external conditions change. (Planning is essential, but your plans are useless.)

...A classic yacht race was the Whitbread Round the World Race. Before the start of the race, the competing yachts spent months pouring over weather charts and chose a strategy for the race based on the normal range of weather conditions. But while they are sailing, they must respond to the conditions actually encountered. They will have a strategy for the race, but will determine their detail plans as they sail the race, responding to today's conditions and the forecast for tomorrow.

In spite of not being able to plan the detail, there are three things that can be asserted:

1. **They can predict the duration of the race to a very high degree of accuracy, a few days in 9 months.**
2. **The boats that come first and second, after 9 months, are only a few hours apart.**
3. **There is a large degree of luck involved.**

The crew who wins is not the crew with the best detail plan to which they adhere doggedly. The people who win are the ones with the best strategic plan and who respond best to the actual conditions on the day. In spite of having to change the plan as the race progresses, the competitors are encountering the same conditions and are very close behind.

The most competent crew—the one with the best strategic plan—is the one who wins.[4]

verizon business ready

4 Republished with the permission of McGraw-Hill Education, from "The Handbook of Project-Based Management: Leading Strategic Changes in Organizations," J. Rodney Turner, third edition, 2014, 19; permission conveyed through Copyright Clearance Center, Inc.

Just as a yacht crew needs to develop capabilities to adapt to the prevailing conditions while staying focused on the destination, organizations need to be able to react effectively to changes in the control environment. That's tough to do when limited to a task-based approach to compliance programs. The global challenge with payment security is not the inherent lack of sustainability or control effectiveness. These are merely symptoms of a widespread problem caused by inadequate strategy, which originates from a lack of proficiency in organizations to design, implement, monitor and evaluate for a sustainable data protection compliance program.

Structuring and maturing compliance programs for sustainability

Payment card data should be protected by strategic design, not by luck. Control performance, i.e., the effectiveness and sustainability of a security control and its control environment, should be measured and predictable with organizations proactively detecting and correcting deviations from performance standards. An improvement in overall maturity (both capability and process) can move the organization from being reactive to disruptions, to being proactive and prepared to course-correct; i.e., it can give organizations the ability to predict outcomes with reasonable accuracy.

60% of surveyed organizations do not apply capability and maturity models to measure PCI security program maturity. Only 50% of these organizations measure controls beyond the requirements in the PCI DSS.

—Verizon global PCI customer 2018–2019 survey

Too many organizations lack the capability to design, implement and maintain the processes needed to achieve predictability in compliance performance. They do not have assurance about the effectiveness and sustainability of the control environment. Protection of payment card data requires a level of assurance that is only possible when the control environment and compliance program are designed to be robust, effective and sustainable and deliver predictable outcomes. Obtaining this assurance is not achievable unless organizations simplify strategic direction and use a clear navigational aid that encompasses capability and process maturity with the integration of a well-designed, standalone payment security compliance program (PSCP) or integrated DPCP.

Without the correct strategy and program alignment, organizations are more likely to address the wrong problems—focusing on the consequences or symptoms of poor program design. They spend more time on implementing compliance controls, measuring the state of the security control at a single point in time. While implementing baseline controls may be an initial milestone, it shouldn't be the only consideration when designing a DPCP.

This mindset stops short of establishing control environments that demonstrate a commitment to competence, a sound organizational structure, assignment of authority, and responsibility with information security policies and practices. The 9 Factors of Control Effectiveness and Sustainability address the components of a security compliance program to ensure that initial compliance is not only met, but is maintained over time. Otherwise, organizations are not able to satisfy the three fundamental control objectives of internal controls (ORCs):

- **Operation objectives**
  The effectiveness and efficiency of the data protection and compliance operations
- **Reporting objectives**
  The reliability, timeliness and transparency of data protection and compliance reporting
- **Compliance objectives**
  Compliance with regulations, not merely on paper, but based on evidence that demonstrably provides reasonable assurance that objectives are achieved and maintained under a framework with an effective system of internal controls

Deep questions to ask—and answer—in advancing your program

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

Here are our deep—or tough—questions for you to consider:

1. **What data do you have, where is it and how does it flow?**
   Are you sure you know where all your data is, and who is responsible for it? How do you keep track of the data you have? Do you know exactly where all the data is that needs to be protected? How much control do you have over sensitive data flows through your environment? Are you tracking all locations? In real time?
2. **Are you secure enough? How confident are you about the protection of your data?**
   How do you know your payment card data is secure? Based on what evidence? Which metrics do you track to answer this question? Does compliance mean your data really is secure?
3. **How confident are you that the right controls are effective and in the right places?**
   How does your control design process identify the controls that are needed? What evidence do you have for the effectiveness of your controls? Do you measure control effectiveness for all controls?
4. **How predictable is your data protection compliance program (DPCP) performance?**
   With how much confidence can you predict the outcome of your key DPCP objectives, and can you do so at any point in time?
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? How repeatable and consistent are your key processes? Can you predict success or failure with a degree of certainty ahead of time?
6. **How quickly can you detect and respond to policy, standard and procedure deviations?**
   How do your expectations on event detection and incident response meet reality? What about your expectations of response with corrective actions?
7. **Do you have controls in place to measure the effectiveness of your DPCP implementation and maturity strategy?**
   How well does it align with industry frameworks such as COBIT, COSO or NIST CSF, and is it able to meet your control objectives? Does your strategy cover all the essential bases, or do you have ongoing gaps in your DPCP strategy?
8. **How do you know that you are prioritizing the right DPCP activities at the right time?**
   Did you prioritize the correct objectives? With resources being limited, how do you know your team is spending time on the right tasks?
9. **How well are you managing the 5 Constraints of Organizational Proficiency: capacity, capability, competence, commitment and communication?**
   Do you have visibility into your organizational ability to manage each of the five constraints?
10. **How well do you understand the 9 Factors of Control Protection Effectiveness and Sustainability? What target maturity levels are you working to achieve in the long term?**
    Do you know where you are with control effectiveness and sustainability, and what your organization's capability will be in one year's time?

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

The 9 Factors of Control Effectiveness and Sustainability

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.[5]

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 the 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 organizations achieve repeatability, consistency and highly predictable outcomes.

The Verizon 9-5-4 Compliance Program Performance Evaluation 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 optimum capacity. (See page 13 for a comprehensive explanation of how this practical, new Verizon framework can evolve your sustainability and maturity program.)

Figure 2. A relational model of the 9 Factors of Control Effectiveness and Sustainability

Factor 1 is the core from which the other factors emanate. After achieving the objectives of the earlier factors, the final outcome, Factor 9, is the ability to self-assess, the output of which can then be used to improve all the factors.

Qualified Security Assessors (QSAs) and other security professionals break your control environment down into components or elements of documentation, processes, technology and people. They analyze each of these components separately, evaluating how each component either enhances or detracts from supporting sustainable control effectiveness. Then the QSAs synthesize the analyses for a complete understanding. This approach differs from what may be the layperson's approach, which is to reach a conclusion of control environment effectiveness without the thorough and discrete analysis of components. The Verizon 9-5-4 Compliance Program Performance Evaluation Framework can help anyone approach control environments more like a qualified security assessor.

5 Verizon 2018 Payment Security Report, page 15

The 5 Constraints of Organizational Proficiency (5 Cs)

In the 2018 PSR, we introduced the 4 Constraints of Organizational Proficiency, i.e., the 4 Cs: capacity, capability, competence and commitment. Based on industry feedback, we are expanding this to five (5) by adding communication.

Capability self-check

1. How capable is your organization today at managing its data protection and compliance risk profile?
2. How capable does it need to be?
3. How can it get to its desired state? By when?

Figure 3. The 5 Constraints of Organizational Proficiency

Capacity

Capacity describes the quantity of something, whether it is sufficient in order to achieve and complete the outcome. This could be the amount of space (e.g., cubic capacity), number of people or even number of hours. In considering whether a team has the capacity to do something, we are really looking at whether they can complete it within a specific timeframe. Do you have the amount of time and enough team members to produce and deliver your data protection objectives over an extended period?

To solve capacity constraints, you can campaign to increase the resources available or decrease the components (especially systems and processes) included in the scope of your data protection program and overall internal control operations.

Capacity also covers funding and resources. Does sufficient staffing exist for compliance personnel to effectively audit, document, analyze and act on the results of the compliance efforts?

Organizations often focus on the capabilities required to succeed, but they should also be mindful of the capacity needed to deliver successfully. A successful organization is aware of all of its assets, understands the business and data protection capabilities required, has sufficient capacity, and is competent in its delivery.

Capability

Capability describes the ability to perform a specific set of actions or achieve a specified set of outcomes. To have capability, individuals and teams need the capacity and skills to perform necessary actions. From an organizational perspective, it is the ability to apply and direct resources to perform data protection tasks and the processes to support them—a condition that permits an individual and an organizational unit to learn and accomplish tasks within their capacity.

Capability is also known as implied abilities, or abilities that are not yet developed. Individuals and teams have the potential to acquire a specific ability or skill that will be helpful in performing tasks. The learned skill or ability adds to the knowledge bank or skill set. It is a collaborative process that can be developed or improved with new skills that makes individuals and teams more capable to complete tasks. In short: Do they understand the processes, and do they have the required equipment?

Data protection capability is often more of an internal struggle of priorities rather than IT or external constraints placed on the organization and its operations. Some organizations lack the qualities (leadership, culture, structure or incentives) to invest in developing sustainable data protection and compliance. The data protection capability of all organizations depends on their potential to direct and apply resources toward internal control, and supporting the DPCP against the allocation of resources elsewhere.

Distinction: Capability is the condition of having the capacity to do something; competence is the improved version of capability. Competency is the possession of the skills, knowledge and capacity to fulfill current needs. It also includes the ability to develop and flex to meet future needs. Capabilities include the active utilization of tools, such as information technology, to manage the program, the data and security. Competency is the effective and efficient use of those tools. Capabilities serve as the starting point of being able to do something and gradually becoming more adept in performing the task. With time and practice, capability can develop into competence.

Adapted from "Ability, Capability, Capacity and Competence," by Kim Parker, The Knowledge Economy, 2016, http://theknowledgeeconomy.blog/2016/04/12/ability-capability-capacity-and-competence/

Competence

Competence describes the quality or state of being functionally adequate, of having sufficient knowledge, strength and skill to do something well enough. Competence is another word for skill or expertise.

Skill has many synonyms, such as ability and competency, which is defined as "the ability to do things well." "Doing things well" implies that actions are effective and efficient for delivering good performances. Effectiveness relies on identifying the right things to do (for example, daily security log monitoring and alerts). Skill is concerned with how to do things in which the skill owner can achieve proficiency. Therefore, competence starts as a person's capabilities. In a sense, competence is proven abilities and improved capabilities. Competence can include a combination of knowledge, basic requirements (capabilities), skills, abilities, behavior and attitude.

It is the quality or state of being functionally adequate or having sufficient knowledge, strength and skill to deliver what is required, such as the knowledge, skills and experience needed to establish and maintain effective controls within a sustainable control environment. Competence, therefore, is another word describing the know-how or skill of an individual or organization. It is the state or quality of an individual or business unit's work. The work can be evaluated as competent if the performance is considered satisfactory but not outstanding.

Competence can also be applied to the improvement or development of one's abilities and skills for the benefit of the person and the group or institution he or she represents. In considering whether a team has the competence to design, implement, monitor and evaluate a compliance program, we are really looking at their effectiveness. Do they have experience with that process or the right training to follow procedures and use supporting IT systems?

Commitment

Commitment describes how willing an organization is—from the board of directors through middle management to each individual—to support a program or objective. The compliance function should have visible support, autonomy, independence and adequate resources, as well as direct participation in steering committees. (See page 14 on steering committees.) To have any assurance in your compliance program, you need commitment.

Organizational commitment ranges from failure to fully committed human and financial resources in support of a robust program. Lack of commitment manifests itself in various ways: failure to understand and address the need for control design or control lifecycle management; deficient engagement on performance and maturity management; development of what amounts to a program that looks good on paper but does not embed effective business processes across an organization.

Assurance is an integral component of commitment. It demands consistency of application and across-the-board discipline to adhere to standards and programs.

The effectiveness of a compliance program requires high-level commitment by an organization's leadership to implement a culture of compliance. The organization's top leaders—board of directors and executives—set the tone for the rest of the organization. How does middle management, in turn, reinforce data protection and compliance standards, and encourage employees to abide by them? Executive leadership and middle management are equally important for setting an example of required behaviors and maintaining the tone at the top. The compliance function should have visible support, autonomy, independence and adequate resources from senior leadership—with broad, direct participation in steering committees.

The documentation of commitments typically includes the following:[6]

- Describing the commitment
- Identifying who made the commitment
- Identifying who is responsible for satisfying the commitment
- Specifying when the commitment will be satisfied
- Defining the criteria for determining if the commitment was fulfilled

verizon business ready

6 Adapted from "CMMI for Development Guidelines for Process Integration and Product Improvement, 3rd ed.," Mary Beth Chrissis, Mike Konrad, Sandy Shrum, Addison-Wesley, Pearson Education, 2011, 214. Reprinted by permission of Pearson Education, Inc., New York, New York.

Communication

Communication describes the ability to achieve clarity and focus on the objectives, tasks and responsibilities, internally and externally, to do the right things, in the proper manner and at the right time. Focusing on good communication is essential to streamline any type of data protection program management process.

The four basic types of business communication essential to mature your DPCP are: internal (upward), internal (downward), internal (lateral) and external.[7]

Internal upward communication:
Anything that comes from a subordinate to a manager or an individual up the organizational hierarchy.

Internal downward communication:
Any type of communication that goes from a superior to one or more subordinates with no room for interpretation on compliance requirements; the language should concisely explain exactly what needs to happen.

Internal lateral communication:
The talking, messaging and emailing among coworkers in the office. This might be cross-department communication or just internal department dealings.

External communication:
Any communication that leaves the office and deals with third parties. It could also involve regulatory bodies

There are a lot of communication constraints, such as physical separation, wrong communication channels, not understanding your audience's needs, and distractions that affect the communications management plan and limit the success of a compliance program. Communication is the lifeblood of the program and each project.

Compliance managers need to understand the 5 Cs to effectively mature and evolve their program. We added communication because without it, program maturation is at risk of being stymied or completely stalled.

The 4 Lines of Assurance

A theoretical assurance model appears in a position paper published by the Institute of Internal Auditors (IIA) titled, "The Three Lines of Defense in Effective Risk Management and Control."[8] This model received a fair amount of critique for its perceived oversimplification. An extended model called the Five Lines of Assurance[9] was proposed to correct the deficiencies in it. In our opinion, the four-lines model, which we developed, is a better fit for the payment security environment.

1. **Individual accountability**
   Assurance comes directly from work units: 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 they are executing risk and control procedures to maintain adequate internal controls. While they 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.
2. **Risk management and compliance functions**
   Risk and compliance teams are the specialized support units responsible for monitoring the implementation of policies and procedures, and serving as the management oversight over the first line. It is the role of the second line to provide the systems and advice necessary to integrate risk management and compliance into key processes and allow the front line to manage for success, and to ensure that the first line of assurance is properly designed, in place and operating as intended. As a management function, the second line of assurance cannot offer truly independent analyses.
3. **Internal audit**
   The internal audit function provides a level of objective, independent assurance, and also timely information to the board that the 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. Internal audit's role is largely detection and corrective, i.e., detect control weaknesses or breakdowns and suggest improvements or remedial action.
4. **External auditors, regulators, external bodies**
   Independent auditors and assessors should provide assurance on the effectiveness of governance, risk management and internal controls. They should evaluate the manner in which the first three lines of assurance achieve control objectives. External assessors provide comprehensive assurance based on a high level of independence and objectivity because they reside outside the organization's structure.

All lines of assurance should work together. Each step in the lines-of-assurance model has a purpose and can promote efficiency and effectiveness through information sharing. You should coordinate activities among the groups responsible for managing the organization's control environment.

verizon business ready

7 Adapted from "Types of Business Communications," Kimberlee Leonard, Houston Chronicle, January 31, 2019, https://smallbusiness.chron.com/types-business-communications-697.html

8 "The Three Lines of Defense in Effective Risk Management and Control," Institute of Internal Auditors, January 2013, https://www.theiia.org/3-lines-defense

9 "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," Tim J. Leech and Lauren C. Hanlon, Wiley & Sons, 2016

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?
- 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 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 4. Compliance Program Performance Evaluation Framework

Figure 4 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 control points (180 in total) 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 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 organization proficiency (i.e., constraint) as it applies to each of the 9 Factors within the chosen line of assurance. A proficiency becomes a constraint when it is underdeveloped because it introduces limitations and restrictions. You can expand the lines of assurance as needed, such as by explicitly adding executive management and board oversight. You can also expand the 5 Cs by adding culture as an additional organization proficiency.

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 the NIST CSF, COBIT and COSO.

Measuring
Organizations can measure control effectiveness and use this data to precisely tailor controls across the environment.

Individually, these components are rather simple, but when combined artfully, they allow you to construct a formidable data protection program.

Steering data protection maturity—the captain's role

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.

Proficiency is critical

Security professionals with the right skills and experience should know how to prioritize their directives and program objectives. Data protection and compliance problems are like opportunities: More of them exist than an organization can simultaneously address. Not all data protection and compliance problems should necessarily be addressed: It is crucial to focus and prioritize appropriately.

Organizations need to document detailed performance standards for their control environments. This process is essential to identify problems and define acceptable vs. unacceptable deviations. When deviations from defined standards exist, and when security incidents occur (such as the decrease in control performance, the design or operational failure of a control or both), the root cause typically is not a single component of the control environment. When multiple contributing factors to a security control failure are unaddressed over time, the failure will likely happen again. The application of a systematic evaluation with risk management techniques can help differentiate one-time events from critical recurring problems.

Moving from reactive to proactive

In gaining control through strategy and program design, CISOs must keep in mind that information security program strategy is all about the how. How will you evaluate and select from the possible paths forward? Too often, data protection programs are developed in an ad hoc manner, in a reactive mode with little advanced planning. A well-defined program strategy provides guidance on how to make decisions and allocate resources to achieve overarching program objectives.

When an organization's security direction becomes a series of disjointed initiatives and policies, the outcome is inevitable: a drop in compliance, reduced control effectiveness and increased risk of a breach. The CISO must provide agile leadership and well-structured governance supported by clear communication and strong directives.

For many organizations, a large part of the journey in PCI security and compliance is about moving from a disjointed set of activities to creating a formalized program. The question of strategy gets to the heart of what it takes to move a program forward. Instead of short-term projects with small, immediate goals, security must evolve into a long-term program with a mission, objectives and strategy that improve the security posture of the organization.

The key objectives of the CISO often include formulating an information security program that leverages collaborations and organization-wide resources; facilitating information security governance; advising senior leadership on security direction and resource investments; designing appropriate policies to manage information security risk. (See Appendix E for an infographic on CISO's responsibilities.)

Mature programs offer services that form a cohesive and coordinated effort led by mindful CISOs. Program objectives should lead to a coordinated set of efforts to achieve each goal over time, structured under a handful of overarching yet clearly defined objectives.

Project vs. program management

Data protection program management is a structured organizational process for the ongoing direction and application of internal and external resources (people, time, budget, processes and technology). Its purpose is to meet defined objectives by integrating the management of related projects in a coordinated manner to obtain benefits and control that is not available when managing them individually.

Program implementation includes activities such as the formulation of a program strategy and facilitation of decisions to define and control (plan, execute and monitor) the tasks for the achievement of program objectives. This is accomplished by executing multiple related projects to implement policies, standards, procedures, awareness (communication), directing and developing skills (education, training), motivation and incentives, performance evaluation, and continuous improvement.

The intent of a data protection compliance management program is to design and execute a governance framework and maintain control over the program activities' extended periods of time. This provides the best possible chance to succeed in achieving the stated objectives with the available resources.

Program benefits include improvement of performance among participating projects through integration, alignment of objectives, economies of scale and broad oversight.

Therefore, the difference between a program and a project is not merely that a program is an ongoing, longer-term endeavor to coordinate a collection of projects. While the project manager's job is to ensure that their project succeeds, the program manager, on the other hand, is concerned with the aggregate outcome(s) or end-state result(s) of the collection of projects in a particular program.

Red flags and program performance indicators

The PCI DSS requires security policies, standards and procedures to be updated annually. How do you know whether managers and other employees are reading and following them?

In his book "The Checklist Manifesto," author Atul Gawande provided some good examples of how checklists can pop up in unusual places with great effect. One was a story of the rock band Van Halen—an American heavy-metal band distinguished by the innovative electric-guitar playing of Eddie Van Halen. They were one of the first big-name bands to take huge roadshow productions. Whereas the usual stage shows would turn up at a venue with two or three eighteen-wheelers of stage equipment, Van Halen would roll into town with nine eighteen-wheelers packed full of gear. With that much equipment, there was always a concern that the stage flooring wouldn't be strong enough to support the extra weight.

To avoid problems, the Van Halen management team would have a huge contract with concert promoters–described by some as being like a version of the Chinese Yellow Pages. So just as a little test, buried in the middle of the rider would be Article 126, the no-brown-M&M clause, which specified that a bowl of M&Ms would always be placed backstage that contained no brown M&Ms. If the brown M&Ms were not removed, the show would be cancelled, and full compensation would be paid to the band. Although at first glance this appeared to be another insane demand of power-mad celebrities, it was actually a checklist item to ensure that the promoters fully understood and complied with the technical requirements of staging the show.

When David Lee Roth, the lead singer of the hard-rock band, saw a brown M&M in the candy bowl, he would line-check the entire production. Guaranteed, he would find technical errors and discover problems. These weren't trifles. Such mistakes could be life-threatening. At an event in Colorado, the brown M&Ms alerted the band to the fact that the local promoters had failed to read the weight requirements, which could have resulted in staging falling through the arena floor.

Other times they found undersized access doors, and so forth. By integrating this simple but bizarre-sounding checklist item into their performance contracts, the band's management team could distinguish the thorough promoters from those trying to cut corners. Van Halen used the candy as a warning flag for an indication that something may be wrong. There are lessons to be learned from this approach for PCI security compliance.[10]

Compliance program potential pitfalls

The well-known symptomatic indicators and program management pitfalls of a DPCP that struggles with constraints ranging from capacity to commitment issues include the following:[11]

Constraints	Common symptoms
Commitment	**1. Lack of leadership** – Compliance needs leadership and support from senior as well as middle management.
	2. Insufficient profile of the compliance function – The compliance function should have a "seat at the table" at senior levels of organizations for it to be effective.
Communication	**3. Competing priorities and incentives** – Organizations must balance compliance issues so that one compliance issue or initiative does not take priority over others and create competition for compliance.
	4. Insufficient communication and training – Training should move beyond one-size-fits-all packages (the one-hour-once-a-year model) and be tailored to the business and cultural issues employees will face.
Competence	**5. Failure to assess and understand risks** – Organizations should understand the risks, which include control risk and maintaining clarity on residual risk.
Capability	**6. Insufficient third-party management** – Organizations must train third parties on their compliance policies and requirements.
	7. Lack of clear procedures to make policies accessible – Policies should not be written in overly complicated jargon or legalese or assumed to be understood by overseas offices that may be operating in several languages.
Capacity	**8. Insufficient monitoring** – Organizations must monitor the performance of their compliance programs effectively.
	9. Insufficient resources – Organizations should provide adequate human and financial resources, or compliance programs will struggle to achieve objectives. Organizations often resort to compensating controls as a short-term fix.

Figure 5. Compliance program potential pitfalls

10 Adapted from "The Checklist Manifesto: How To Get Things Right," Atul Gawande, Profile Books, 2009, 80; see David Lee Roth explain the story at: https://vimeo.com/36615187

11 Adapted from "Why Anti-corruption Programs Fail: Turning Policies into Practices," Center for Responsible Enterprise And Trade (create.org), 2015, https://create.org/resource/why-anti-corruption-programs-fail-turning-policies-into-practices/

Companies worldwide are already spending large sums on compliance and should ensure that the resources are well spent. Better measurement can help managers identify redundant or ineffective initiatives that they can replace or eliminate—and ultimately reveal opportunities to make programs more effective.

Program management design mistakes

The following are typical program management design mistakes that organizations make:

- Failing to secure early stakeholder buy-in when establishing the compliance program
- Failing to clearly identify goals and desired outcomes (which should include building in sustainability and effectiveness of the control environment)
- Setting up a project instead of a program
- Applying a narrow frame from a project management perspective
- Focusing on project rather than program outcomes
- Failing to establish clear program objectives; focusing on compliance and not on data protection
- Underestimating the comprehensive nature and complexity of a data protection program, thereby not securing the capabilities needed for ongoing support of the program
- Failing to build sustainable processes supported by the 5 Cs
- Maintaining organizational silos—hampering communication, performance and sustainability
- Focusing on technology; undervaluing processes and procedures
- Forgetting, underinvesting, rushing—inadequate organizational competency development
- Falling short on training and educational efforts

Navigating data protection and compliance program management

The history of navigation spans centuries. From the days of prehistoric dugout canoes and Viking ships to SpaceX and GPS, navigation has aided civilization. Managed by rudders, steering wheels or stars, navigation provides humankind with strategic direction.

Organizations implement navigation for guidance and direction in the form of steering committees. These entities are central to the initiation, design, implementation and management of long-term compliance programs—such as PCI security compliance programs.

In payment security, steering committees play significant roles in the data protection and compliance priorities of organizations and manage the general course of operations. They help to steer the position, course and even the distance traveled of security practices. By definition, they are a form of corporate governance made up of high-level executives, authorities and stakeholders who provide strategic oversight and guidance to one or more projects central to organization. They meet at key stages during the course of a project and influence strategic decisions. In short, a steering committee does exactly what its name suggests: steering projects, programs and organizations toward desired successful outcomes.

While their primary purpose in payment security is to direct data protection and compliance programs, steering committees also fill several important roles, including:

- Giving input on issues concerning the development of a project or organization
- Providing insight on concerns related to the budget, marketing, hiring, etc.
- Determining what outcomes need to be realized through a project or undertaking
- Prioritizing steps and goals that need to be taken and realized in a project
- Helping develop policies and procedures relevant to a project or operation
- Projecting potential risks and monitoring or eliminating them as required
- Setting timelines and monitoring progress
- Offering advice on business or project topics for which they have oversight

General data protection program management principles

The following are general principles that apply to the design, management and evaluation of data protection programs:

A control environment's overall behavior depends on the entire structure.
You cannot break apart a system and deal with its parts individually without recognizing the interdependency. When you break apart an elephant, you do not have a bunch of little elephants. Similarly, when you break apart a compliance environment, you do not have a bunch of independently functioning controls—you have interdependent controls and control systems that are part of a control environment.

A circular relationship exists between the overall system and its parts.
Data protection and compliance problems cycle through an organization. You need to recognize the patterns of events and realize that they are not just events themselves. Look at the events in the context of the overall system and figure out how to break the vicious cycle of unnecessary or prolonged problems.

Structures determine behaviors, which determine events.
Focusing on events and attempting to deal with them in isolation, i.e., without considering the structures and systems in the organization that caused or contributed to those events, does not facilitate developing robust strategic solutions. Identify which of the 5 Cs of Organizational Proficiency need to be addressed to solve the problem, which lines of assurance are impacted and how the 9 Factors can help avoid problem reoccurrence.

Problems usually lie in the relationships between parts.
If the strategic planning of a data protection program does not address the integration of goals and plans, all kinds of problems can ensue. The problem often becomes conflicting demands placed on people and teams within the organization. For example, employees may have conflicting roles, resource allocations are sporadic and inconsistent, services are less efficient, and compliance processes may not be getting adequate administrative support.

Long-lasting change emerges from changes to structures.
Inexperienced CISOs attempt to change the data protection and compliance performance of the organization, preaching at teams and individuals while producing no solid results. Experienced CISOs learn that to effect long-lasting change among their employees, it is essential to establish a sound structure with clear roles, goals and responsibilities, and to monitor progress toward those goals.

Today's problems are yesterday's solutions.
Often, organizations fail to see the long-term ramifications of applying their favorite quick-fix solutions. For example, opening up ports on a perimeter firewall with the intent of resolving an outage with a public-facing web application that mysteriously stopped responding. In reality, a new security risk is then introduced by exposing additional services unnecessarily, when what should happen is that the developers should fix the app. Quick fixes to symptoms rather than addressing the actual source of a problem may make things appear better in the short term, but Band-Aids will continue to need to be applied until the wound is healed.

The harder you push, the harder the system pushes back.
It does little good to tell a compliance team to just "suck it up" and do a better job when dealing with any of the 5 Cs. Their performance will likely decrease, and they will feel more frustration, anger and despair. Rather than coming to them with dire warnings about the potential consequences of data protection and compliance failures, first listen to the employees and members of the board to hear each side of the story.

The easy way out usually leads back in.
Doing what is familiar is easy and comfortable. This mindset is why compliance teams often resort to doing what they were already doing when they realize that their program is struggling. They just do it harder. Perhaps H.L. Mencken said it best, "For every difficult and complex problem, there is an obvious solution that is simple, easy and wrong."

Faster is slower.
If leaders do not take the time and energy required to develop and implement effective data protection and compliance plans, it might seem like they have more time to attend to the day-to-day matters in their organization. They soon realize that they are attending to the same problems repeatedly. This does not mean that leaders should not make decisions and act quickly—it means that most of those quick decisions should be guided from defined plans, policies and practices.

Adapted from "Field Guide to Consulting and Organizational Development: A Collaborative and Systems Approach to Performance, Change and Learning," Carter McNamara, Authenticity Consulting, 2006, 422.

Program management approach

The maturity of a compliance program 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.

Successful, continuous compliance improvement and sustainability seldom, if ever, diverge from a systematic and 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."[12]

How do you define compliance program management success?

The design of a DPCP is critical to that success. Getting it right the first time will save you time, money and the overall sanity of your workplace, but requires considerable clarity and commitment to doing the right things right, which depends on:

- How well the program is structured
- What and which outcomes you focus on
- The assignment of resources and priorities

Not defining data protection program management success is a typical program management design mistake. The definition of success is vital to drive the program toward outcomes that will support control effectiveness and sustainability.

12 "Management Cases, revised edition," Peter F. Drucker, 2009, reproduced with permission from the Drucker 1996 Literary Works Trust

A successful program management habit: Begin with the end in mind

Start your program by defining the exact outcomes you want to achieve—with clarity. At the end of your initial program development, you want to have an environment with clear visibility on program performance—both in terms of individual project performance and how predictable you can be achieving your key milestones and overall program objectives.

Achieving this clarity and predictability milestones is done by optimizing the in-house and acquired capacity, capability, available competence, commitment and communication across all lines of assurance.

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. Components to include in your evaluation:[13]

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—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 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 its line of business? (For more on how to answer these questions, refer to the Verizon Data Breach Investigations Report,[14] Verizon Insider Threat Report,[15] and Verizon Incident Preparedness and Response Report.[16])

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 employees' 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 deviances 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 through 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?

verizon business ready

13 Adapted from "Evaluation of Corporate Compliance Programs – Guidance Document," U.S. Department of Justice Criminal Division, April 2019, https://www.justice.gov/criminal-fraud/page/file/937501/download

14 Verizon Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir

15 Verizon Insider Threat Report, https://enterprise.verizon.com/resources/reports/insider-threat-report/

16 Verizon Incident Preparedness and Response Report, https://enterprise.verizon.com/resources/reports/vipr/

Define success

A DPCP can be considered successful when it progresses toward and delivers a mature control environment with the ability to improve continuously, 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 is sustainable, with a level of assurance of robustness and resilience, i.e., the ability to operate without significant deviation from its performance standards for extended periods with the available resources. 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 DPCP.

Some components of a successful data protection strategy and maturity navigational map include:

- Clearly defined program objectives, activities and priorities supported by all stakeholders
- Adequate capacity, capability and competence
- A structure that maximizes the problem-solving capability

Data protection compliance metrics

W. Edwards Deming's book, "Out of the Crisis," notes that "what you cannot measure, you cannot improve." With the appropriate metrics, an organization will have a basis to determine how and where to allocate limited resources. Thus, measurements and metrics provide avenues for organizations to gain a more concrete understanding of the effectiveness of their DPCPs. Various metrics (coverage, impact, performance, etc.) should be constructed to encourage performance improvement, effectiveness, efficiency and appropriate levels of internal controls across the DPCP.

Measurement and metrics defined

- Measurement refers to a specific, single, point-in-time snapshot of raw data
- Metrics compare predetermined baselines against a series of measurements taken over time and provide objective interpretations of the data collected through the measurement process

Why use metrics?

Metrics can facilitate better awareness and better decision-making. They can provide a consistent and repeatable framework for the analysis of complex situations and a mechanism for identifying broken processes or unusual activity. This allows executives and managers to monitor performance and identify corrective actions.

When management communicates the key metrics to measure organizational compliance, it contributes to the culture of compliance within an organization. Metrics help demonstrate effectiveness in the process (i.e., structural or design changes) and outcomes (i.e., behavioral changes) and assist in focusing limited resources to higher priority areas. They help demonstrate the risk tolerance of an organization.

The purpose of governance metrics is to provide the information needed by senior management, including executive-level security managers, to make the decisions necessary for long-term guidance of a security program. Metrics also provide assurance that the security program is operating according to internal performance standards. Overall, a quantifiable, objective measurement will assist in showing the return on investment of a compliance program.

Metrics should be reviewed regularly to ensure that they apply to the program and control objectives. The outcome of metrics data analysis should focus on reviewing the main contributors and, where possible, the root cause of an identified systemic issue. The result should be fixing the problem vs. fault-finding. Control deficiencies should not be treated as limited aberrations that will resolve on their own volition. The appropriate application of metric analysis and reporting is essential to achieve a sustainable and effective control environment. However, metrics are not the end-all of demonstrating control environment effectiveness. They provide indicators that can show a positive or negative trend in a specific operational area, such as access control, system hardening, security management, vulnerability management, etc.

Metrics evolve with program maturity

Organizations use various drivers to implement a DPCP. For many organizations, the main driver is to satisfy contractual obligations and regulatory pressures. Whatever the reasons for implementing a DPCP, they should not just be about identifying and implementing required security controls. The effectiveness of the control environment must be measured, reported and improved. Without knowing how to measure the function, robustness and resilience of security control systems, how do you know that they are working effectively?

A correlation often exists between the maturity of DPCPs and the maturity of security program and control performance metrics programs. Organizations should develop and maintain metrics programs according to organizational maturity in their compliance program and activities.

The PCI DSS (v3.2.1. and previous versions) does not include explicit requirements for measuring and reporting on the effectiveness of the control environment. While many compliance officers seem to understand that the opportunity is there for the taking, they are failing to employ metrics programs and technology for a better understanding of the effectiveness of their compliance programs.

A basic high-level presentation of compliance program maturity is presented in the following table.

	Emerging	Evolving	Mature
Metrics maturity	• No objective measure of quality • A basic and underdeveloped measurement program • Metrics collection, analysis and reporting not integrated into business-as-usual processes • Incomplete definition and communication of metrics collection methods • DPCP performance not actively measured	• Narrow scope – a focus on coverage metrics only, tracking the completion of tasks, without measuring and reporting effectiveness • Compliance issues remain unaddressed due to lack of mitigation efforts, despite metrics and reporting	A developed metrics program that frequently measures and reports on: • Control environment performance and its effectiveness • Individual control system performance and effectiveness with effective facilitation of non-compliance mitigation
Program maturity	• "Put out fires" mentality • Low performance visibility • DPCP processes undefined • Incomplete definition and communication of objectives and outcomes • Project activities not directly tied to strategic DPCP objectives and outcomes • Lack of technical and business tools to support DPCP • Lack of standardization • Responsibilities not assigned	• "Planning" mentality – many deliverables in progress with future-dated outcomes • Incomplete documentation: processes selectively defined and documentation in progress • Technical and business tools selectively identified • Ad hoc implementation, configuration and tailoring • Rigid operations	• Proactive, "anticipatory" mentality • Defined and documented DPCP processes, with high organizational awareness and understanding • Technical and business tools used to enhance competitive advantage • Flexible, adaptive operations

Figure 6. Security program and metrics maturity correlation

What should be measured?

For ease of explanation, the performance measurements of compliance programs can be broken down into the following categories:

- **Management controls:** Data protection strategy, compliance strategy, business and compliance objectives, policies, standards, procedures, improvement plans, management reviews
- **Business processes:** Risk assessment, risk treatment, incident preparedness and response
- **Operational controls:** Operational procedures, change control, control design, control implementation and review, capacity management, release management, back up, secure disposal, equipment off site, problem management
- **Technical controls:** Configuration management, system hardening, vulnerability management, software patch management, access control, antivirus controls, intrusion detection systems (IDS), firewall, content filtering

The application of the Verizon 9-5-4 Framework offers a practical model for measuring the performance of the 5 Cs across each of the 9 Factors and to report the performance of each line of assurance.

To establish your measurement criteria:

- Confirm, through risk assessment, the need for additional controls beyond those prescribed by the PCI DSS
- Align metrics program objectives, ensuring they map back to the business and data protection program objectives
- Identify the criticality of control systems to the successful operation of the control environment
- Identify the frequency of control measurements by the nature and criticality of the control
- Establish a baseline, against which you can compare all future measurements
- Use existing indicators wherever possible—key performance indicators (KPIs) help define and measure progress toward a particular goal

Measuring various elements of any DPCP must include several perspectives, such as the extent to which a control is successfully deployed, the performance of a control when it is in operation and the effectiveness of a control in meeting the defined objectives. Metrics should be defined to monitor these nuanced aspects of control performance.

Metrics—Strategic, management, operational

"It is important to understand the distinction between strategic, management, and operational metrics. Though they are easy to obtain and abundant, most technical IT operational metrics are of little use in determining strategic direction or managing an information security program. This can be likened to the operation of an aircraft that has three types of basic instrumentation. One is operational information regarding the machinery, such as oil pressure, fuel supply, temperature, and so forth, which is analogous to IT metrics. The second is aircraft management information such as airspeed, attitude, heading, and altitude, which is needed to manage the aircraft properly but, ultimately, only relevant if the destination is known. Flying safely in circles is not likely to be very useful. The third is navigational or strategic information including direction to the destination and position.

All three types of information are necessary for proper operation and to meet the overall strategic objectives of the organization such as operating an airline. Whether operating an airline, manufacturing widgets, or managing a security program, the issues are the same and the types of information required are as well. The majority of organizations nevertheless attempt to operate security using primarily operational information, which makes as much sense as flying aircraft without knowing position or destination, attitude or altitude."[17]

Control coverage measures the deployment status of a security control across a total population of components. It characterizes how far a solution was implemented and tracks inconsistencies in deployment. The closer this value is to 100%, the more complete the implementation of the control. As an example, you can use Windows Server Update Services (WSUS) to monitor the completion of a Windows patch rollout to a desktop estate or the completion status of annual security awareness training across all employees. Any deviation below 100% should be examined carefully and ultimately justified. Typically, this metric can be broken down by location, owning business unit, type of device, type of vulnerability or severity. The goal is to achieve measurements as close as possible to 100%—i.e., total coverage.

verizon business ready

17 Republished with permission of Wiley & Sons from "Information Security Governance: A Practical Development and Implementation Approach," Krag Brotby, 2009, 27; permission conveyed through Copyright Clearance Center, Inc.

Control effectiveness measures the extent to which controls were designed and implemented and are supported by processes. This could be represented as the percent of controls that meet control design standards, control risk standards and control operation standards. As an example, the number of issues identified in an application vulnerability assessment could be used as a measurement to determine the effectiveness of the software development lifecycle process.

Operational performance measures the number and severity of deviations from performance standards and speed in which teams corrected them. For example, the number of compliance tasks completed on time during each month and quarter, and time to close for any corrective actions. This can, for example, incorporate mean time to repair (MTTR) measurements to track how long it takes on average to remove a control performance deficiency after discovery. The metric can be expressed in some unit of time: hours, days, weeks, etc. In general, the lower the value of this metric, the less time threat actors have to exploit vulnerabilities.

Program impact metrics convey the impact of the compliance program on the organization's mission, i.e., program milestone reporting that provides ongoing progress toward a strategic goal.

Provide periodic reports to the DPCP steering committee, appropriate management teams and core business process and system owners. These should illustrate metrics over time, provide mitigation recommendations where necessary and track the status of corrective actions.

Defining metrics collection and analysis profiles

Each measurement requires a proper definition, which can include:

- A descriptive title
- A defined scope
- A purpose and objective
- Chosen indicators
- A defined measurement method
- Measurement frequency
- Data source and data collection procedures
- Date of measurement and responsible personnel
- Level of effectiveness achieved (or level of maturity, in case of a maturity metric for controls), with causes for non-reproducible and contrastable measurement that should facilitate corrective action
- A checklist to determine the quality of metrics

It is essential that each metric be relevant to decision making. Ask yourself:

Is the metric objectively measurable?
It should express something objective and repeatable.

Does the metric include a clear statement of the end-results expected? What is the decision that the metric is supposed to support?

Does the metric focus on effectiveness and/or efficiency of the system being measured?

Does the metric allow for meaningful trends or statistical analysis?
It should be expressed as a number or give a result as a percentage, ratio or some other kind of actual measurement. It should not be expressed as subjective opinions, such as "low risk" or "high priority."

Does the metric include milestones and/or indicators to express qualitative criteria?
It should contain units of measure—time, dollars or some numerical scale. It should not just say "red," "yellow" or "green" risks.

Are the metrics challenging but at the same time attainable?

Are assumptions and definitions specified for what constitutes satisfactory performance?

Were those responsible for the performance being measured fully involved in the development of this metric? Has the metric been mutually agreed upon by the stakeholders?

Was the metric evaluated to determine if it supports the organization's information security program goals and objectives, and ultimately the overall organization's mission?

What is the value to measuring it further?

Why do some CISOs consistently command the budget and resources they need while others struggle? What can budget-constrained CISOs do to garner the support they need for their programs? A research report from the Institute of Applied Network Security (IANS) by Phil Gardner, Founder and CEO, reveals the following successful strategies from CISOs (see iansresearch.com).

Owning the security narrative within the organization is important:

Stories beat metrics: Although metrics can be powerful tools, several CISOs argue that when it comes to securing a budget, it's more important to deliver cogent stories.

Craft long-arc and short-arc stories: CISOs who master the art of driving the narrative tend to develop two classes of security stories. One type tells a multi-year story of integrating InfoSec into the fabric of the organization. This long-arc narrative understands the business and articulates how InfoSec powers growth and profitability. The short-arc stories detail particular investments and how they improve risk posture. Importantly, these two classes of security stories are coherent and fit together well.

Build internal channels and alliances: Stories need audiences. When successful CISOs are denied access to the key decision-makers, they build and maintain informal channels and alliances to spread their message and advocate spending goals. Talking to peers or people lower in the organization can get things bubbled up in an executive's area of responsibility.

Informal conversations count: Successful CISOs don't miss opportunities to communicate the value of InfoSec. They indicate that even watercooler chats can make a difference. Small, casual efforts keep security top-of-mind and can lead to long-term budget support.

Avoid technical jargon: Successful CISOs craft their stories in language that fellow business leaders understand. They frame their technical solution in terms of how it will benefit the organization. If the listener does not understand the story because of jargon, then he or she is unlikely to retell or spread it within the organization.[18]

Verizon global PCI DSS maturity survey findings

- 42% of survey respondents indicated that the compliance team is responsible for tracking security metrics
- 12% indicated that the risk team is responsible for tracking metrics
- 19% indicated that their QSA is responsible for tracking security metrics
- 12% made internal audit responsible for tracking metrics
- 40% indicated that the IT security department is responsible for tracking metrics
- Less than a quarter of organizations (5%) indicated that someone else (other than mentioned above) is responsible for tracking metrics

Verizon 2018-2019 survey

Introduction to maturity models

More is spoken and written about data protection today than ever. We have more books, websites and conferences than ever before dedicated to this subject. Data protection budgets continue to increase year after year. The demand for information security professionals is higher than ever before, and the battle to recruit qualified professionals is a constant struggle. It's difficult to commit time and resources to compliance program management maturity when competing demands and dynamics are at play.

The complexity of data protection programs results in a large number of ways to fail. Organizations cannot enhance data protection—and they certainly cannot improve sustainability and effectiveness—when they are in a perpetual state of crisis. Reactionary approaches to data protection and compliance don't work; clear directions are needed to break the inertia that results from sailing into the wind.

Maturity models provide a benchmark for the evolution of business processes that can substantially improve data protection and compliance performance. Organizations should include maturity assessments (Factor 8 of the 9 Factors of Control Effectiveness and Sustainability) as an integral part of their compliance program. It facilitates the standardized and consistent evaluation of your data protection capabilities, processes and architecture. Maturity assessments also measure progress and support decision-making. This helps clarify where improvements can be made, which tasks and investments in technology and controls should be prioritized, and why.

Organizations do their best when they focus their process improvements on a manageable number of process areas at a time. Therefore, the first improvements should focus on those processes that have the greatest potential impact should things go wrong. At more mature levels, you look beyond process definitions and work on the consistency of application and adherence, training, monitoring and evaluation. All this work converges toward automation and best practices.

Benefits of maturity models

Maturity models are useful when comparing a current (and often chaotic) situation against several factors. They indicate how capable an organization is of achieving continuous improvement through the consistent application of business processes.

Maturity models allow an organization to have its data protection compliance processes and methods evaluated against a clear set of metrics and objectives that establish a benchmark. They can help you evaluate process performance and drive improvement over time. Maturity models are usually the first step in the process of prioritizing opportunities to improve data protection compliance across an organization.

Also in the context of payment card data protection, the mature operation of an environment will include established capabilities and sustainable processes that demonstrate repeatable, consistent and ongoing measurement of control effectiveness, highly predictable performance outcomes, and continuous improvement.

18 "The Battle of the Budget," Phil Gardner, IANS, April 4, 2018, https://www.iansresearch.com/how-we-differ/all-blogs/philosophies/the-battle-of-the-budget

Is it practical, effective and actionable?

Since the release of the PCI DSS, organizations expressed the need for practical, actionable guidance on how to measure the effectiveness and maturity of their DPCPs. PCI DSS provides a minimum baseline only. However, organizations need a holistic business process-management approach to improve their data protection capabilities and processes. This can be further enhanced by combining PCI DSS with complementary security frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), among others.[19]

You need to know how your program is performing compared to industry baselines. To do so, track KPIs, objectives and key results (OKRs), or other goal- or objective-driven metrics. OKRs are like signposts that show how close you are to meeting your objectives. These metrics, as useful as they are, often can be hard to apply to qualitative data. This is where maturity models can become an incredibly useful tool for continuous improvement—achieved by creating ongoing review processes that can be used on day-to-day business processes to evaluate their effectiveness and identify areas for improvement.

A note of caution: Measuring anything makes it easier to drive improvements, but measuring the wrong things can lead to costly investments that don't support program objectives. It is important to ensure that you establish metrics that are in line with your desired outcomes.

The five primary use cases for applying a maturity model are:

1. **Clarifying approach**—As a roadmap for building capability for orderly strengthening of data protection
2. **Measuring maturity**—As a framework for assessing capabilities against industry practices and standards
3. **Guiding actions**—As a communication vehicle to communicate what is meant by effective
4. **Diagnostics**—As a diagnostic tool using levels of maturity to track gap improvement
5. **Aligning stakeholders**—As a way to assign responsibilities and set goals and targets

Maturity model architecture

Maturity models are not intended to be prescriptive in terms of how a process should be carried out but rather define characteristics of effective and sustainable processes. Architecturally, maturity models typically have "levels" along an evolutionary scale that define measurable transitions from one level to another.

An organization can use this scale to define its current state, determine its future, more-mature state, and develop the capabilities and qualities it must attain to reach that future state.

Capability maturity model definitions

To understand maturity models, you should understand key definitions:[20]

Process capability: The range of expected results that can be achieved by following a process; a predictor of future project outcomes. Capability in this context is the ability of an organization to collectively deliver organization objectives, not confined to individuals, and encompasses people-related knowledge, skills and behavior. A capable process consistently produces predictable results and outputs that are within specification. As each process develops, its capability should improve.

Process performance: A measure of the actual results achieved by following a process (on a particular project or environment). Process performance focuses on the results achieved, while process capability focuses on results expected. Based on the attributes of a specific project and the context within which it is conducted, the actual performance of the program may not reflect the full process capability of the organization.

Process maturity: The extent to which a specific process is explicitly well-defined, controlled, repeatable, measured, analyzed, improved and effective. Maturity implies a potential for growth in capability. Process maturity provides an indication of how close a developing process is to being complete (managed, documented and performed) and capable of continual improvement through qualitative measures and feedback. For a process to be mature, it has to be complete in its usefulness, automated, reliable in information, and continuously improving.

Process capability maturity levels classify an organization according to the performances of specific processes; the organization is deemed capable if it satisfies specified process performance and quality objectives. Process maturity levels classify an organization's ability to control various steps or processes. The activities are conducted according to a documented method; everyone knows what is expected of them and performs accordingly.

19 "NIST Mapping," PCI Security Standards Council, July 17, 2019, https://blog.pcisecuritystandards.org/nist-mapping

20 For additional information, see https://cmmiinstitute.com

Types of maturity models

More than 75 published maturity models exist, each defining different levels and focused on various disciplines, such as software engineering, project management, IT development, quality, change management, cybersecurity, risk management and so on.

Generally, most models use a five-level scale, such as:

Level 0 = Non-existent: Nothing in place. No recognition of need. Not part of mission.

Level 1 = Starting: Limited capability. Starting to put in place.

Level 2 = Partly: Partly in place (say 30%–<60%). Capability exercised to some extent.

Level 3 = Largely: Largely in place (say 60%–<90%). Capability effectively practiced.

Level 4 = Fully: Fully in place (say >90%). People fully aware and trained, responsibilities integrated.

For example, in the Capability Maturity Model Integration (CMMI) model that is developed and maintained by the Software Engineering Institute (SEI) at Carnegie Mellon University, there are five maturity levels numbered 1 through 5. Other models may have six levels numbered 0 through 5.

A useful five-point scale that we published in the 2018 Verizon PSR[21] (figure 20 on page 41) is "HB 158:2018, Delivering assurance based on ISO 31000:2009 risk management—Principles and guidelines." In the context of risk management and compliance, compliance is:

1. **None:** Very little or no compliance with the requirement in any way
2. **Very little:** Only limited compliance with the requirement
3. **Some:** Limited compliance with requirement. Certainly agree with the intent, but limited compliance in practice
4. **Good:** Management completely subscribed to the intent, but there is partially complete compliance in practice
5. **Complete:** Absolute compliance with the requirement—in intent and in practice—at all times and in all places

For further details, see Appendix G in this report for a book list on maturity models.

Maturity model categories

In general, maturity models can be categorized as one of the three following types:

- Progression models
- Capability maturity models (CMMs)
- Hybrid models (combination of progression and capability maturity models)

Progression models

Progression maturity models represent a simple progression or scaling of a characteristic. The purpose of a progression model is to provide a navigational aid for improvement. For example, a maturity progression for arithmetic methods might be: pencil and paper > slide ruler > calculator > spreadsheet. In this example, Level 1 might be expressed as "primitive" and Level 3 "tool enabled." Progression models do not measure capability or process maturity.

While the NIST CSF isn't a maturity model, it does use a progression of tiers that in many ways is similar to a progression maturity model. According to NIST, "These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed."[22]

Capability maturity models

A simple capability maturity model (CMM) focuses on an organizational capability. These models offer ways to measure or track the maturity of the culture and how embedded a capability is in the organization. Capability levels can help you understand dependencies among the practices of a process, and can help you identify which improvements to perform first.

COBIT is a well-known capability maturity model for IT governance that is derived from the CMMI model.

21 Verizon 2018 Payment Security Report, https://enterprise.verizon.com/resources/reports/payment-security/2018/

22 "Cybersecurity framework," National Institute of Standards and Technology - US Department of Commerce, https://www.nist.gov/cyberframework/

Levels	Characteristics
Level 1 **Initial** (Chaotic)	Ad hoc performance. Undefined and undocumented processes. Capabilities are not repeatable or sustainable. Outputs and success depend on skills and efforts of specific individuals and heroics.
Level 2 **Repeatable**	Some repeatable processes with some consistent results, but process discipline is unlikely to be rigorous, especially under stress. Partial conformance with standards.
Level 3 **Defined/ Integrated**	Managed practices are uniformly applied. Defined and documented, generally standardized processes are established, with consistent process performance subject to some degree of improvement over time. Policies and procedures are defined, documented and integrated into each other and the organization's infrastructure.
Level 4 **Managed**	Processes and outputs are quantitatively understood and controlled. The use of process metrics and other ways to manage, adjust and adapt processes to ensure effective control without measurable losses of quality or deviations from specifications.
Level 5 **Optimizing**	Continuous improvement, learning inside and outside the organization. Individual, unit and organization performance measures are fully integrated to drive performance improvements. Integrated across the organization with improved governance and risk management. Risks are measured and managed quantitatively.

Figure 7. Capability Maturity Model Levels

Hybrid models

Overlaying characteristics of the progressive model with attributes from CMMs can create a hybrid maturity model. This type of model reflects transitions between levels that are similar to a capability model (i.e., that describe capability maturity) but architecturally use the characteristics, indicators, attributes or patterns of a progression model.

One example of a hybrid model is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).[23]

Measuring the level of maturity of your data protection and compliance program (DPCP) via self-assessment using an appropriate maturity model can provide a starting point for continuous evaluation of program performance. You should formalize this monitoring using measurements and metrics (see page 21 for the section on metrics).

Immaturity model levels

Alternative models for maturity are also available, although some are more professional than others. The levels of this capability immaturity model are useful for a laugh—and hopefully not for describing your organization.

- **0: Negligent indifference**—All problems are perceived to be technical problems
- **-1: Obstructive**—Counterproductive processes are imposed. Status quo über alles
- **-2: Contemptuous arrogance**—Complete lack of a training program
- **-3: Undermining sabotage**—Rewarding failure and poor performance[24]

Maturity model implementation

There is a famous adage that says, "Essentially all models are wrong, but some are useful."[25] This is true for risk maturity models as well. It's important to understand that maturity models are constructs of experience, opinion and imagination, and seldom the results of applied scientific methods. When implementing a maturity model, you should not assume that organizational process and capability growth is a linear progression through a number of discrete phases, marked by unique characteristics. Progressing from a lower phase of development or sophistication (maturity) to a higher phase rarely goes perfectly or evenly across all fronts. For some organizations, the investment cost, resource constraints, time and management distractions mean that progression on all capabilities is not a realistic target.

Each maturity level develops a capability that must be met to progress to the next maturity level. An organization may take several years to move from one maturity level to the next or prioritize one capability over another. You must also be careful when defining a final state of maturity. In the real world, any ideal state tends to vary according to circumstances. A final state can undermine a drive toward continuous improvement. What happens when you reach the final level of a maturity model? Is it ever safe to stop improving? Therefore, the final stage is usually one of continuous refinement and improvement, and data protection compliance teams should remain focused on meaningful outcomes, not on celebrating the achievement of maturity levels.

verizon business ready

23 "SEI Partners with DoE and Industry to Improve Power Grid Cybersecurity," Software Engineering Institute, Carnegie Mellon University, 2012, http://www.sei.cmu.edu/newsitems/ SEI-Partners-with-DOE-and-Industry-to-Improve-Power-Grid-Cybersecurity.cfm

24 https://en.wikipedia.org/wiki/Capability_Immaturity_Model

25 "Science and statistics," Journal of the American Statistical Association, 71: 791–799, Box, G. E. P., Taylor & Francis, Ltd. on behalf of the American Statistical Association, 1976

A maturity model improves data protection compliance management capabilities in a disciplined and consistent way but cannot guarantee that all organization initiatives will be successful. All models have natural limitations.

All DPCPs need to mitigate payment card data risks within time and money constraints. In some cases, it might make sense to mature competencies to 90% of the potential capability because the additional 10% improvement might be cost prohibitive. Developing this data protection navigational map, and being purposeful about investment and return on investment, will help gain traction for future budgeting.

Some tools to help you assess your level of maturity and move your program forward

The 7 levels of change:
A strategy for creativity, innovation and continuous improvement

Level 1: Effectiveness	Doing the right things
Level 2: Efficiency	Doing things right
Level 3: Improving	Doing things better
Level 4: Cutting	Stopping doing things
Level 5: Copying	Doing things other people are doing
Level 6: Different	Doing things no one else is doing
Level 7: Impossible	Doing things that can't be done

Einstein pointed out that: "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—we must do things differently.

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

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 it requires to implement.

Effectiveness: Learn the basics of data protection and compliance—what are the right things to do and how to immediately change enough to become effective. The Pareto Principle 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%.

Efficiency: This change requires a thorough understanding of all the aspects of data protection in order to identify and then focus on doing very well those things 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 involve coaching or explanations by others familiar with the job or business activity.

Improving: This involves thinking about ways to improve or fine-tune—speed things up, shorten delivery time, increase functionality, reduce downtime. It makes something more effective, efficient, productive and value-adding.

Cutting: This involves analysis of core functions and applies the Pareto Principle to focus on stopping doing things—cutting out the 80% of activities that only yield 20% of the value. It focuses on eliminating waste. Done systemically while keeping all organizational interrelationships and subsystems in perspective, major organization-wide results can be achieved.

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 do things and enhancing upon their processes is the hallmark of a successful innovator.

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 move the organization into areas where nobody else is doing it.

Impossible: Market constraints, resource limitations or organization 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.[26]

26 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

The state of PCI DSS compliance, 2019: And 12 key requirements

By Anne Turner, Senior Consultant,
Verizon PCI Security Practice

An interim assessment—or initial Report on Compliance (iRoC)—provides a valuable opportunity for organizations to validate the effectiveness of PCI DSS control management. Full compliance with PCI DSS, measured during interim compliance validation, is no longer increasing. It continued its upward trend for at least five years until 2017, when it declined by 2.9 percentage points (pp).

Organizations are required to not only achieve 100 percent full 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 assessment to determine the percentage of assessed entities that achieved full compliance for each PCI DSS Key Requirement in 2018.

Global compliance fell 15.8 pp in 2018, to 36.7%. That's the lowest since 2013, and followed a trend of decreasing sustainability seen across the previous three years. While overall compliance fell, the control gap, which represents how far organizations are from full compliance, remained consistent with the previous year at 7.2%.

Requirements 5 and 7 remained the most consistently maintained, as we saw across the 2017–2019 PSR reporting years.

The largest compliance drop occurred against Requirement 6, as organizations struggled to maintain effective vulnerability management, software development and change processes. It is then perhaps not too surprising that Requirement 11 remained the poorest performer—both in overall compliance and control gap—as organizations struggle to sustain compliance with security testing requirements year after year.

Regionally, Asia-Pacific (APAC) outperformed the Americas as well as Europe, the Middle East and Africa (EMEA). From an industry perspective, finance and IT services both performed better than retail and hospitality, with hospitality lagging somewhat behind other sectors.

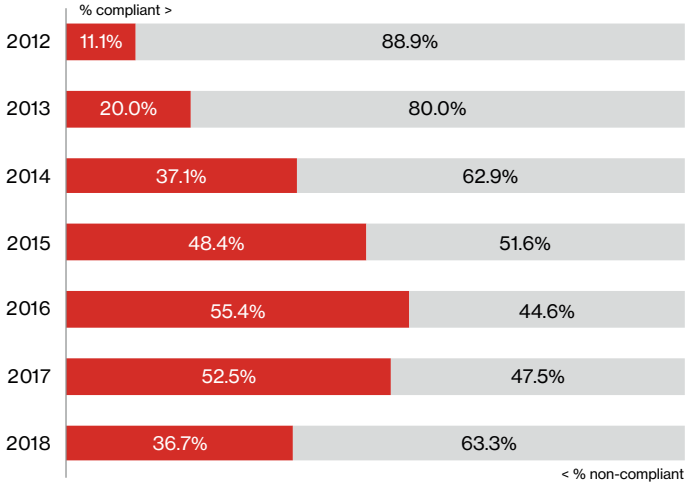


Figure 8. PCI DSS full-compliance history (organizations meeting all requirements during interim validation)

The PCI Data Security Standard (PCI DSS) consists of 12 PCI DSS Key Requirements, 78 base requirements and over 400 test procedures. We measure the performance of the four key industries on three key metrics:

a. Full compliance
b. The control gap
c. Use of compensating controls

Full compliance

The share of companies achieving 100% PCI DSS compliance at interim validation. All companies 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 provides a measure of how far the assessed entities were from full compliance. This is shown right-to-left for clarity.

Compensating controls

This percentage indicates how many companies used one or more compensating controls for the specified section of the DSS (not how many compensating controls were used).

The compliance story

This year's PSR includes some exciting additions. For the first time, it contains assessment data compiled from additional QSA companies. This expands on the view and perspective provided in previous PSRs.

The 2019 PSR includes data from 302 engagements around the world, where the findings of multiple onsite compliance validation assessments for unique legal entities were each recorded in a complete and integrated PCI DSS Report on Compliance document. We expect the data to improve even further, as more QSA companies come together to provide a holistic view of compliance to the PCI DSS. This is important, as the entire payment card industry moves to the new standard, PCI DSS v4.0, in 2021.

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

Organizations in APAC show stronger ability to maintain full compliance: 69.6% maintained conformance to the security standard. On the other hand, 20.4% of organizations in the Americas maintained full compliance.

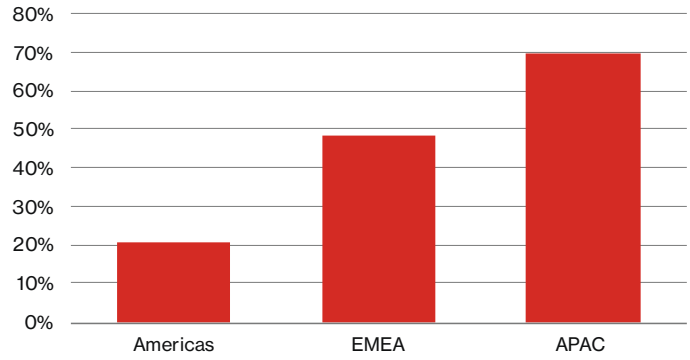


Figure 9. Full compliance by region

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

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

Since the majority of organizations in the Americas are unable to maintain compliance, it is important to understand how well—or how poorly—they protect sensitive payment card data. Of course, companies that are fully compliant have a control gap of zero. For the others, the control gap decreased to 10.2%, which is 6.2% points better than what was documented in the 2018 PSR. That translates to just under 90% compliant for most organizations. If 90% is an "A," then the average control gap would result in a "B."

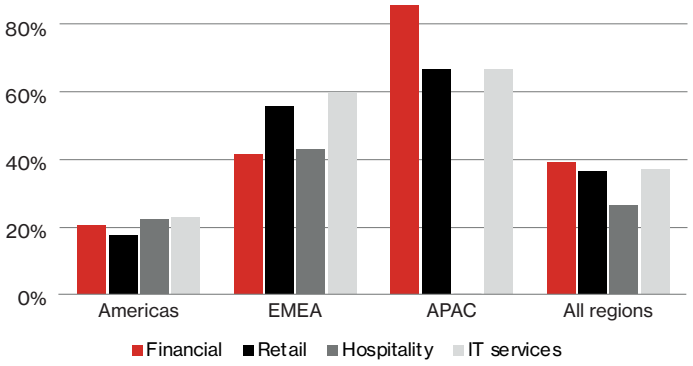


Figure 10. Global PCI DSS compliance by industry

Interesting notes about the control gap

Seven of 12 requirements have controls in the bottom 20. Requirement 11 has consistently ranked last, and 5.4% (seven of the 38) of Requirement 11 controls are in the bottom 20.

Two controls in the bottom 20 relate to organizations that are not compliant with having reviewed a charter for PCI DSS compliance and assigning executive managers for accountability.

These controls are first steps to establishing a compliance program to protect data. With these controls in the bottom, there is more than a 95% probability that your organization has not committed to a sustainable data protection compliance program.

While a smaller control gap means that you are moving in the right direction, the controls with the largest gap to full compliance are 16 pp to 33 pp away from the lowest possible compliance—and security risk.

Data breach correlation

In the 2018 PSR, we introduced data breach correlation statistics alongside the compliance analysis for the first time. In this year's report, more detailed insights are included, based on data breach metrics from PCI forensic investigations (PFIs) performed by the Verizon Threat Research Advisory Center (VTRAC) | Investigative Response Team from 2016–2018.

It is important to note it is not always possible to identify with any certainty the cause of the data breach nor contributing factors. In 28.7% of cases, identifying a specific requirement as causing a breach was not possible. In 27.4% of cases, the extent to which a requirement could be identified as contributing to a breach is unknown. This is largely due to poor log management practices, weak incident response (IR) procedures and limited capabilities within organizations to preserve evidence in the wake of an incident. All of this leaves investigators with a dearth of forensic information.

Data breach correlation summary

- No organization that suffered a data breach was compliant across all 12 requirements over the three-year data set
- No organizations—at the time they were breached—were compliant with the following requirements: Requirements 3, 8, 10–12
- Requirement 9 had the highest compliance rates of all PCI DSS requirements among breached entities, but failures were still observed in 75.0% of organizations
- 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, with a 7.0% gap. IT services had a near-zero control gap of approximately 1.0%

Introducing our VTRAC | Investigative Response Team views from the front lines

The State of compliance section of the 2019 PSR includes more detailed breach correlation data than ever before. Additionally, we've included real-world, firsthand observations from our field investigators who conduct PCI data breach investigations.

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 breached 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.

However, in revisiting payment card security breaches investigated by the VTRAC | Investigative Response Team, we can definitively state that we have never, ever reviewed an environment, or investigated a PCI data breach involving an impacted entity, that was truly PCI DSS compliant. This is true even if they had a signed Attestation of Compliance (AOC).

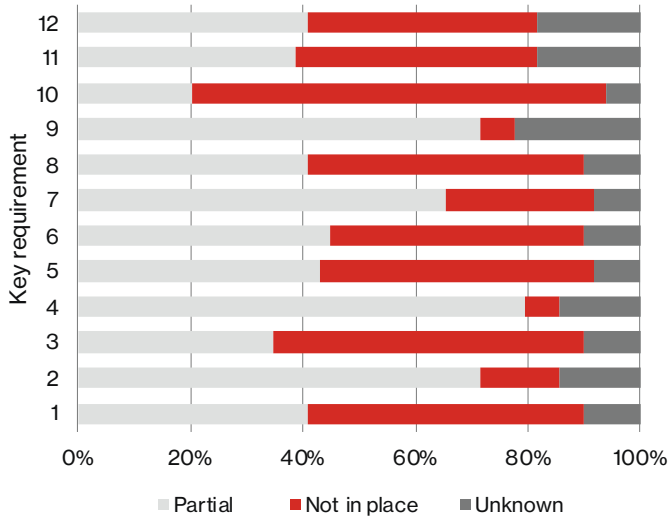


Figure 11. PCI DSS control status of breached organizations

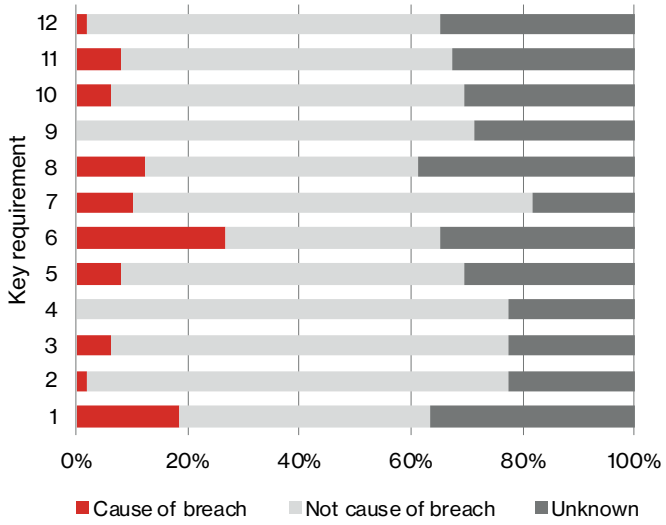


Figure 12. Requirements identified as cause of data breach in PFIs

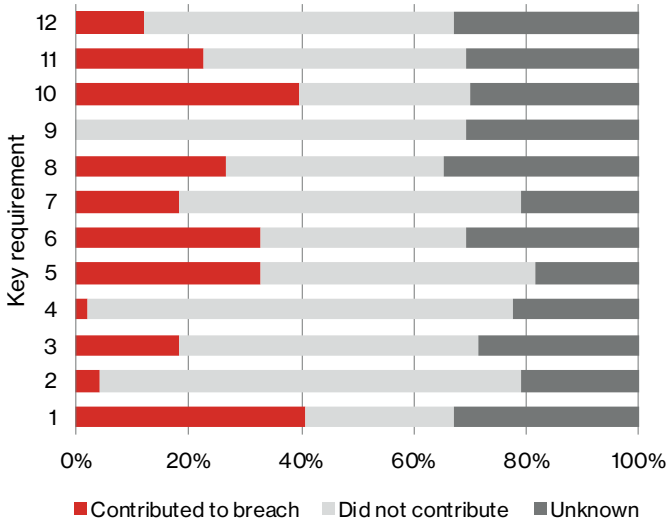


Figure 13. Requirements identified as contributing to data breach in PFIs

PCI DSS and incident response

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

- **Reqs. 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
- **Reqs. 11.1.2, 12.5.3** – Establishing IR procedures for security monitoring and responding to alerts, including rogue wireless monitoring, security event logs, intrusion detection and change detection solutions
- **Reqs. 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
- **Req. 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: Maintain a firewall configuration

This Requirement covers the correct use of a firewall to filter traffic as it passes between internal and external networks, as well as traffic to and from sensitive areas within the organization's internal networks.

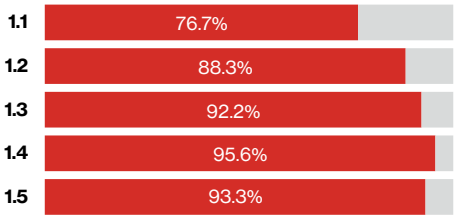


Figure 14. Requirement 1 – full compliance

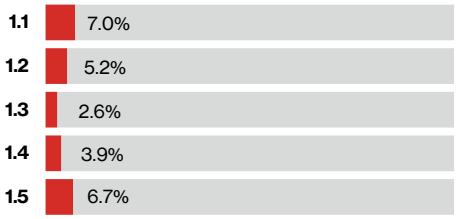


Figure 15. Requirement 1 – control gap

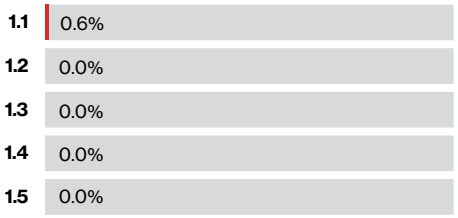


Figure 16. Requirement 1 – compensating control use

While we've seen improvement over the past two years, this year's review shows full compliance dropped to sixth for all requirements. A major decrease occurred in the use of compensating controls for all industries. While fewer companies demonstrated security measures were "in place," the gaps were slightly smaller.

The hospitality industry struggled the most with Requirement 1, having the lowest compliance score and the largest control gap.

A significant percentage of companies were unable to show compliance in a post-breach situation.

Europe on top

Ranking for this requirement went from fifth in the previous year to sixth. The number of organizations able to demonstrate full compliance was 72.8%, an 8.4 pp decline from the previous year. This comes after two years of improvement for Requirement 1.

Financial institutions fared better than other industries. This was an improvement of 2.2 pp from the previous year.

Hospitality, for the second year in a row, was the least compliant, at 57.9%. This is 14.9 pp below the average for all industries, and the second year of decrease in that industry.

All regional averages were within 1.1% of the global score.

Service providers have a strong lead with security practices in this area over merchants. Merchant averages were 21.6 pp below the average for all assessments.

Control gap flat

The control gap for those unable to demonstrate compliance was the same as reported in 2018, at 5.2%. Gaps for Controls 1.1 and 1.5 increased, while Controls 1.3 and 1.4 had smaller gaps.

Retail had the smallest control gap, at 3.9%, and hospitality had the highest one at 7.9%.

The Americas was the only region to reduce the control gap, at 3.5%. Europe and APAC control gaps were 4.8% or higher.

Service providers were closer to full compliance with Requirement 1, with a score of 4.1%.

Global drop in compensating controls

Only one industry, the financial industry, was using a compensating control for Requirement 1. A 6.0% drop occurred in the use of compensating controls in the past year.

State of control compliance

Control 1.1 had the lowest full compliance score, the highest control gap, and was the only one to use a compensating control. The drop in Control 1.1 was 7.6% points.

Hospitality lags behind

After struggling for a few years, financial organizations improved their position relative to other industries. They had the highest rate of full compliance over other industries for Requirement 1. They were also the only industry requiring the use of compensating controls. Hospitality, with the highest control gap, was the most challenged in maintaining compliance with this requirement. Retail and IT services were 1 pp apart from each other.

All industries, with the exception of hospitality, demonstrated this requirement was possible to achieve with no compensating controls.

Data breach correlation

PCI Forensic Investigations (PFIs) revealed that 18.4% of breaches were due to a failure of Requirement 1 security controls. Even when it wasn't the cause of a breach, 49.0% of organizations were noncompliant with this requirement.

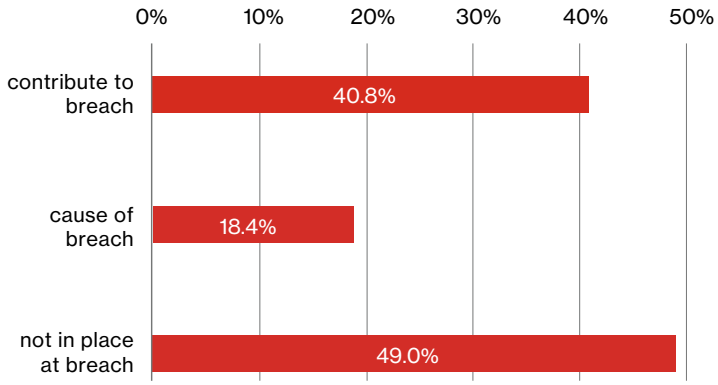


Figure 17. Requirement 1—breach correlation

Build and maintain secure networks and systems

When identified as a deficiency—and we do identify it as such—it's normally considered a contributing factor, as documented in the PFI final reports that we submit to the breached entity and affected payment card brands. This is because in many payment card environments, firewalls are the front line of defense. Using vendor-supplied and default passwords is like leaving the keys in the ignition and the car running at the gas station—with hundred-dollar bills spread across the dashboard. It's like yelling to attackers, "Rob me! Rob me!" Unfortunately, as we found in our investigations, a good number of victim organizations did yell, "Rob me!"

We reserve the right to mention the virtues of multi-factor authentication and credential best practices at another time, but we cannot complete this section without writing about default passwords.

The VTRAC | Investigative Response Team has examined entities that not only failed to remove default passwords, but also those that changed default passwords to easily guessable combinations. To divulge a few easily guessable passwords would allow the reader to know the impacted entities. How? Well, the company name was a component of the password.

Default passwords were sometimes a contributing factor and related to legacy applications and devices.

Requirement 1 controls

1.1	Implement firewall and router configurations
1.2	Restrict connections between CDE and untrusted networks
1.3	Prohibit direct public access between Internet and CDE
1.4	Install personal firewall software
1.5	Documented policies and procedures for managing firewalls

2: Change vendor-supplied defaults

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

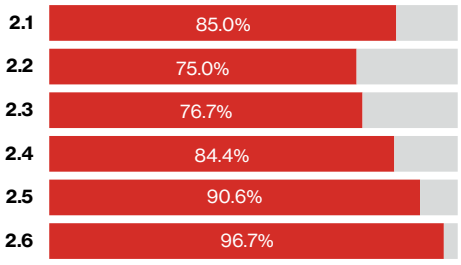


Figure 18. Requirement 2 – full compliance

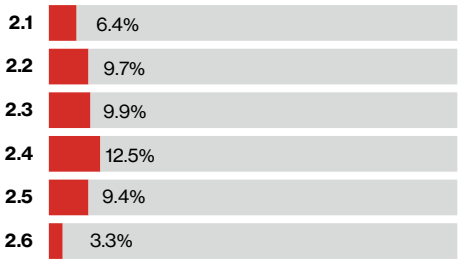


Figure 19. Requirement 2 – control gap

Figure 20. Requirement 2 – compensating control use

The ranking for this requirement went to seventh from eighth and remains in the bottom half of all requirements. Despite the improved rankings, full compliance decreased by 7.9 pp to 68.3%.

For those unable to achieve full compliance, the control gap improved slightly at 9.0%. All organizations are using fewer compensating controls.

The finance industry had the highest full compliance and use of compensating control; hospitality was the lowest.

Rank up, compliance down

Performance for Requirement 2 dropped 7.9 pp from the 2018 PSR. Despite the downward change, the ranking moved up to seventh of all requirements. A little more than two-thirds of organizations had full compliance with this requirement.

Hospitality was the lowest organization to achieve full compliance, which is more than 25 pp (26.2%) below other industries. Additionally, less than half (42.1%) demonstrated compliance.

The Americas was the only region below the global average for full compliance. Only 65.6% of organizations in the Americas had full compliance.

Service providers and merchants were within 3.1 pp of the global average, with merchants being the most challenged for this requirement.

Largest gap for merchants

The control gap improved by less than half of a percentage point and remained at number 10 in the rankings – at 9.0%.

Retail showed a wider control gap from the previous year, at 12.4%. For retail, this was the largest gap for all the requirements.

APAC had, again, the highest gap of all the regions. The Americas was the only region to improve from the previous year, with the financial and retail industries showing a smaller control gap. Financial did best, with a control gap of 7.3%. Hospitality, on the other hand, was at 13.5%.

Europe doubles since 2018

Requirement 2 moved to fourth position, with 1.8% fewer companies using compensating controls, and the score dropping from 7.4% to 5.6%.

The EMEA region used more compensating controls than other regions. 7.8% of organizations compensated to meet requirements; more than double from the previous year.

Service providers and merchants were 1.3 pp apart from each other. Merchants showed the most improvement, but still used more compensating controls than service providers.

Retail and IT services had the lowest scores, at 2.3% and 2.9%. Hospitality used 3.5 times more compensating controls than other industries, at 10.5% – the highest use of compensating controls.

Two controls make top 20

Test procedure 2.2.4.c (inspect sample) and Control 2.4 (maintain inventory) were two of the top 20's most improved since the 2018 PSR.

Finance takes the lead

Hospitality had the fewest number of organizations achieving full compliance (26.3%) in relation to other industries. Comparatively, it had the largest control gap (12.6%), while using the fewest compensating controls (10.5%).

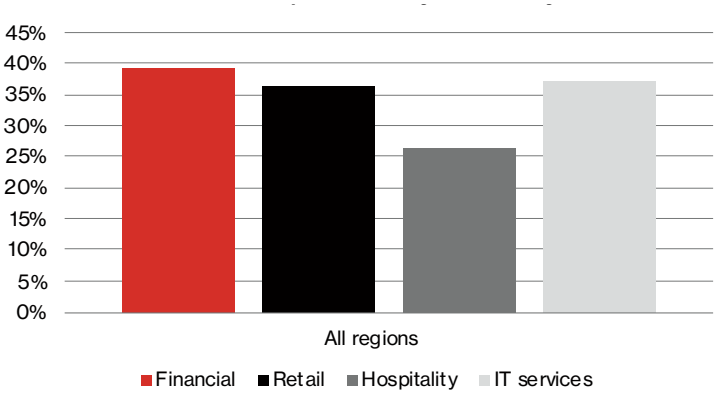


Figure 21. Full compliance by industry

Finance had the greatest number of organizations achieving full compliance (39.0%) and the largest percentage using compensating controls (30.5%).

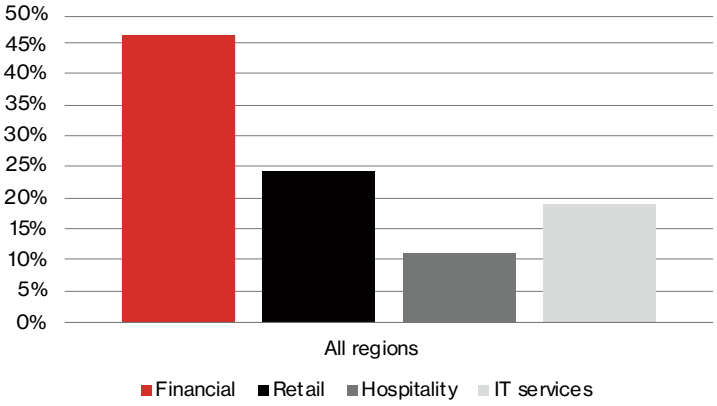


Figure 22. Assessment share by industry

Data breach correlation

A large difference exists between compliance and the cause of a breach. Compliance was at 68.3%, while 14.3% of breached entities struggled with control failures. In most cases, Requirement 2 was not identified as either causing or contributing to breaches.

Only 2.0% of breaches resulted from Requirement 2 control failures, and just 4.1% of Requirement 2 failures were a contributing factor.

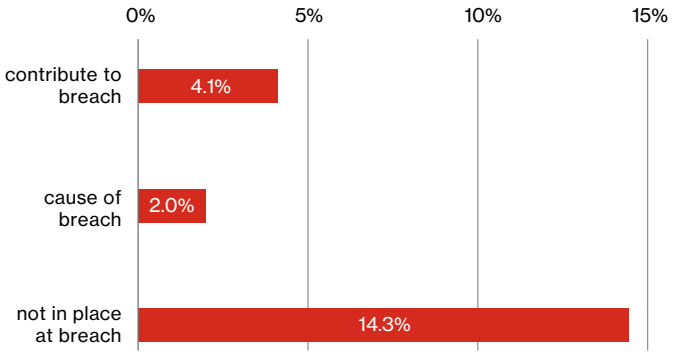


Figure 23. Requirement 2 – breach correlation

Requirement 2 controls

2.1	Change vendor-supplied defaults, unnecessary accounts disabled
2.2	Develop configuration standards
2.3	Encrypt non-console administrative access
2.4	Maintain an inventory of in-scope system components
2.5	Documented policy and procedures for managing vendor defaults
2.6	Shared hosting providers data protection responsibility

3: Protect stored cardholder data

This Requirement covers the protection of stored cardholder data and sensitive authentication data. It states that all stored data must be protected using appropriate methods, and must be securely deleted once no longer needed.

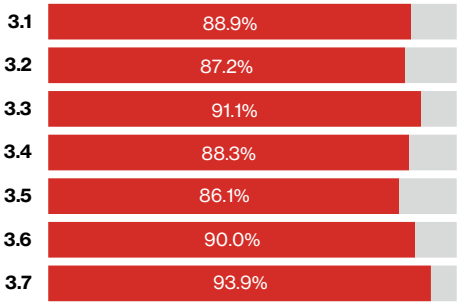


Figure 24. Requirement 3 – full compliance

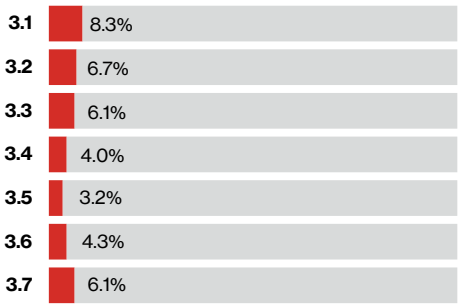


Figure 25. Requirement 3 – control gap

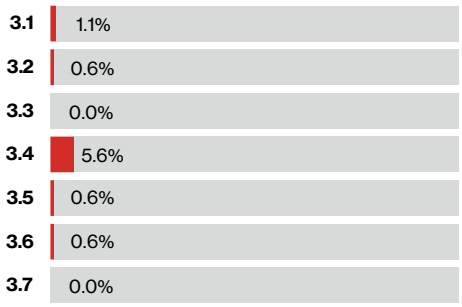


Figure 26. Requirement 3 – compensating control use

We previously saw a small improvement in full compliance for this requirement, but that trend was not sustained. Still, Requirement 3 improved in ranking for both full compliance and control gap, suggesting that organizations are finding other areas of the standard more challenging to maintain.

Hospitality lagged behind other industries with this requirement, but also had some unique challenges to overcome, including a lack of mature solutions designed for hospitality environments.

Drop after three year's growth

The ranking for this requirement has improved over the 2017–2019 PSR reporting years from 11th in the 2017 PSR to fourth in the 2019 PSR. Unfortunately, the improvements seen in full compliance in the 2018 PSR were not sustained, and full compliance fell by 1.2 pp to 76.7%.

The Americas achieved an 11.9 pp improvement in full compliance compared to the previous year, while EMEA dropped 10.7 pp and APAC dropped 10.7 pp.

Service providers reported 78.4% full compliance and only a 0.9 pp decrease compared to 2017. Merchants suffered a more significant drop in full compliance, falling 12.9 pp to 71.7%.

IT services outperformed other sectors, but finance was the only sector to improve compared to the previous year.

From the bottom to the top

This requirement was ranked 11th in 2017, but jumped to second this year, as the control gap reduced 5.7 pp to 4.7% compared to the previous year. This is a significant improvement.

The Americas saw the most significant improvement, reducing the control gap by 14.7 pp compared to the previous year.

APAC saw an 8.3 pp increase in the control gap, to 12.2%, the widest globally for this requirement.

Finance had the largest improvement in control gap, from 14.1% in 2017 to 5.9%. Retail also improved by 5.9 pp to 2.0%, as compared to the previous year.

Reduction in all regions

Compensating controls were used across this requirement, with the exception of Controls 3.3 and 3.7. Control 3.4 was the most frequently compensated, at 5.6%.

The use of all compensating controls reduced from the previous year. Most significantly, Control 3.4 reduced by 5.9 pp, and both Controls 3.5 and 3.6 by 3.5 pp.

Finance organizations were the most frequent users of compensating controls at 11.0%, while the hospitality sector did not implement any compensating controls in 2018.

State of control compliance

Control 3.6 improved the most over the previous year, while Control 3.5 had the largest control gap increase. There were no controls that featured in the bottom 20, but 3.7 did make it into the top 20, ranking ninth overall.

IT services in top spot

IT services performed significantly higher than other sectors, with full compliance of 94.3% – just a 0.2 pp drop from the previous year. Retail outperformed finance by 6.3 pp, despite dropping 8.0 pp since 2017.

Hospitality lagged somewhat behind the other sectors, at 52.6%. It also reported the greatest increase in control gap, at 8.0 pp to 11.1%, suggesting that these organizations are struggling to implement effective compliance solutions that satisfy their organizational requirements.

Data breach correlation

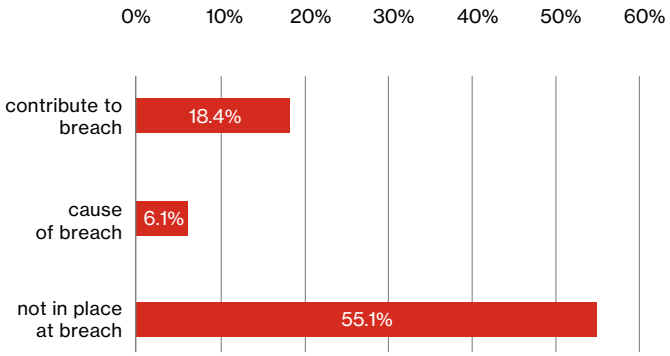


Figure 27. Requirement 3 – breach correlation

None of the breached entities analyzed within the PFI cases were compliant with Requirement 3 at the time of breach.

Requirement 3 was not in place at 55.1% of breached entities, the second-highest level of noncompliance for any requirement of breached entities.

However, Requirement 3 controls contributed to only 18.0% of breach cases. Requirement 3 controls are unlikely to directly cause a breach, but are implicated in any PFI case, as theft of cardholder data is generally the result of failures in how the data was stored or managed.

Requirement 3 controls

3.1	Keep data storage to a minimum
3.2	Do not store sensitive authentication data after authorization
3.3	Mask primary account numbers (PANs) when displayed
3.4	Render PAN unreadable anywhere it is stored
3.5	Protect keys used to secure stored CHD against disclosure
3.6	Key-management processes
3.7	Documented policies for protecting stored CHD

Protect cardholder data

When the VTRAC | Investigative Response Team investigates PCI data breaches, it often observes a lack of understanding by management regarding cardholder data (CHD) storage and the protection associated with sensitive authentication data (SAD), which can lead to this requirement causing or contributing to a breach. It is disheartening to see the CHD or SAD showing up in log files, temporary files, database tables and even backup files (boo.). A comprehensive understanding of the CHD flow and environment can help organizations avoid failure on this requirement.

4: Encrypt data in transit

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

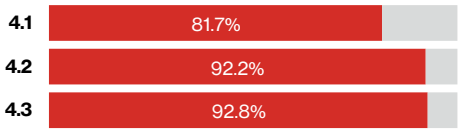


Figure 28. Requirement 4 – full compliance

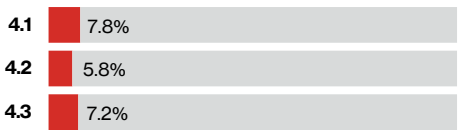


Figure 29. Requirement 4 – control gap

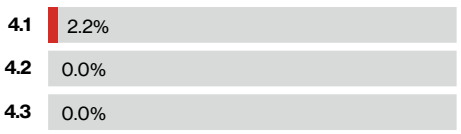


Figure 30. Requirement 4 – compensating control use

This requirement's ranking has remained consistent across the 2017–2019 PSR reporting years, despite a 9.1 pp decrease in full compliance in 2018.

While no organizations implemented compensating controls for this requirement in the previous year, both merchants and service providers implemented them in 2018.

Hospitality continued to lag behind the other industry sectors in full compliance, but was the only sector to reduce the control gap, so progress is clearly being made.

Holding rank in third

Full compliance fell for this requirement, from 86.9% in 2017 to 77.8%. Despite this, it retained the third-place ranking that it has sustained for the 2017–2019 PSR reporting years.

Retail and IT services outperformed the other sectors. IT services and financial both reported large drops in full compliance, with IT services dropping 12.9 pp and financial services 17.1 pp.

Hospitality, while lagging behind the other sectors at 63.2% full compliance, was the only sector to report an overall improvement compared to the previous year.

All global regions achieved full compliance within 2 pp of each other. EMEA was at 76.6%, just behind the Americas (78.5%) and APAC regions (78.3%).

APAC widens most, performs worst

The control gap increased from 1.4 pp to 7.5% over the previous year, slipping in rank from seventh to eighth.

APAC noted the highest control gap, at 12.4%, as well as reported the greatest increase compared to the previous year.

The Americas region narrowed the control gap by 4.6 pp to 4.5%, compared to 2017 figures.

Retail successfully lowered the control gap, while for all other industries it widened.

Merchants saw a negligible increase of 0.1 pp and reported a control gap of 6.2%, compared to 7.9% for service providers.

Compensating controls

In 2017, there were no compensating controls reported for this requirement, but 2018 saw 2.2% of both merchants and service providers introduce compensating controls to meet Control 4.1 (in all locations where cardholder data is transmitted).

Finance reported the highest use of compensating controls for this requirement, followed by retail. Neither hospitality nor IT services used compensating controls.

APAC had the highest use of compensating controls, but all regions were represented in the 2018 figures.

Drops across the board

Full compliance fell for each control, along with small increases in the control gap. Control 4.1 featured in the bottom 20 for 2018.

Retail only sector to improve gap

Hospitality was the only sector with a small improvement in full compliance of 1.6 pp. All other sectors saw a drop, with IT services suffering the most, with a decline of 17.1 pp from the previous year.

However, only retail reduced the control gap compared to 2017, with all other sectors widening it. IT services had the largest increase, with 8.4 pp.

Service providers reported the highest levels of full compliance, but merchants had a smaller control gap.

Data breach correlation

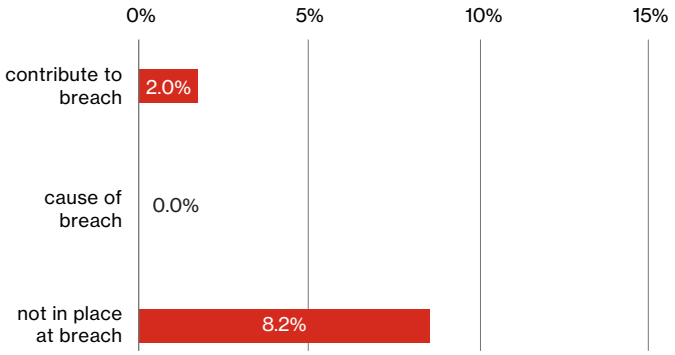


Figure 31. Requirement 4 – breach correlation

Requirement 4 was one of only two requirements not identified as a cause of breach in the PFI cases reviewed, and it was cited as contributing to a breach only in 2.0% of cases.

Trends

Within the retail industry, mostly online retailers experience compromises. In the hospitality industry, traveler accommodation, travel arrangement and reservation service organizations are breached most often.

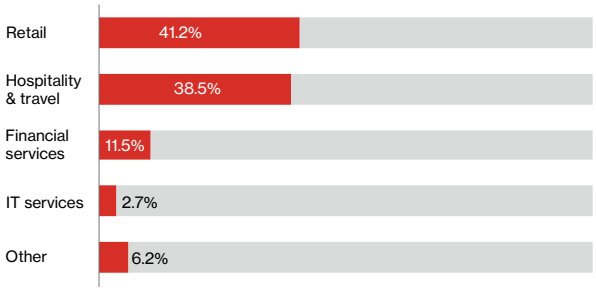


Figure 32. Confirmed global payment card data breaches by industry. Source: 6 Year Trend – Verizon PFI global caseload 2010–2016

Requirement 4 controls

4.1	Use strong cryptography and protocols
4.2	Never send unprotected PANs by end-user messaging
4.3	Procedures for encrypting transmissions of CDE

5: Protect against malicious software

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

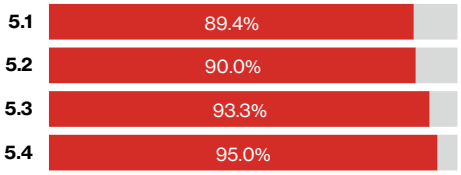


Figure 33. Requirement 5 – full compliance

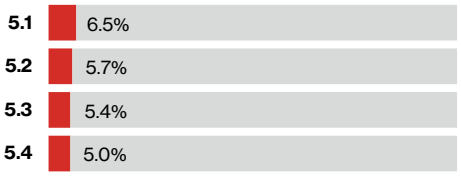


Figure 34. Requirement 5 – control gap

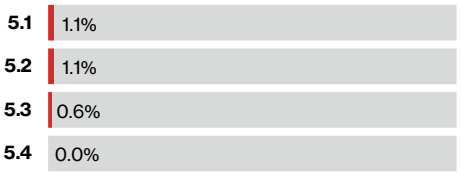


Figure 35. Requirement 5 – compensating control use

Requirement 5 is often considered one of the more straightforward PCI requirements to meet and is one of the most consistently maintained requirements over time. Requirement 5, along with Requirement 7, ranked top for full compliance for the first time in three years.

However, breached organizations are often found to be lacking when it comes to this requirement, with close to 50% of breached entities noncompliant at the time of breach.

Top spot despite compliance drop

The ranking for this requirement went from second in the previous two years to first alongside Requirement 7, making these the most consistently maintained over time. However, full compliance was down 2.1 pp from the previous year, to 85.6%.

Requirement 5 is ranked first, alongside Requirement 7, for full compliance, rising from second in 2016 and 2017.

Globally, the control gap saw only a minor increase of 0.3 pp compared with the previous year. However, EMEA saw its control gap increase by 3.8 pp to 5.4%, and APAC saw its control gap increase by 1.4 pp to 4.7%.

The Americas was the top performer, at 86.0% full compliance. Both EMEA and APAC regions saw a drop in full compliance compared to the previous year. EMEA dropped 7.0 pp and APAC dropped 6.3 pp.

Finance gap grows; others shrink

The control gap increased marginally, by 0.3 pp in 2018 to 5.8%, with Control 5.4 seeing the largest increase.

Finance had the greatest increase in control gap, from 2.8% in 2017 to 8.5% in 2018. All other industry sectors saw a reduction in control gap, with retail improving by 8.2 pp, over the previous year.

The Americas region reported the highest control gap at 6.3%, but this was a reduction of 2.3 pp compared to the previous year. EMEA increased the control gap in 2018, by 3.8 pp, and APAC increased the control gap in 2018, by 1.4 pp.

Merchants outperformed service providers, both in full compliance and control gap, reporting a 3.0% control gap compared to service providers' 6.7%.

Hospitality use highest, retail had none

The use of compensating controls barely increased from 2018's 1.6% to 1.7%.

The Americas contributed the most to this, with 2.2% of organizations using compensating controls. This was a 0.5 pp increase over 2017.

The APAC region did use compensating controls to meet Requirement 5. This was a reduction of 2.8 pp compared to the previous year. Hospitality saw the highest use of compensating controls at 5.3%, with retail reporting no compensating controls for this requirement.

State of control compliance

There were no controls from this requirement on either the top 20 or bottom 20 lists.

Requirement 5 controls

5.1	Deploy anti-virus software
5.2	Maintain all anti-virus mechanisms
5.3	Anti-virus actively running and cannot be disabled
5.4	Documented policies for malware protection

Hospitality most improved; finance flagging

Retail outperformed other sectors, achieving 90.9% full compliance of this requirement, an improvement of 3.4 pp over 2017 figures.

The hospitality sector showed the most improvement, increasing full compliance by 7.3 pp over the past year, to 84.2%.

Finance was the weakest sector, at 82.9% full compliance, and reported the highest control gap at 8.5%. Retail saw the greatest reduction in the control gap, dropping from 10.5% in 2017 to 2.3% in 2018.

5.3% of hospitality organizations turned to compensating controls to meet Requirement 5, the highest across all sectors. Retail reported no compensating controls for this requirement.

Data breach correlation

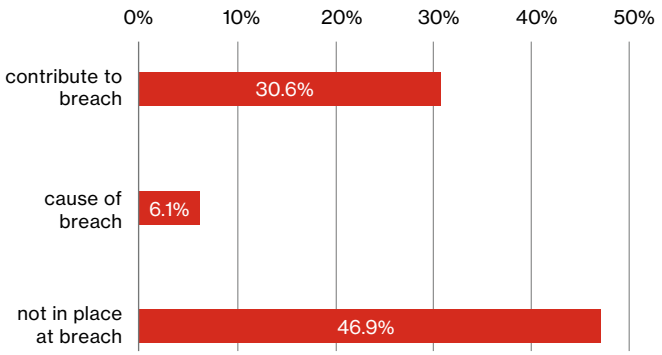


Figure 36. Requirement 5 – breach correlation

Requirement 5 is often considered one of the more straightforward PCI requirements to meet. However, 46.9% of breached entities were noncompliant with this requirement at the time of breach.

Requirement 5 was identified as contributing to the data breach in 30.6% of cases, and was the cause in 6.1%.

Maintain a vulnerability management program – Part 1

The key term for this category is "maintain." We've seen many breached entities without antivirus protection installed. An even greater number of breached entities had antivirus protection installed, but failed to ensure it was properly maintained. Many breached entity environments weren't configured to receive regular updates, leading to attackers deploying malware – often legacy malware. In some events, security controls allowed attackers to reconfigure the antivirus protection to allow malware to persist.

In a smaller set of breached environments, we noticed malicious scripts that were well-known and old enough to be part of antivirus definitions. Without a fully functioning antivirus solution, these viruses were able to execute, resulting in, or contributing to, a successful data breach.

6: Develop and maintain secure systems

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

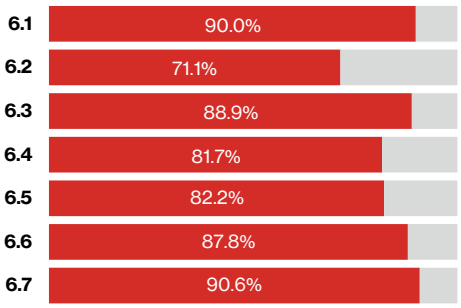


Figure 37. Requirement 6 – full compliance

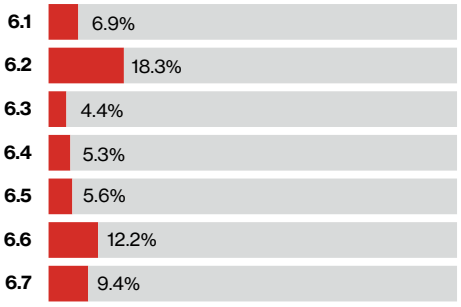


Figure 38. Requirement 6 – control gap

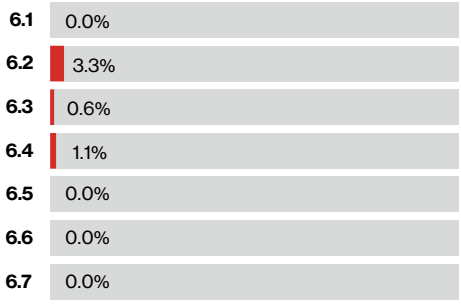


Figure 39. Requirement 6 – compensating control use

Requirement 6 saw the most significant reduction in compliance of all requirements in 2018, with Control 6.2 (ensure that all system components and software are protected from known vulnerabilities) presenting the greatest challenge.

This is a major concern, as this requirement was identified as the leading cause of breach in our analysis of PFI cases.

Largest drop in 2018

The ranking for this requirement went from seventh in the previous year to 11th, and saw the largest drop in full compliance of all requirements. The number of companies to demonstrate full compliance decreased by 20.9 pp to 56.1%, compared to 77.0% from the previous year.

Retail organizations outperformed other sectors, with 59.1% achieving full compliance. However, this was still a significant drop of 22.2 pp from the previous year.

Hospitality was the least compliant sector at 47.4%, representing a 21.9 pp drop from the previous year.

Overall, service providers outperformed merchants, but both sectors saw significant decreases in full compliance compared to the previous year, with service providers falling 34.6 pp to 50.0% and merchants falling 21.1 pp to 58.2%.

Americas make gains

The control gap globally increased by 0.9 pp in 2018, to 6.2%. It ranked sixth, down from fourth overall.

The APAC region reported the highest control gap for this requirement, at 9.9%, and also saw the largest increase 8.8 pp compared to the previous year.

The Americas was the only region that managed to reduce its control gap, dropping from 9.8% in 2017 to 4.5% in 2018.

Hospitality had the highest control gap across industry sectors, at 12.6%. Retail was lowest, at 2.3%.

Big decline in compensating controls

2018 saw an overall reduction in the use of compensating controls for this requirement, falling from 12.3% in 2017 to 4.4% in 2018.

Control 6.2 was previously among the most often compensated control, but 2018 saw an 8.1 pp reduction to 3.3%.

Compensating controls were observed for Controls 6.3 (0.6%) and 6.4 (1.1%) in 2018; they were not reported in the previous year.

The APAC region used the most compensating controls for this requirement, at 8.7%.

Hospitality was the only sector not reporting use of compensating controls in 2018.

Control 6.2 among the weakest

Control 6.2 was 18 of the bottom 20 controls in 2018. Only Controls 11.2 and 11.3 performed worse. Full compliance across all controls dropped compared to the previous year, and the control gap for all Requirement 6 controls decreased, with the exception of Control 6.4, which saw a small increase of 0.1 pp.

Requirement 6 controls

6.1	Reputable outside sources used for vulnerability info
6.2	Protect components and software from known vulnerabilities
6.3	Develop secure software applications
6.4	Follow change control processes
6.5	Address common coding vulnerabilities
6.6	Protect public-facing web applications against known attacks
6.7	Policies and procedures for secure systems and apps

IT services fall most

Full compliance declined across all industry sectors in 2018. IT services saw the greatest decline, falling 31.7 pp to 57.1%.

Retail was the only sector that successfully reduced the control gap, improving by 6.5 pp to 2.3%, compared to the previous year. Hospitality reported the largest control gap, at 12.6%.

Finance reported the highest use of compensating controls in 2018, at 7.3%. Hospitality did not use any compensating controls to meet this requirement.

Data breach correlation

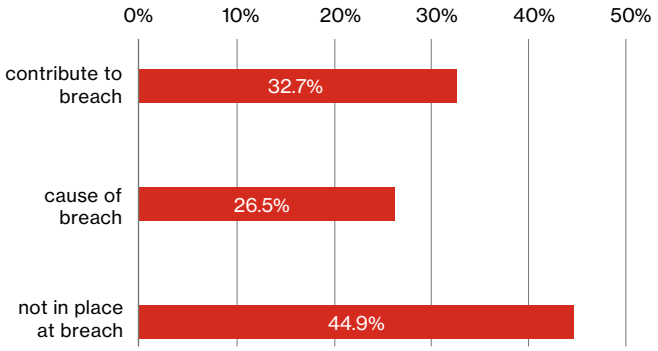


Figure 40. Requirement 6 – breach correlation

Requirement 6, at 26.5%, was identified as the leading cause of analyzed PFI cases and the highest of all PCI DSS requirements.

It was also cited as contributing to 32.7% of the reviewed data breaches.

Maintain a vulnerability management program – Part 2

This requirement prescribes that organizations establish a process for identifying vulnerabilities, patching and performing code review. Many of our investigations involved e-commerce sites that were exploitable via cross-site scripting, insufficient input validation and improper error handling, etc. These were all common coding errors that were identifiable and correctable in a basic code review process.

Organizations should sign up for vendor security advisory notifications. Most solution vendors support an email alert service or RSS feed, and may offer tailored feeds based on specific solutions or technologies. Organizations should ensure automated monitoring and review alerts daily.

7: Restrict access

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.

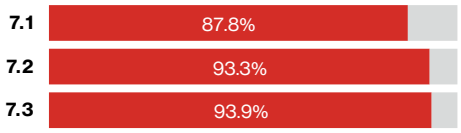


Figure 41. Requirement 7 – full compliance

Figure 42. Requirement 7 – control gap

Figure 43. Requirement 7 – compensating control use

Once again, this requirement tops the overall compliance table, as it has done across the 2017–2019 PSR reporting years.

Requirement 7 is the most consistently maintained over time, although even for this requirement, the figures show a year-on-year drop in compliance since 2016.

Most consistently sustained

Requirement 7 has maintained the top ranking for the 2017–2019 PSR reporting years. This is the most consistently maintained of all PCI DSS requirements over time, across all regions and industry sectors.

Full compliance did drop slightly in 2018, by 3.0 pp to 85.6%. Requirement 7 has remained top-ranked for full compliance for the 2017–2019 PSR reporting years. All sectors saw full compliance figures drop compared to the previous year, with hospitality falling the most by 21.5 pp to 63.2%.

The Americas region outperformed EMEA and APAC for both full compliance and control gap in 2018.

Control gap contracts

The control gap improved slightly, decreasing from 5.7% to 5.0%, raising Requirement 7 from sixth to third of 12.

The Americas reported the lowest control gap, with a reduction from 10.2% in 2017 to 2.7% in 2018.

Both APAC and EMEA saw the control gap widen; APAC by 8.2 pp to 10.7% and EMEA by 5.9 pp to 6.3%. Finance and retail reduced the control gap compared to the previous year, with hospitality seeing the largest increase of 5.8 pp to reach 9.6%.

Noteworthy effort

This is one of three requirements where compensating controls were not used to meet PCI DSS requirements, indicating that organizations can follow the PCI DSS as written. It's a significant achievement.

Top 20 achievements

Controls 7.2 and 7.3 both feature in the top 20 most-compliant controls, with Control 7.2 coming in 14th and Control 7.3 coming in ninth.

Hospitality drops the ball

IT services reported the highest full compliance, at 94.3% – a minor decrease of 0.2 pp from the previous year. Hospitality suffered the most significant reduction, dropping 21.5 pp to 63.2%.

Service providers reported a minor 1.0 pp reduction in full compliance compared to 2017, with merchants falling 14.0 pp in the same period.

Both hospitality and IT services saw the control gap widen from the previous year, with hospitality 5.8 pp and IT services 2.3 pp. Retail reduced the control gap by 2.6 pp and finance by 1.2 pp.

No sectors reported the use of compensating controls to meet this requirement.

Data breach correlation

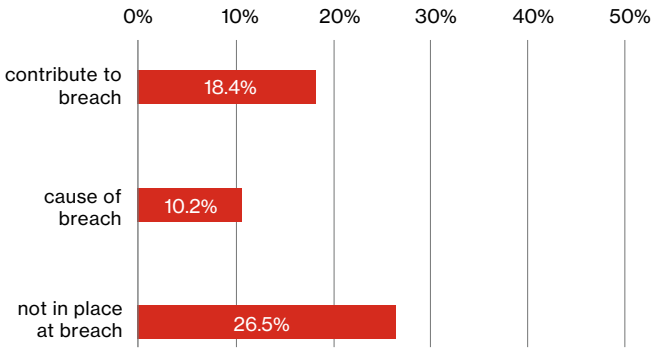


Figure 44. Requirement 7 – breach correlation

Requirement 7 contributed to 18.4% of breaches and was identified as the cause in slightly more than 10% of cases (10.2%).

Control weaknesses against Requirement 7 controls were identified in almost 90% of cases (89.8%, including partial and not-in-place).

Requirement 7 controls

7.1	Limit access to system components
7.2	Access control system based on need to know, set to deny all
7.3	Policies and procedures for restricting access to CHD

Question: In which month are payment card data breaches most likely to occur?

Answer: October (14%), followed by March (12%) and January (10%). The rest are spread out throughout the year.

Source: 6 Year Trend—Verizon PFI global caseload 2010–2016

8: Authenticate access

This Requirement mandates that access to system components is identified and authenticated, requiring that each user be assigned a unique identification.

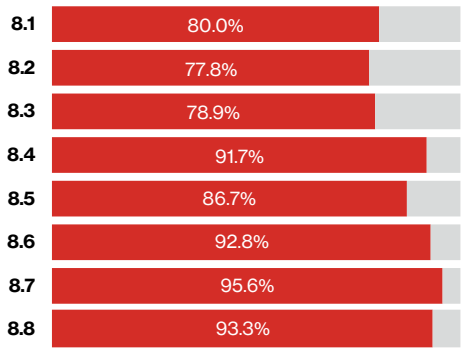


Figure 45. Requirement 8 – full compliance

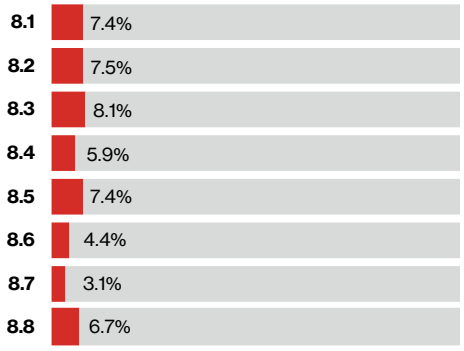


Figure 46. Requirement 8 – control gap

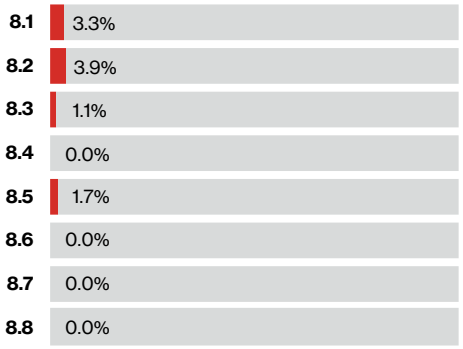


Figure 47. Requirement 8 – compensating control use

The 2019 PSR shows an overall reduction in full compliance for this requirement, a trend that has continued over the 2017–2019 PSR reporting years.

Organizations continue to struggle most with remote access requirements and in managing the requirements for unique user IDs.

It is sobering to note that no breached entities were compliant with Requirement 8 controls at the time of breach, according to PFIs performed by Verizon's VTRAC | Investigative Response Team.

Trending downward

Full compliance fell by 11.8 pp in 2018 to 64.4%, ranking ninth of 12.

Retail organizations reported 70.5% full compliance, ahead of finance at 67.1% and IT services at 62.9%.

APAC outperformed the other regions, at 73.9%, but this still represented a significant reduction in full compliance, decreasing from 94.4% from 2017.

Retail closes gap

The control gap decreased 0.9 pp to 6.9% in 2018, raising Requirement 8 one position to seventh of 12.

The Americas region reduced control gap by 9.2 pp to 4.5% from the previous year; EMEA saw the control gap increase 6.9 pp and APAC 8.6 pp.

Finance and retail both reduced the control gap in 2018 – retail by a significant 9.9 pp to 4.2%.

Hospitality had the largest increase in the control gap of 4.1 pp to 12.5%.

Service providers reported a marginally smaller control gap than merchants, at 6.8% compared to 7.1%.

Most frequent for compensating controls

Requirement 8 remains the most commonly compensated requirement, although this year it's joined by Requirements 3 and 11 at 6.7%.

Hospitality was the only sector that didn't implement compensating controls for this requirement in 2018.

The use of compensating controls reduced 14.6 pp compared to the previous year, to 6.7%. Some 8.2% of service provider organizations implemented compensating controls in 2018, compared to 2.2% of merchants.

Control 8.2 had the highest proportion of compensating controls for this requirement at 3.9%. No compensating controls were used against Controls 8.4, 8.6, 8.7 or 8.8.

Struggle with unique ID; remote access

Both Controls 8.1 and 8.3 feature in the bottom 20 controls for 2018, ranking 12th and 13th overall, demonstrating that organizations continued to struggle with managing unique user credentials and remote access requirements.

Requirement 8 controls

8.1	Policies and procedures for user identification
8.2	Proper user authentication management
8.3	Multi-factor authentication for all remote access to CDE
8.4	Communicate authentication policies to all users
8.5	Do not use group, shared IDs
8.6	Authentication mechanisms not shared among multiple accounts
8.7	Restrict all access to any database containing CHD
8.8	Policies and procedures for identification and authentication

All sectors fall

A reduction in full compliance occurred for this requirement across all industry sectors. Hospitality saw the largest drop of 11.7 pp to 42.1%.

Retail successfully reduced the control gap by 9.9 pp compared to the previous year, while IT services saw an increase of 1.8 pp and hospitality an increase of 4.1 pp.

Full compliance by service providers dropped by 15.1 pp to 64.2%, while merchants saw a smaller reduction of 7.9 pp to 65.2%.

Finance and IT service sectors reported the greatest use of compensating controls, but both noted a sizeable reduction over 2017: 19.2 pp for IT services and 10.0 pp for finance.

Data breach correlation

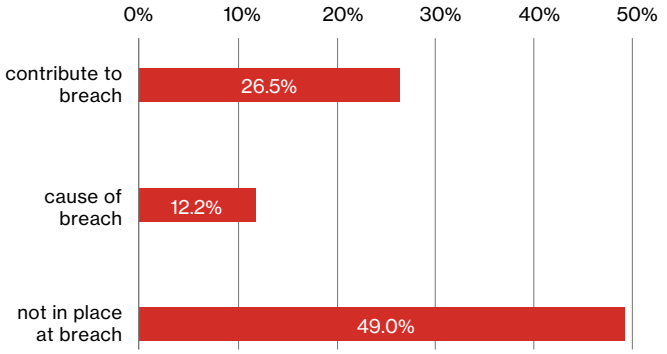


Figure 48. Requirement 8 – breach correlation

No breached entities were compliant with Requirement 8 controls at the time of breach; 49.0% of breached entities were noncompliant overall, with a further 40.8% only partially meeting the requirement's control objectives.

Control failures against Requirement 8 were found to cause 12.2% of breaches and, in turn, contributed to 26.5% of analyzed PFI cases. These figures are exceeded only by Requirement 1 and Requirement 6.

Implement strong access control measures – Part 1

Failure to adhere to this requirement category can relate to multiple areas. These can be as simple as failing to enforce password changes every 90 days, or allowing unlimited failed access attempts to systems. Other areas are the result of poor remote access and administration controls, where organizations did not implement multi-factor authentication or failed to restrict physical access to network devices.

9: Control physical access

This Requirement stipulates that organizations must restrict physical access to all systems within the DSS scope and all hard copies of cardholder data.

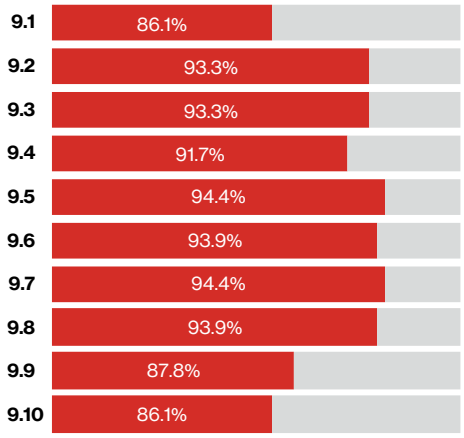


Figure 49. Requirement 9 – full compliance

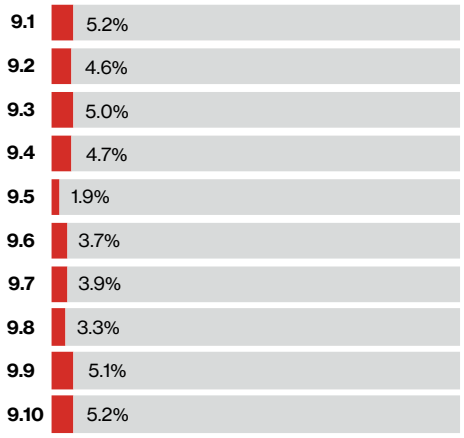


Figure 50. Requirement 9 – control gap

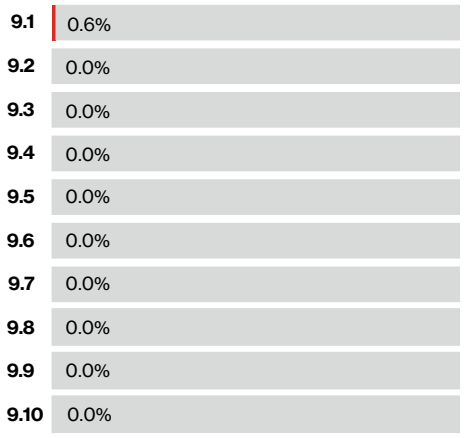


Figure 51. Requirement 9 – compensating control use

While this requirement has maintained a consistent compliance ranking across the 2017–2019 PSR reporting years, full compliance has dropped year-on-year over the same time period. It's notable that both compliance and control gap for Control 9.9 significantly improved compared to the previous year, as this control has now become established.

Maintaining rank as compliance falls

The ranking for this requirement has remained the same for the 2017–2019 PSR reporting years. At fourth – it is tied with Requirement 3 in 2018 – full compliance dropped 6.1 pp to 76.7%.

All regions were within 5.0 pp of each other this year, with the Americas region achieving 78.5% compared to 75.0% for EMEA and 73.9% for APAC.

Finance maintained the highest level of full compliance at 84.1%, but hospitality was the only sector that improved from the previous year, increasing by 9.3 pp to 63.2%.

IT services had the largest drop in full compliance, falling 11.6 pp from the previous year to 82.9%.

Top spot for smallest gap

The control gap improved 0.5 pp to 4.5% from the previous year, with the smallest control gap of all requirements, maintaining the top ranking from the previous year.

Both IT services and hospitality increased the control gap with IT services at 3.2 pp and hospitality at 2.2 pp. Retail reduced it 6.3 pp and finance reduced it 1.0 pp from the previous year.

The control gap reduced for both service providers and merchants, compared to 2017.

The Americas region achieved a 5.8 pp drop to 2.7%, while the control gap for the EMEA and APAC regions widened.

Only retail adopts alternative controls

The use of compensating controls reduced by 0.3 pp from the previous year. In 2017, all sectors reported compensating controls for this requirement, but in 2018, these were replaced in all sectors other than retail, and the use of compensating controls was limited to merchants.

The retail sector also reduced reliance on compensating controls by 4.0 pp to 2.3% from the previous year.

Compliance improvements for 9.3, 9.4

Requirement 9 controls all reduced full compliance, with the exception of 9.3 and 9.4, from the previous year. It was more of a mixed picture for the control gap, with four increasing and six reducing, compared to 2017.

Control 9.9 had the biggest reduction in control gap at 16.6 pp from the previous year, while full compliance dropped 5.7 pp to 87.8%.

No controls from this requirement made the bottom 20 lists.

Only hospitality gains

Financial services achieved higher levels of full compliance than other sectors, at 84.1%. While hospitality was the most challenged in maintaining this requirement, it was the only one to improve full compliance over the previous year, increasing by 9.3 pp to 63.2%.

Retail showed the largest improvement in the control gap, falling 6.3 pp to 6.3%. The IT services control gap increased from 0.2% in 2017 to 3.4% in 2018.

Only retail adopted compensating controls for this requirement, with finance, IT services and hospitality replacing the compensating controls reported from the year before.

Data breach correlation

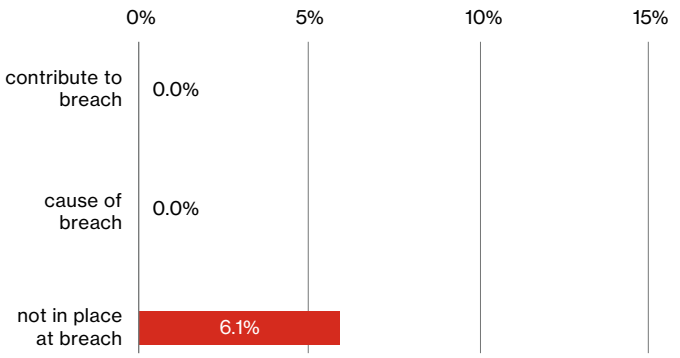


Figure 52. Requirement 9 – breach correlation

Requirement 9 control failures had the lowest overall impact on the data breaches analyzed; no breaches were caused by Requirement 9 failures, nor did they contribute to any breaches.

Interestingly, while Requirement 9 had the lowest level of noncompliance at 6.1%, 69.4% of all PFI cases were only partially compliant with the requirement.

Implement strong access control measures – Part 2

Here's an example of unsafe physical access to certain devices: A breached entity that was deemed compliant asserted that it restricted physical access to sensitive devices (e.g., routers, switches, wireless gateways, etc.). However, our site review found these devices in an unlocked closet in a common hallway shared by unrelated entities – in a large mall. The breached entity was convinced of the problem only after presented with photographs demonstrating these control failings.

Requirement 9 controls

9.1	Appropriate facility entry controls and monitoring access of CDE
9.2	Distinguish between onsite personnel and visitors
9.3	Control physical access for onsite personnel to sensitive areas
9.4	Procedures to identify and authorize visitors
9.5	Physically secure all media
9.6	Control internal and external distribution of media
9.7	Control storage and accessibility of media
9.8	Destroy media when no longer needed
9.9	Protect data capture devices; tampering/substitution
9.10	Documented policy restricting physical access to CHD

10: Track and monitor access

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 DSS scope and synchronization of all system clocks.

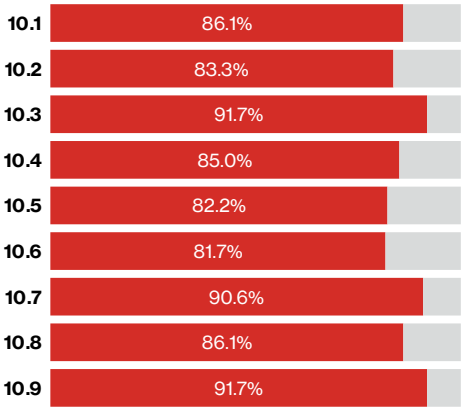


Figure 53. Requirement 10 – full compliance

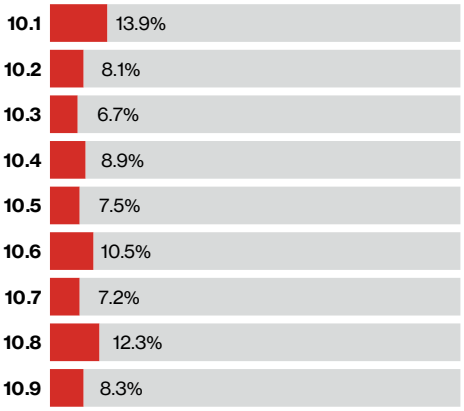


Figure 54. Requirement 10 – control gap

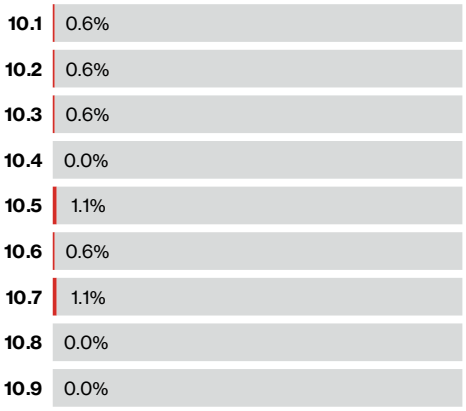


Figure 55. Requirement 10 – compensating control use

While there was some improvement relative to other requirements in this year's review, full compliance decreased and the control gap slightly increased. Increasing numbers of organizations are unable to maintain Requirement 10 controls, and they are failing by an increasing margin.

No breached entities were fully compliant with Requirement 10 at the point of breach, and failings against this requirement contributed to the breach in 40.8% of PFI cases.

Merchants outdo service providers

Full compliance for Requirement 10 fell from 73.0% the previous year to 67.8%, a drop of 5.2 pp. Despite this drop, this requirement improved in ranking by two places, reaching eighth.

Retail outperformed other sectors, with IT services struggling to maintain compliance at 57.1%.

Merchants outperformed service providers by 11.2 pp, with 76.1% of merchants achieving full compliance.

EMEA was the strongest region in terms of full compliance at 70.3%, with the Americas bringing up the rear at 65.6%.

Americas shrink gap

The control gap increased 0.3 pp to 8.8%, improving this requirement's ranking by one position to nine of 12.

The APAC region reported a large 14.0 pp increase in control gap to 18.4% in 2018. Europe saw only a 1.9 pp increase, while the Americas had a decrease in control gap at 8.7%, 4.6 pp lower than the previous year.

The retail sector showed a control gap of 1.8%, a reduction of 12.3 pp compared to the previous year. All other sectors reported a growing control gap, with IT services showing the greatest increase at 12.1 pp.

Merchants (7.1%) outperformed service providers (9.4%).

IT services top users

2.2% of organizations implemented compensating controls to meet this requirement, 3.5 pp lower than in the previous year with Controls 10.5 and 10.7 being the most commonly compensated.

Globally, EMEA had the highest use of compensating controls at 3.1%, and no compensating controls were used in the APAC region.

From an industry perspective, IT services topped sectors at 5.7%, closely followed by hospitality at 5.3%.

Control 10.6 in bottom 20

While Control 10.6 saw the lowest full compliance at 81.7%, it was Control 10.8 that reported the largest control gap at 12.8%. Control 10.6 ranked in the bottom 20 controls in 2018, replacing Control 10.2 from the 2018 PSR.

Requirement 10 controls

10.1	Audit trails linking access to individual users
10.2	Automated audit trails to reconstruct events
10.3	Record user ID, date and time, events
10.4	Time-synchronization technology
10.5	Secure audit trails so they cannot be altered
10.6	Review logs to identify anomalies or suspicious activity
10.7	Retain audit trail history for at least one year
10.8	Reporting of failures of critical security control systems
10.9	Policies and procedures for monitoring all access

Retail comes out on top

Retail reported the highest full compliance across industry sectors at 81.8%. It was the only sector reporting an improvement in full compliance over the previous year.

IT services saw the greatest change in the control gap compared to the previous year, increasing with 12.1 pp to 12.6%.

IT services and hospitality had the greatest use of compensating controls for this requirement. IT services saw a slight increase of 0.2 pp, while hospitality decreased a significant 18.8 pp.

Data breach correlation

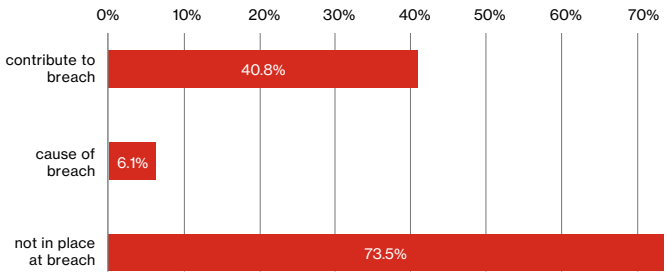


Figure 56. Requirement 10 – breach correlation

Requirement 10 had the highest rates of noncompliance across all the PCI DSS requirements in the reviewed PFI cases; 73.5% of breached entities were identified to be failing against Requirement 10 at the time of breach. No breached entities were fully compliant with Requirement 10 at the point of breach.

While not overly significant in causing data breaches (6.1%), these failures were the highest contributing factor (jointly with Requirement 1) in 40.8% of cases.

Incident preparedness

Requirement 10 plays a fundamental role in the identification of potential security incidents through the configuration, collection and monitoring of security event logs from all system components.

Effective logging mechanisms implement automated audit trails for all system components, which enable reconstruction of events as part of any investigation (Control 10.2).

These logs are only of value to IR efforts if they are synchronized to a single reference time source (Control 10.4), which allows correlation of log activity to piece together the progress of an incident.

Financial organizations struggle most with implementing controls under Control 10.2 – the ability to reconstruct events through proper audit trails.

Retail organizations struggle with a range of controls: user identification and elevation of privileges (Control 10.2.5), due diligence processes for engaging service providers (Control 12.8.3), procedures for detecting unauthorized wireless access points (Control 11.1.2), and maintaining an IR Plan (Control 12.10).

Regularly monitor and test networks

When investigating a breached entity, the audit trail is critical to both understanding and limiting the scope. Having no logs, improperly configured logging parameters or an inadequate retention policy (few to no logs) are sure ways to hamper investigative responders. Over the past few years, we've noticed that more organizations are (finally) developing the ability to recreate the breadcrumbs left by an attacker traversing their networks. Security can only be achieved by implementing effective controls and then actively monitoring and modifying them as needed. PCI DSS-compliant organizations keep critical security controls in place throughout the year, and test them as part of an ongoing security monitoring process.

11: Test security systems and processes

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

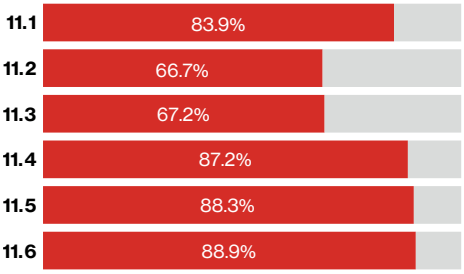


Figure 57. Requirement 11 – full compliance

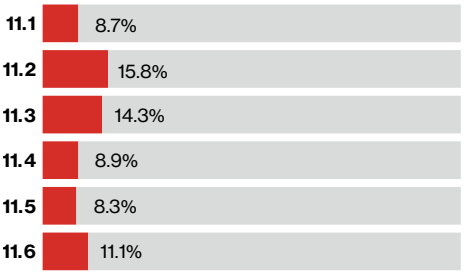


Figure 58. Requirement 11 – control gap

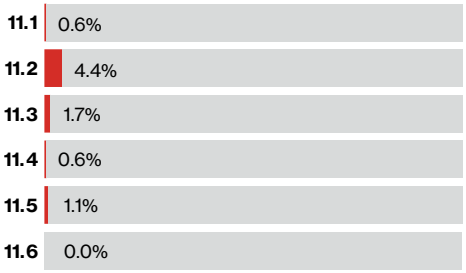


Figure 59. Requirement 11 – compensating control use

Requirement 11 continues to lag at the back of the pack when it comes to full compliance. With the lowest compliance ranking for the 2017–2019 PSR reporting years, this requirement also has the widest control gap, meaning not only are organizations not maintaining compliance, they are also failing on a larger number of controls.

Because this requirement can help organizations identify weaknesses that could be exploited and result in a breach, it's of concern that compliance is not improving.

Back of the pack

Requirement 11 was the lowest-performing requirement in 2018, with only 54.5% full compliance globally; a drop of 13.6 pp from the previous year. Requirement 11 has remained the least maintained of all requirements across the 2017–2019 PSR reporting years.

The APAC region maintained the highest full compliance across all global regions, at 69.6%.

Requirement 11 is ranked 12th of all the requirements, as is the case since 2016.

Hospitality was the least compliant sector at 47.4%, dropping 21.9 pp. But IT services saw the greatest fall – 34.6 pp – compared to the previous year.

Only Control 11.5 saw an improvement in full compliance compared to the previous year.

Lowest compliance, largest gap

As well as reporting the lowest full compliance of all requirements, Requirement 11 also had the largest control gap, at 12.6%. This represented a small 0.7 pp increase from the previous year.

APAC had the widest control gap at 15.0%, with the Americas at 12.3% and EMEA at 12.1%.

The Americas region reduced the control gap from 19.2% in 2017 to 12.3% in 2018, while both APAC and EMEA saw increases.

Hospitality scored the greatest control gap at 24.4% and had the largest increase from the previous year at 16.4 pp. Retail reduced the control gap by 11.9 pp, to 6.4%, compared to 2017.

Highest in Americas, none in APAC

Along with Requirements 3 and 8, 6.7% of organizations implemented compensating controls to meet this requirement. A majority of these were applied to meet Control 11.2 (4.4%).

Compared to the previous year, all regions reduced their use of compensating controls. The Americas, at 8.6%, retained the highest use, with no use of compensating controls by APAC.

Finance reported the highest use at 8.5%, an increase of 2.9 pp over the previous year.

Control 11.2 was the biggest loser

Controls 11.2 and 11.3 had the lowest full compliance, some 20 pp below other Requirement 11 controls. Control 11.2 was the least compliant control in the bottom 20 lists, with a control gap of 33.3%. 11.3 subcontrol also features in the bottom 20, reporting a control gap of 16.7%.

IT services suffers greatest fall

Retail maintained full compliance in 61.4% of organizations, ahead of other industry sectors. IT services suffered the greatest fall in full compliance at 34.6 pp, which was lower than the previous year.

Retail also had the smallest control gap and was the only sector that lowered the control gap from the previous year. Hospitality saw the largest change in the control gap, increasing 16.4 pp to 24.4%.

Use of compensating controls fell globally in 2018 but increased for finance and IT services in the same timeframe.

Data breach correlation

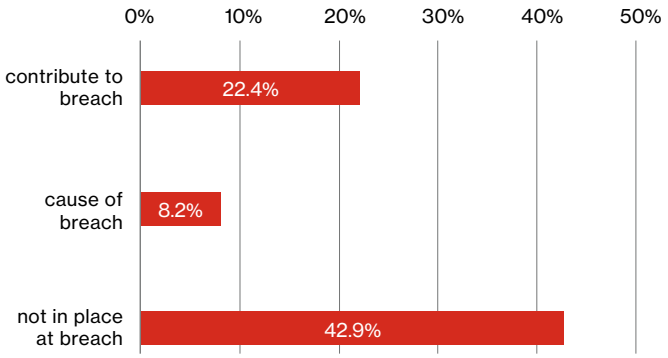


Figure 60. Requirement 11—breach correlation

No breached entity was fully compliant with Requirement 11 controls at the time of breach. Requirement 11 was identified as the cause of data breaches in 8.1% of cases, just ahead of Requirements 3, 5 and 10 (all 6.1%). It also was cited as contributing to the breach in 22.4% of cases.

Incident preparedness

Requirement 11 includes specific requirements for the identification and reporting of unauthorized (rogue) wireless access points (Control 11.1.2), a specific definition of an event that should be reported into an IR process (Control 12.10).

Worth noting is that the IT services industry demonstrates the highest IR preparedness year after year. The only requirement needing attention within IT services is IR procedures for unauthorized wireless access points (Control 11.1.2) and procedures to review and test the IR Plan annually (Control 12.10.2), according to the 2017 data set.

Requirement 11 controls

11.1	Test for the presence of wireless access points
11.2	Run network vulnerability scans
11.3	Implement penetration testing
11.4	Use intrusion-detection systems
11.5	Deploy change-detection mechanism
11.6	Documented procedures for monitoring and testing

Trends

The smaller the organization, the more frequent the payment card breach.

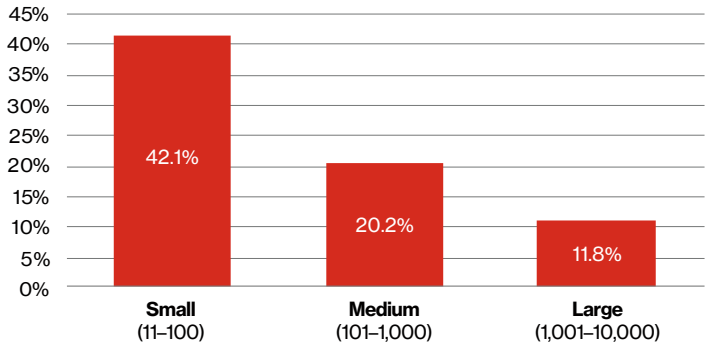


Figure 61. Highest percentage of payment card data breaches based on organization size (# of employees). Source: 6 Year Trend—Verizon PFI global caseload 2010–2016

12: Security management

This Requirement demands that organizations actively manage their data protection responsibilities by establishing, updating and communicating security policies and procedures aligned with the results of regular risk assessments.

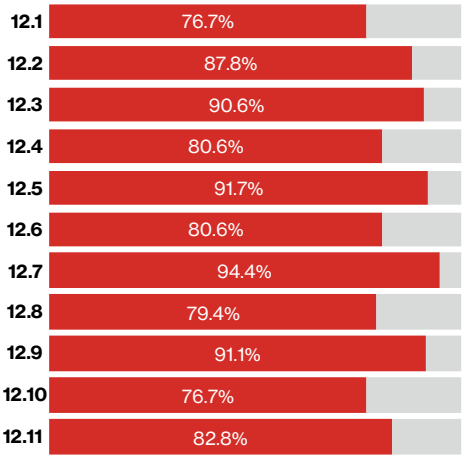


Figure 62. Requirement 12 – full compliance

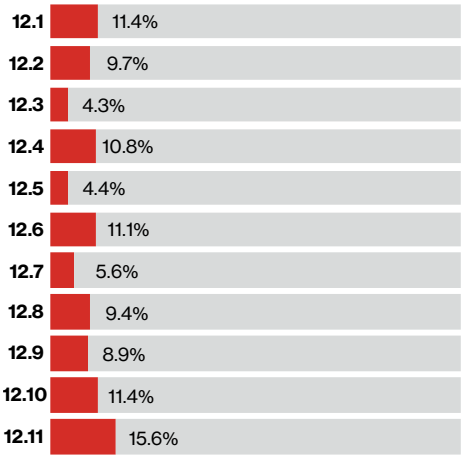


Figure 63. Requirement 12 – control gap

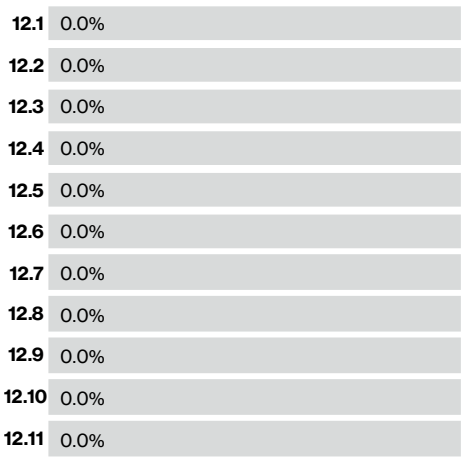


Figure 64. Requirement 12 – compensating control use

Despite a slight improvement in compliance ranking for this requirement, full compliance has fallen year-over-year since 2016. This, in combination with an increasing control gap, suggests that organizations are failing to effectively address the policy and governance aspects of compliance.

While this requirement does not include technical security controls, it still has implications for data breaches, particularly in relation to IR, where organizations continue to face compliance challenges.

Continuing drops across the board

The ranking for this requirement went up one place from 11th in the previous year to 10th. Despite this, full compliance fell 7.4 pp to 62.2%, continuing the downward trend seen in the previous year.

While APAC achieved the highest levels of compliance compared to other global regions at 73.9%, it also had the most significant drop in full compliance, falling 12.2 pp from 2018, which was at 86.1%.

Europe remained the most consistent, reporting 70.3% full compliance compared to 71.4% from the previous year.

IT services and retail both reported significant reductions in full compliance, with IT falling 20.5 pp to 62.9% and retail declining 18.2 pp to 56.8%.

Big slide from second to 11th

The control gap increased 3.9 pp to 9.0%, falling from second to 11th in ranking.

Hospitality recorded the largest control gap at 13.2%, with retail the smallest at 6.6%.

Retail was the only sector to see a reduction in control gap compared to the previous year.

The Americas region had the lowest control gap globally, but reported a 0.3 pp increase to 7.9%. APAC, at 14.3%, had the largest increase, up 10.8 pp from the previous year.

Compensating controls no longer required

This is one of three requirements without the use of compensating controls, a change from the previous year where a small number of companies in the EMEA region (3.6%) used them.

Compliance declines for all controls

Full compliance for all controls dropped compared to the previous year, with the control gap also widening for most. Only Control 12.11 saw a significant reduction in control gap, improving 10.9 pp compared to 2017.

Controls 12.4.1 and 12.11 both feature in the bottom 20 lists and report some of the largest control gap increases at subcontrol level.

Requirement 12 controls

12.1	Publish, maintain and disseminate security policy
12.2	Implement a risk-assessment process
12.3	Develop usage policies for critical technologies
12.4	Define InfoSec responsibilities for all personnel
12.5	Assign InfoSec management responsibilities
12.6	Implement a formal security awareness program
12.7	Screen potential personnel prior to hire
12.8	Manage service providers with policies and procedures
12.9	Service providers acknowledging responsibility
12.10	Implement an incident response plan
12.11	Additional requirements for service providers

Service providers ahead of merchants

The finance sector maintained the highest level of compliance at 67.1%, a small increase of 0.9 pp from the previous year.

IT services saw the most significant drop in full compliance, falling 20.5 pp to 62.9%. However, it was hospitality that had the greatest increase in control gap, widening 8.7 pp to 13.2%.

Service providers slightly outperformed merchants in full compliance, at 62.7% compared to 60.9%, with merchants also reporting the larger control gap of 9.9% compared to 8.7%.

Data breach correlation

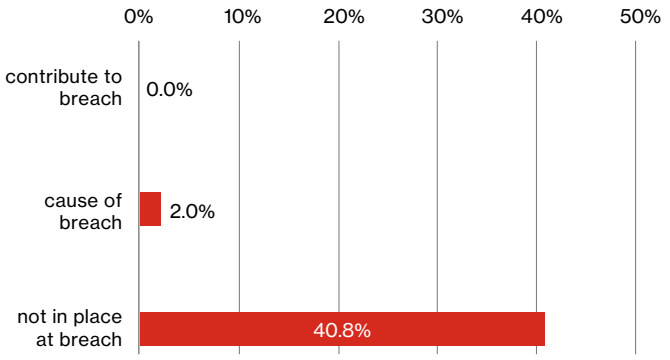


Figure 65. Requirement 12—breach correlation

Requirement 12 was not in place in 40.8% of PFI cases, and no breached entities were compliant at the time of breach.

Requirement 12 was not reported to be significant in causing breaches. It covers topics such as information security policy, risk assessment, awareness training, human resources, third-party management and IR. The nature of these controls is not direct technical (i.e., Requirements 1–8, 10–11) or physical security controls (i.e., Requirement 9), so any exploitation of a control failure would be unlikely to singularly cause a breach. However, weaknesses in these controls were noted as contributing to a few PFI cases (12.2%).

Incident preparedness

IR planning is defined within PCI DSS Requirement 12; Control 12.10 requires that an IR Plan be in place for immediate response to a system breach. The ability to respond in a timely and effective way to all incident situations also needs to be in place (Control 12.5.3). The plan must be reviewed and tested at least annually (Control 12.10.2). Further, the plan must be able to evolve, based on lessons learned and changes to the business environment, and be in line with industry developments (Control 12.10.6).

IR procedures depend upon the ability to detect events related to unusual activity within an environment. Security logging and alert monitoring is a critical component of any IR process. Control 12.10.5 advises that in addition to security logging and log monitoring, an IR process must incorporate alerts from security monitoring systems, including IDS/IPS, firewalls and file-integrity monitoring solutions.

The effectiveness of any IR effort relies on the availability of personnel to respond to events and alerts (Control 12.10.3). Personnel with security IR responsibilities also must be appropriately trained (Control 12.10.4). Investing in developing IR capabilities also means investing in the people responsible for IR delivery.

Worth noting is that hospitality struggled most with user identification and authentication (Control 10.2.5), reviewing and testing the IR Plan (Control 12.10.4), and training staff on breach responsibilities (Control 12.10.4), according to the 2017 data set.

Maintain an information security policy

Although we've investigated a few cases where the breached entity had no formal information security policy, this factor by itself wasn't deemed as a contributor to the breach across events. However, when an entity had no formal security policy in place, there were often companion cultural characteristics, such as a reliance on automated security tools with no level of monitoring or human review of log data and audit trails. Failure to monitor and analyze alerts is also a noncompliant item.

A note about AOCs from our VTRAC | Investigative Response Team

We conducted investigations where we learned that the breached entity bought and paid for a report that asserts its achievement of PCI DSS compliance. We've also engaged in investigations where all parties involved claimed, "There's nothing here to see folks, we are compliant." When the VTRAC | Investigative Response Team responded to a suspected payment card data breach, these AOCs—although sometimes sincere and other times paid for—failed the audit by our incident responders.

So, what about the AOCs? Our team has evaluated breach environments after they were deemed compliant by an assessor, self-assessed by the breached entity and even never assessed but assumed to be compliant.

The following are items noticed in our assessment of a breached environment as it relates to AOCs and reports on compliance (ROCs):

1. Entity was compliant in time, but environmental changes left the revised environment vulnerable
2. The assessor missed a noncompliant item
3. Assessor didn't receive full disclosure from the in-scope entity

These are only a few points of failure. Not all control failures contribute to data breaches. Data breaches can happen because controls aren't in place, or because the controls weren't being actively used or maintained. Neither a signed AOC nor an ROC will shield an entity against a motivated attacker, but actual achievement and maintenance of compliance gives an organization a fighting chance.

So, what's the real relevance of PCI DSS compliance and entities' noncompliance? If all 12 requirements were in place, could an entity avert a breach? Based on our investigations, breaches could likely be "avoided" or "sniffed out" early in the attack path. Some of the identified deficiencies can be appropriately described as contributors to the attack. When multiple deficiencies are combined, the impact is greater or prolonged.

Bottom 20 lists

The 20 biggest control gaps

DSS Ref	Gap	Description
11.2	33.3%	Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as required.
6.2	28.3%	Ensure that all system components and software are protected from known vulnerabilities.
11.3.3	27.2%	Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected.
6.2.b	26.7%	Select a sample of system components and related software, and compare the list of security patches.
1.1	22.8%	Inspect the firewall and router configuration standards.
11.2.1.b	21.1%	Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high risk" vulnerabilities as defined in PCI DSS Control 6.1 are resolved.
11.2.1.a	21.1%	Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.
8.3	21.1%	Incorporate multi-factor authentication for remote network access originating from outside.
8.1	19.4%	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators.
8.1.b	18.9%	Verify that procedures are implemented for user identification management.
8.3.1.a	18.9%	Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the cardholder data environment (CDE).
4.1	18.3%	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission.
10.6	17.8%	Review logs and security events for all system components to identify anomalies or suspicious activity.
11.2.2.a	17.2%	Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.
12.4.1.b	17.2%	Examine the organization's PCI DSS charter to verify that it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.
12.11.b	16.7%	Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.
11.3.1.a	16.7%	Examine the scope of work and results from the most recent internal penetration test.
11.3.2.a	16.7%	Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per defined methodology • At least annually • After any significant changes to the environment
12.11	16.7%	Service providers only: Perform reviews—at least quarterly—to confirm personnel are following security policies and operational procedures.
12.4.1.a	16.1%	Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.

Figure 66. The 20 biggest PCI DSS control gaps in 2018

Control gap by testing procedure

Biggest increases in gap (2018 vs. 2017)

Rank	Gap (2018)	Gap (2017)	Change	DSS Req	Description
1	28.3%	12.3%	16.0 pp	6.2	Ensure that all system components and software are protected from known vulnerabilities.
2	26.7%	11.5%	15.2 pp	6.2.b	Select a sample of system components and related software, and compare the list of security patches.
3	18.9%	4.1%	14.8 pp	8.3.1.a	Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE.
4	16.7%	2.5%	14.2 pp	12.11.b	Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.
4	16.7%	2.5%	14.2 pp	12.11	Service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.
6	17.2%	3.3%	13.9 pp	12.4.1.b	Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.
7	15.6%	2.5%	13.1 pp	12.11.1	Examine documentation from the quarterly reviews to verify they include documenting results of the reviews. Review and sign off on results by personnel assigned responsibility.
8	21.1%	8.2%	12.9 pp	8.3	Incorporate multi-factor authentication for remote network access originating from outside.
9	16.1%	3.3%	12.8 pp	12.4.1.a	Verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.
10	33.3%	21.3%	12.0 pp	11.2	Examine scan reports and supporting documentation to verify that internal and external vulnerability scans occurred.
11	14.4%	2.5%	12.0 pp	12.11.a	Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies.
12	15.0%	4.1%	10.9 pp	8.3.1.b	Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.
13	13.9%	3.3%	10.6 pp	10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security.
14	10.0%	0.0%	10.0 pp	2.3.f	SSL and/or early TLS: Review the documented risk mitigation and migration plan.
15	12.8%	3.3%	9.5 pp	10.8.1.a	Examine documented policies and procedures, and interview personnel to verify that processes are defined and implemented to respond to a security control failure.
16	13.3%	4.1%	9.2 pp	2.2.b	Verify that system configuration standards are updated.
17	12.2%	3.3%	8.9 pp	10.8.b	Examine detection and alerting processes, and interview personnel to verify that processes are implemented for all critical security controls.
17	12.2%	3.3%	8.9 pp	11.3.4.1.a	Affirm that penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls or methods.
17	12.2%	3.3%	8.9 pp	10.8.a	Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems.
20	21.1%	12.3%	8.8 pp	11.2.1.b	Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans to verify that the high-risk vulnerabilities as defined in PCI DSS Control 6.1 are resolved.

Figure 67. The 20 largest increases in control gap in 2018

Appendix A:

Methodology

State of compliance

This research is based on analysis of quantitative data gathered by QSAs from multiple organizations. We diversified our annual data set by engaging external collaborators—domestic and international, large and small.

These findings are presented globally, with additional comparisons between geographic regions (Americas, EMEA and APAC), between four main industry verticals (financial, retail, hospitality and IT services) and organization validation type (service providers and merchants).

The assessments carried out for this report covered both PCI DSS versions 3.2 and 3.2.1. Unless explicitly stated otherwise, all of the references to controls and test procedures refer to DSS 3.2. It often requires multiple assessments to produce an assessment report. In several cases, an assessment report is the product of assessments conducted globally or across a specific region. In some cases, the number of in-scope locations exceeded 100 locations per report.

The PCI DSS compliance assessments were conducted in 2018. Trend analysis includes year-over-year comparisons to determine how the state of compliance evolved over multiple years. These changes in contributors, and the potential changes in their areas of focus, add a layer of difficulty when identifying trends over time.

The accompanying figures show how the organizations from which we gathered interim PCI DSS assessment data to create the report break down by industry and region.

Validation type:
Service providers: 220
Merchants: 82

The composition of the 2017–2018 PCI DSS state of compliance data set:
302 legal entities

Regional representation:
Americas: 151
APAC: 59
EMEA: 92

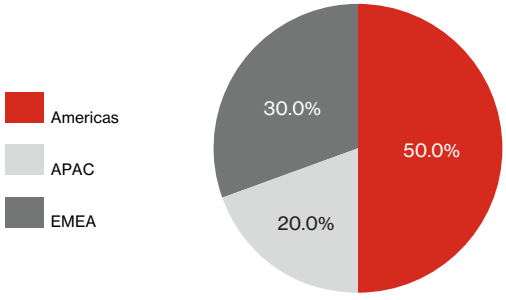


Figure 68. State of compliance geographic regions

Country representation:

Primary locations where assessments were conducted (in-scope locations include more than 60 countries):

Americas: Brazil, Canada, Chile, Mexico, United States, Uruguay

APAC: Australia, Hong Kong, India, Japan, Malaysia, New Zealand, Singapore, South Korea, Taiwan, Thailand

EMEA: Denmark, Finland, France, Germany, Ireland, Italy, Kingdom of Bahrain, Netherlands, South Africa, Switzerland, United Kingdom

Industry representation:
Financial: 153
Hospitality: 32
Retail: 60
IT services: 53
Contact centers: 4

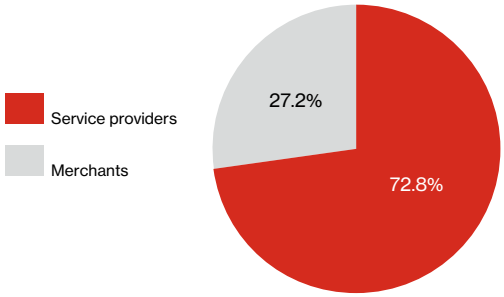


Figure 69. Validation type

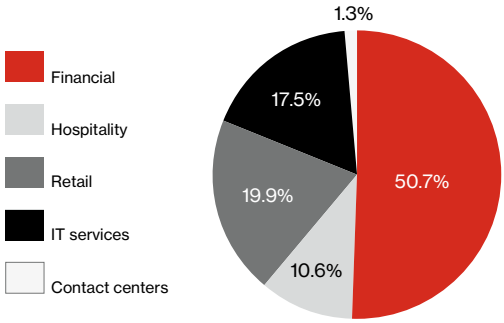


Figure 70. Industry representation

Data contributors

Global PCI DSS compliance management survey
Verizon conducted an opt-in survey of PCI DSS-compliant organizations to determine how they approach compliance program management, and obtain insights on compliance program governance, performance measurement, continuous improvement and capability maturity.

There were 55 respondents, spread almost equally across the Americas, Europe and APAC.

See page 90 for a list of contributing organizations.

Data breach correlation

Data for the data breach correlation section (see page 32) is separate from our PCI DSS data set. This provides unparalleled insights, with "real-world data," on which organizations experience data compromises, and how their behavior and ability to conform to compliance regulations affected the sustainability and effectiveness of their control environments.

The data comes from investigations into organizations following a breach of payment card data. These investigations were carried out by the VTRAC | Investigative Response Team in 2016–2018. The data for long-term analysis of confirmed payment card data breaches includes investigations conducted in 2010–2016. The data sets of organizations undergoing regular compliance validation and those that were breached do not overlap. None of Verizon's PCI DSS customers experienced a data breach.

Appendix B:

Mobile security: an escalating concern

By Cynthia B. Hanson, contributor, Verizon PCI Security Practice

Designing a framework that incorporates Verizon's payment security models can help solve security gaps in mobile technology—gaps that can lead to payment security breaches. Mobile security is a critical issue as global mobile usage and data traffic skyrocket. In a mere two years—from 2017–2019—mobile traffic more than doubled worldwide. In the Verizon 2018 PSR, we introduced the 9 Factors of Control Effectiveness and Sustainability, and 4 Constraints of Organizational Proficiency (4 Cs)—updated this year to the 5 Constraints of Organizational Proficiency (5 Cs)—as useful models for building a better security framework. At a time when cybercriminals are taking advantage of the widening security gaps in mobile device development, these models can help build better mobile payment security (see page 13) while complementing other frameworks, such as ISO27001, NIST or SANs.

Mobile: a new target of choice for cybercriminals[27]

As technology continues to evolve, the resulting complexities and overlapping communication networks must continually be addressed. Add in ever-increasing numbers of mobile devices, mobile data traffic, e-mobile transactions, m-commerce, and evolving mobile-related payment technology, and you have an ideal situation for cybercriminals. Mobile users are far more vulnerable to social attacks attempted on mobile devices.[28] Unaddressed mobile security gaps are creating new attack surfaces in previously secure corporate networks.[29]

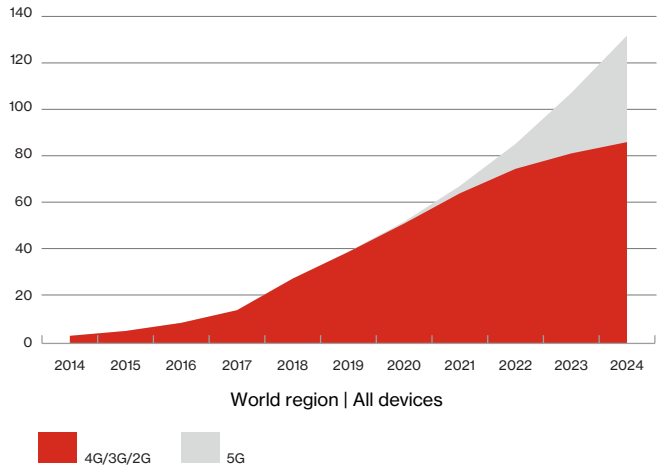


Figure 71. Global mobile data traffic (EB per month), Ericsson Mobile Data Traffic Outlook

The rapid increase in global mobile data traffic has created a wider landscape for the picking for payment security breaches. Mobile traffic numbers worldwide are projected to approximately double every two years through 2022. In just the past year, mobile data traffic increased 82% worldwide. Much of the rise was due to a significant jump in China's data traffic and increasing numbers of smartphone subscriptions in India.[30] Concurrently, technology users are being pushed outside the perimeters: Use of the cloud, for example, has changed the traditional boundary for access controls and security. Increasing numbers of employees are accessing work email and other work-related activities on personal phones. The combination of cloud-delivered software and mobile devices is weakening existing built-in network controls, VPNs and physical infrastructures, and bad actors know it. For a bad actor, mobile devices are a great target because they are continuously connected to the internet—and often to corporate servers. They also contain a wealth of information and multiple avenues for access, such as location, vulnerable apps (such as flashlights), photos of slides with corporate data, etc.[31] Without proper protections, this crossover or overlapping of mobile personal and work usage increases vulnerability in four critical areas: networks, devices, apps and user behavior.[32]

verizon business ready

27 "It's time to tackle mobile security," Verizon Mobile Security Index, 2019, https://enterprise.verizon.com/resources/reports/mobile-security-index/
28 ibid.
29 "A Business Case for a Mobile Security Solution," Robin Gray, Wandera, Jan. 28, 2019, https://www.wandera.com/mobile-security/a-business-case-for-a-mobile-security-solution/
30 Ericsson Mobility Report, June 2019, https://www.ericsson.com/en/mobility-report/reports/june-2019
31 "Post-Perimeter Security: Addressing Evolving Mobile Enterprise Threats," Tara Seals interviews Patrick Hevesi (Gartner), David Richardson (Lookout), Mike Burr (Google), Threatpost, March 20, 2019, https://threatpost.com/post-perimeter-security-mobile-enterprise/142880/
32 "It's time to tackle mobile security," Verizon Mobile Security Index, 2019

Verizon's 2019 Mobile Security Index (MSI) survey findings—the perception gap

For the past two years, Verizon has commissioned an independent research firm to survey more than 600 mobility professionals on mobile-related usage. One of the key findings cited in the Verizon Mobile Security Index 2019 report was "the perception gap."[33] Some 33% of respondents reported a mobile device-related compromise, up 5% from the 2018 MSI report. Of those compromised, 62% characterized it as "major" and 41% as "major with lasting repercussions." Some 67% of respondents admitted a lack of confidence in mobile security as compared with the security of other devices.

Despite growing risks and increasing numbers of significant breaches, a surprising percentage of organizations donned rose-colored glasses in relation to their mobile security capabilities:

- 33% ranked their security measures as "very effective"
- 84% ranked their security measures as "effective"
- 79% were convinced they would find infected mobile devices
- 77% were certain they would uncover employee misuse

Some 48% of respondents knowingly sacrificed "security for expediency of organizational performance" and did not take necessary steps to protect themselves.[34] Only 45% of organizations had installed mobile endpoint security. The percentages for other defenses, such as anti-malware and mobile threat defense, ranked even lower.

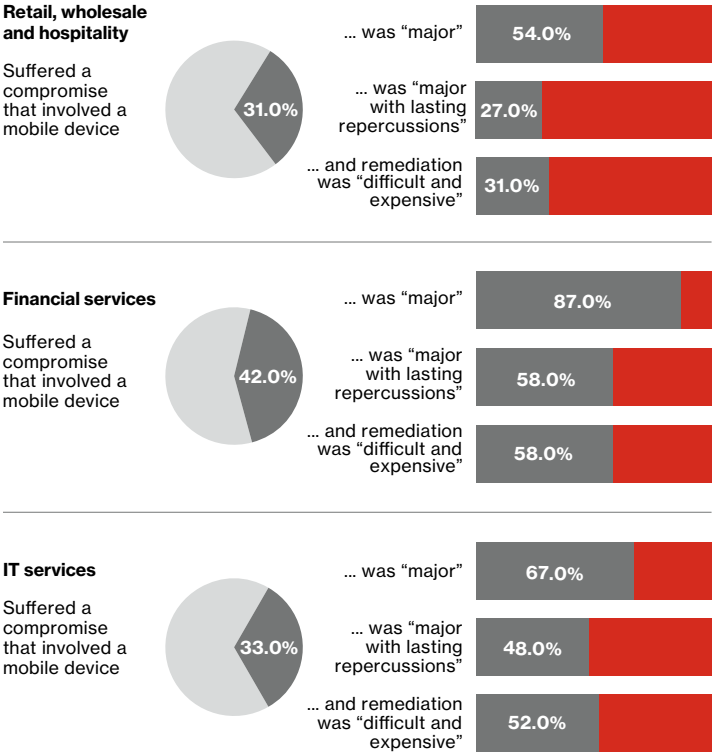


Figure 72. 2019 Verizon Mobile Security Index survey findings

verizon business ready

33 "It's time to tackle mobile security," Verizon Mobile Security Index, 2019

34 Verizon Mobile Security Index, 2018, https://enterprise.verizon.com/resources/reports/mobile-security-index/

How can these mobile trends impact payment security?

The explosion of mobile device ownership worldwide, and the concurrent rising wave of data usage, is driving e-mobile, which is significantly increasing e-commerce. "In 2019, retail e-commerce sales are projected to increase 14.0%; m-commerce is expected to rise 28.8%. Smartphone commerce is projected to reach nearly $200 billion."[35]

The rapid increase in mobile payments brings with it a plethora of concerns for payment security. Digitalization is rapidly reshaping retail due to the evolution of disruptive technologies, consumer and generational shifts in shopping, and new forms of competition that require company adaptation. Other significant changes in retail include a shift away from malls and brick-and-mortar establishments, in-store tech, omnichannel marketing, mobile-based restaurant and hotel billing and ordering of services, and an increase in online delivery and ordering for groceries, restaurants, pet care, etc. This transformation, paired with mobile's proliferation, is resulting in an escalation of mobile payments worldwide. With mobile recently overtaking the desktop in web traffic, social engineering techniques and attacks are on the rise.[36] This is no time for organizations to be slow or hesitant about acting on mobile security.

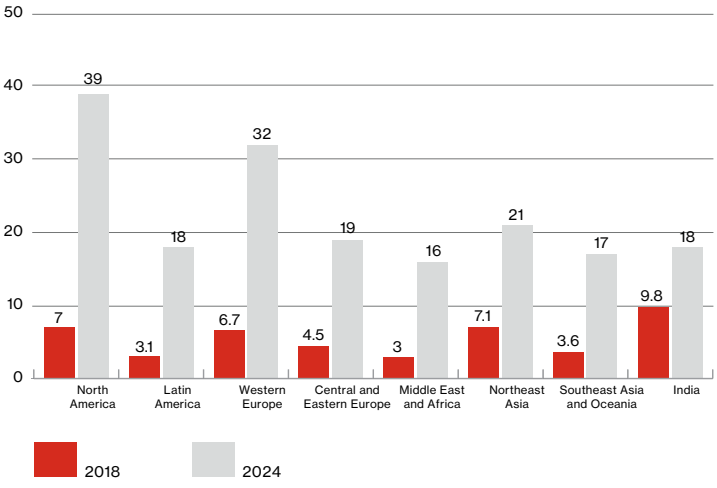


Figure 73. Mobile data traffic per smartphone (GB per month), Ericsson Mobile Data Traffic Outlook

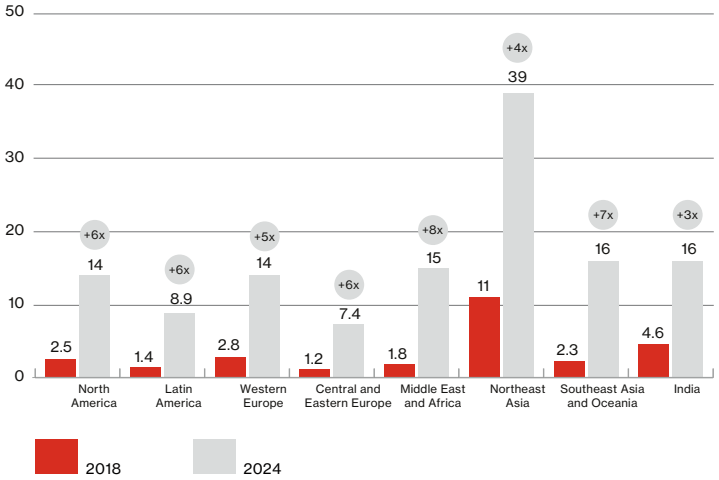


Figure 74. Regional mobile data traffic per smartphone (EB per month), Ericsson Mobile Data Traffic Outlook

"In the Financial Services industry, some 69% of the primary smartphones used for work are Bring Your Own Device (BYOD)," according to a 2018 Forrester survey of 416 information workers in the financial services industry.[37]

Increasing numbers of employees are using their personal mobile devices to access organization email, lists, databases, downloads and other work-related activities, while also inadvertently downloading questionable apps, clicking on phishing links and using faux sites and the cloud without proper protections. This crossover of personal and professional use leaves devices vulnerable to proxy malware, which opens SOCKS proxies on mobile devices that can provide attackers access to any network to which the device connects.[38] SIM card attacks on mobile devices—called SIM jacking or swapping—are also a recent, growing threat that can result in fraudulent transfers of money, business documents and sensitive data (see sidebar written by the U.S. Secret Service, page 70). This gap allows cybercriminals to potentially penetrate corporate servers and private databases by tricking users, or in the case of SIM card attacks phone company personnel. Threat actors are continually trying to outsmart the system by creating new methods for accessing data and assets.

The most common threat vectors are poorly coded apps, malware (including ransomware), rogue or insecure Wi-Fi, and phishing—the number-one threat on mobile. Mobile users are 18 times more likely to encounter phishing than malware.[39]

Yet many organizations continue to support BYOD programs because using employee-owned devices is more cost-effective than using company-issued devices—unless BYOD devices lead to a breach.

verizon business ready

35 "The Future of Retail 2019: Top 10 Trends that Will Shape Retail in the Year Ahead," Andrew Lipsman, eMarketer, December 5, 2018, https://www.emarketer.com/content/the-future-of-retail-in-2019

36 "Understanding the mobile threat landscape in 2019," Wandera, 2019, https://www.wandera.com/mobile-security/mobile-threat-landscape/

37 "Forrester Analytics Global Business Technographics Workforce Benchmark Survey," 2018, https://go.forrester.com/

38 "Post-Perimeter Security: Addressing Evolving Mobile Enterprise Threats," Tara Seals, Threatpost, March 20, 2019, https://threatpost.com/post-perimeter-security-mobile-enterprise/142880/

39 "Phishing attacks are moving to messaging and social apps at an alarming rate," Liarna La Porta, Wandera, May 8, 2018, https://www.wandera.com/mobile-security/phishing/mobile-phishing-attacks/

Applying Verizon's models to enhance mobile maturity

First introduced by Verizon in 2018, the "Baseline, Better, Best" matrix (see page 67) is a highly practical program maturity tool for helping companies implement the next levels of mobile security. Addressing the entire security lifecycle is imperative to secure overlapping technologies, which means following steps to assess, protect, detect and respond. This approach is commonly used by companies for their IT systems, and Verizon believes the time has come to include mobile devices in the plan.

In the 2018 PSR, Verizon introduced the 9 Factors of Control Effectiveness and the 4 Constraints (4 Cs) of Organizational Proficiency (now the 5 Cs; see page 10 of this report). Application of these models can enhance and support more standard methods used to combat mobile security issues.

Enhancing mobile and payment security through the 9 Factors

The 9 Factors are highly applicable to four critical areas of mobile vulnerability—the networks, devices, apps and user security. Worth noting is that Factor 8, maturity measurement, is highly applicable to all four of these areas of mobile security. Stagnation is deadly to any kind of evolution; agility and adaptation ensure growth. As mobile technology morphs and expands, the need to include mobile security in maturity measurement processes is increasingly critical.

The networks: Many are familiar with the phrase, "adapt or die." The greatest risk to network security from mobile devices can be the slow rate to which companies are adapting to mobile's potential impact. Networks must be redesigned with mobile in mind; their foundations should be underpinned with standards such as the 2018 General Data Protection Regulation (GDPR) forged by the European Union and the February 2019 mobile device security guidelines created by NIST[40] in the U.S. For example, Gartner uses a basic pre-work mobile security strategy of full unified endpoint management (UEM), which includes assessing the levels of data being installed on devices to determine the different types of tools, practices and configurations needed.[41]

Applying the factors: Factor 2, control design, is a major consideration when addressing interlinking network security. It's critical to integrate mobile security into your organization's overall IT security design, and to build a framework that can be adapted as needs—and threats—evolve. Factor 8, maturity measurement, is also highly relevant. Companies must be agile and constantly maturing in their approach to mobile security.

Maintaining a wash-rinse-repeat approach to data protection can put your organization in the crosshairs.

Devices: Device loss and theft is one of the greatest risks data organizations can face, especially if phones are not locked and contain confidential information. Lost corporate devices could be traced to more than 25% of data breaches within the financial services sector from 2006–2016.[42] That's why regularly patching and updating mobile devices is critical to reducing the risk of mobile security breaches. Implementing Full Disk Encryption (FDE) renders data on stolen devices useless. Mobile Device Management (MDM) also enables remote wiping of corporate apps and associated data. Additionally, IT departments should also distribute apps to employees to avoid fake or infected ones, and then secure those apps on devices before transaction are made.

Applying the factors: Factor 3, control risk, is an important consideration for mobile device security, because "any control failure can severely handicap an organization's ability to protect cardholder data."[43] The failure to lock a device that contains organization information can be the channel to a payment security breach—especially if the device is stolen or left in a public place.

Apps: M-commerce is on the rise, requiring the increased use of apps for mobile payments. Users should be encouraged to use only official app stores, as they enforce app vetting. Even then, many companies lack visibility or measures to "understand and prevent data leaks on their mobile devices that can happen even when using approved and seemingly trustworthy apps downloaded from these sources."[44] Travel and fitness apps are especially easy targets. Phishing was the culprit in more than 42% of mobile-related compromises reported in the 2019 MSI survey. Enterprise users are three times more likely to be a victim of a phishing attack on mobile than non-mobile.[45]

verizon business ready

40 "Mobile Device Security – Cloud and Hybrid Builds," Joshua Franklin, et al., National Institute for Standards and Technology, February 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-4.pdf

41 "Post-Perimeter Security: Addressing Evolving Mobile Enterprise Threats," Tara Seals, Threatpost, March 20, 2019

42 Bitglass, Financial Services Breach Report 2016, https://pages.bitglass.com/Report-Financial-Services-Breach-Report-2016-LP.html

43 Verizon 2018 Payment Security Report, 2018, https://enterprise.verizon.com/resources/reports/payment-security/2018/

44 "Understanding the mobile threat landscape in 2019," Wandera, 2019

45 "It's time to tackle mobile security," Verizon Mobile Security Index, 2019

Evolving your mobile security strategy

		Baseline	Better	Best
Assess Understand your devices, your data, who has access, and what the threats are.	Implement	• Ensure that mobile is included in all your security plans and policies • Understand risk factors, including geolocation, industry, size, and critical data streams • Understand and manage your employees' data usage	• Take a full accounting of your assets to determine risks and potential exploits • Track updates and patches and coordinate deployment • Define guidelines for acceptable use, including file transfer	• Measure your environment against applicable regulatory frameworks • Establish a security-first employee focus and culture • Implement a risk evaluation and scoring framework
	Maintain	• Regularly assess defenses to confirm that detection capabilities meet set standards	• Test employee mobile security awareness at least once a year	• Perform regular, at least quarterly, 360° reviews of mobile threat landscape and security posture
Protect Harden assets, protect data and secure the emerging mobile perimeter.	Implement	• Deploy a device enrollment policy • Implement a strong password policy and verify adherence • Limit Wi-Fi to approved networks • Prevent employees from installing apps downloaded from the internet • Establish formal policies for corporate-liable/BYOD detailing employees' responsibilities	• Implement a unified endpoint management (UEM) system to pre-configure devices with approved apps, limit additions to company app store and set/manage policies • Deploy a private network solution to any device that gathers or accesses sensitive data • Leverage voice, messaging and file encryption solutions	• Implement device segmentation, keeping personal and work data and applications separate • Change device procurement policies to favor cellular over Wi-Fi • Develop governance policies for the transfer of data between IoT devices
	Maintain	• Regularly review access to systems and data	• Identify users who are out of compliance or misusing assets	• Use activity-based monitoring to block malicious behavior
Detect Identify vulnerabilities and anomalies quickly to enable speedy response to reduce impact.	Implement	• Deploy mobile threat detection software to scan for vulnerabilities • Implement log monitoring to spot signs of attacks and device misuse	• Introduce a solution to identify and prevent complex phishing attacks – including those happening outside email • Implement processes to identify devices that are out of compliance	• Introduce data visibility and content control tools • Deploy secure productivity apps to protect collaboration • Implement secure IoT device visibility and management platform
	Maintain	• Provide regular security training on the dangers associated with mobile devices and how to spot warning signs of an incident	• Review apps to identify anomalies such as excessive permissions and potentially dangerous behavior like scanning corporate networks	• Use data loss prevention (DLP) tools to limit data transfer, provide early warning and enable forensics
Respond Remediate issues, recover operations and enable forensic analysis.	Implement	• Implement policies to contain attacks by locking down private information and isolating infected, lost or stolen devices	• Create an incident response plan that informs employees of what to do in the event of an incident • Implement push messaging to tell users and admins what to do in the event of an incident	• Automate corrective actions to reduce response time and limit exposure • Implement employee-friendly policies and solutions tailored to BYOD security
	Maintain	• Remind employees how to report any suspicious activity – make it an easy-to-remember email address or phone number	• Exploit the complete range of UEM capabilities to identify full range of threats and trigger responses	• Run regular response exercises on areas of concern (e.g., phishing)

Figure 75. Verizon 2019 Mobile Security Index: Baseline, better, best.

Applying the factors: The safety of apps is very much a user behavior issue. Factor 1, control environment, is key to creating an educated workforce attuned to app safety. "Control environment is created through the culture of an organization and is defined and enforced through the values, priorities and management styles of the business."[46] Without a security-conscious culture, too much responsibility is left to the individual, which endangers the entire organizational framework.

User behavior: Companies need strong corporate policies for corporate and personal devices that interface with corporate data and assets. The user-behavior challenge can be broken down into: misuse of corporate resources and accessing inappropriate content and exposing organization data and assets to increased risk.[47] BYOD users should be required to familiarize themselves with the many threats specific to mobile, such as SMS attacks and spoofing, smishing or social engineering of malicious software onto devices, man-in-the-middle attacks over Wi-Fi, and fake websites. Smishing is short for SMS phishing, and it works much the same as phishing. Users are tricked into downloading malware onto their phones from an SMS text as opposed to from an email to their phone.

However, even when corporate policies are in place, users may still be lured into using questionable apps and convenient public Wi-Fi. Mobile can also convey a false sense of safety, and small keyboards make it easy to accidentally click on links and advertisements harboring hidden dangers. Good user practices require a lot of self-assessment (Factor 9), and organizational restrictions and guidelines with strong security components should be in place.

Self-assessment:
Do you have infected devices right now?

Look up how many mobile devices your organization has in the chart below. The upper and lower bounds show how likely it is that at least one of them is infected.

Number of devices	Likelihood of having at least one device infected with a malicious app
100–249	3% – 7%
250–499	7% – 14%
500–999	14% – 26%
1,000–2,499	26% – 53%
2,500–4,999	53% – 78%
5,000–9,999	78% – 95%
10,000+	95% – 100%

Figure 76. Self-assessment: Do you have infected devices right now? Data provided by Wandera.

Applying the factors: Factor 1, control environment, is fundamental to addressing user behavior. A mature organization should shoulder the core responsibility and educate employees, while also holding them accountable for engaging in safe and supportive organizational practices. Factor 9 is also a critical management consideration.

Self-assessment:
Would your users use these access points?

Many attacks take advantage of familiar public Wi-Fi names (SSIDs). Users may already have these stored in their device, which could try to connect automatically.

How many of these would you connect to without checking their legitimacy?

Southeastern_WiFi	The C1oud
Hilton Honors	Starbucks WiFi
hhonors	Airport_Free_WiFi_
McDonalds Free WiFi	Signature
Marriott_GUEST	Fairmont
PretCustomer	@Hyatt_WiFi
American Airlines lounge Wi-Fi	Courtyard_GUEST
starbuckz free wifi	Wifi_Guest

These SSIDs were among the most often identified by Wandera as exhibiting suspicious behavior, suggesting that they were actually being used by a rouge hotspot.

Note that some of these are misspelled – starbuckz? – giving the game away. Yet, users still connect to them.

Figure 77. Self-assessment: Would your users use these access points? Data provided by Wandera.

46 Verizon 2018 Payment Security Report, 2018, https://enterprise.verizon.com/resources/reports/payment-security/2018/
47 "It's time to tackle mobile security," Verizon Mobile Security Index, 2019

The 9 factors when applied to mobile security

Factor 1	**Control environment**	Establishing and maintaining a control environment that governs the use of mobile devices is a foundational step for managing payment security risks associated with the use of mobile devices.
Factor 2	**Control design**	Mobile devices require a very firm control design profile, detailing the exact specifications for controlling applications that can be installed on the device.
Factor 3	**Control risk**	Securing mobile devices requires constant vigilance. It is essential to evaluate and frequently re-evaluate the effectiveness of the controls in place to protect sensitive data stored and accessed by mobile devices.
Factor 4	**Control robustness**	Mobile devices, like desktop computers, operate in dynamic, ever-changing business and threat environments and require multiple lines of defense. Protection of data in mobile environments should be maintained despite disruptions, unwanted changes or attacks, i.e., the ability to absorb significant amounts of "damage" before experiencing control failure.
Factor 5	**Control resilience**	Organizations should develop and maintain the ability to rapidly detect and respond to mobile devices that don't conform to operating specifications per the control design profile. Security events and incidents involving mobile devices should be thoroughly analyzed to improve the robustness of the mobile security framework and controls.
Factor 6	**Lifecycle management**	Mobile devices often have a shorter lifespan than desktop devices. With rapidly changing hardware and applications, security controls in place for mobile devices should be managed and controlled from their inception to retirement. Each stage of the control security lifecycle should have checkpoints to evaluate the effectiveness of the controls and identify areas of improvement.
Factor 7	**Performance management**	The performance of data protection across the entire mobile device landscape should be monitored and measured (development, implementation, monitoring and evaluation or evolution – DIME).
Factor 8	**Maturity measurement**	It's essential to evaluate the organizational process and capability maturity for each of the key aspects of mobile security, and to apply a roadmap for its incremental development and improvement.
Factor 9	**Self-assessment**	Relying on external parties for the DIME of mobile security environment may not adequately support continuous improvement of capabilities and timely detection of events. Organizations should develop in-house capabilities to achieve higher levels of payment data protection maturity across the mobile landscape.

When mobile device fraud leads to a payment security breach

By the U.S. Secret Service Global Investigative Operations Center

Maintain an information security policy

The U.S. Secret Service (USSS), along with our local, state and federal partners, are committed to aggressively investigating subscriber identification module (SIM) swapping fraud and educating the general public on this rising trend in criminal activity. "SIM swapping" is a type of account takeover or identity theft technique that generally exploits a cybersecurity weakness in multi-factor and two-step verification with the use of mobile phone numbers.

Phase one of a SIM swap involves the criminal first trying to obtain personal and public information about the person they are targeting. This step is typically completed by a person completely separate from the person committing SIM swapping activity, who will research to identify individuals on various chat forms or social media platforms that they believe are worth targeting. The USSS has noticed a growing trend of cryptocurrency users being targeted as victims on these various platforms, due to their public display of their cryptocurrency wealth. When a target is chosen, the criminal will usually attempt to gain access to private information through various tactics, such as email phishing. Once the necessary information is accessed and taken, they will then sell or give it to the fraudster looking to commit the SIM swap.

SIM swapping reveals weakness in multi-factor authentication

This tactic allows the fraudsters to gain control of a victim's mobile phone number, permitting phone calls and SMS messages to be routed to devices controlled by the criminal. The individual then uses their control to reset passwords on online accounts or request multi-factor authentication codes that allow them to bypass security measures. This is often facilitated by an insider or bribed employee within a service-provider company in order to have the SIM card switched. This continued control is further used as a gateway to gain access to online accounts, such as a victim's email, cloud storage and cryptocurrency exchange accounts.

The USSS continues to work closely with the Regional Enforcement Allied Computer Team (REACT) Task Force in Santa Clara County, Calif., to investigate high-technology crime across multiple jurisdictions. The REACT Task Force is one of the premier investigative groups focused on SIM swapping cases. In recent highlights, REACT arrested 20-year-old Joel Ortiz on July 12, 2018, after he stole $5 million in cryptocurrency from 40 victims through SIM swapping. A Santa Clara County resident originally contacted REACT after AT&T notified him that, in February 2018, an impersonator transferred his account to another SIM and reset some of his email passwords. In March 2018, the victim noticed his social media and cryptocurrency accounts were accessed, and about $10,000 worth of bitcoin was stolen. The hacker later called the victim's wife and sent text messages to his daughter including the message, "TELL YOUR DAD TO GIVE US BITCOIN."

REACT immediately obtained search warrants to identify the hacker's SIM and smartphones used to access the accounts, and discovered Ortiz's email address was used on one of the hacker phones. The emails contained a photo of Ortiz holding his ID, which led to warrants that uncovered cryptocurrency accounts linked to Ortiz and his criminal activity. Ortiz was arrested, pled guilty and is now serving a 10-year sentence.

Appendix C:

Breach Simulation Kits to test your IR Plan

By John Grim, VTRAC | Research, Development, Innovation

PCI DSS Control 12.10.2 requires annual testing of an assessed entity's IR Plan. The information provided below by the VTRAC | Investigative Response Team can serve as a model. These scenarios, together with the countermeasure worksheet and solutions, form Breach Simulation Kits (BSKs). BSKs can facilitate data breach simulation workshops involving internal IR stakeholders and tactical responders, as well as external entities.

Conducting a BSK workshop session is a five-step process.

Step 1 – Getting started

To facilitate a BSK workshop, you'll need:

- A suitable facility – a "war room" or conference room free of noise and other distractions
- A whiteboard or butcher-block paper and markers
- Printouts of scenarios and countermeasure worksheets (and highlighters) for each participant

A typical BSK workshop session consists of 1 to 2 scenarios and can last for 1 to 2 hours, depending on participant knowledge levels and experience.

Step 2 – The scenario

Begin the workshop by distributing printouts of the scenario (including situation, response and lessons learned) to participants (optional: distribute the countermeasure worksheet).

Give participants 10 to 15 minutes to read the scenario, highlight and take notes. Allow participants to talk and discuss among themselves.

Step 3 – Countermeasure worksheet

After participants read the scenarios, facilitate a discussion by selecting a participant to walk through the situation, response and lessons learned. Discuss key observations on countermeasure. Take notes on the whiteboard or butcher-block paper (or use the countermeasure worksheet) by progressing through the six phases of incident response (include prevention and mitigation countermeasures).

Give the participants 15 to 20 minutes to discuss, and be sure everyone has an opportunity to speak.

Step 4 – Countermeasure solutions

Distribute countermeasure solutions (answers). Continue facilitating the discussion by comparing participant solutions to countermeasure solutions. Do they differ? Did the participants come up with more actionable items than those provided in the countermeasure solutions?

Give the participants 10 to 15 minutes to discuss.

Step 5 – Lessons learned

Complete the session by conducting a lessons-learned discussion, noting participant feedback (e.g., what went well, what went less smoothly and what can be improved on in the next session). Assemble feedback and countermeasure solutions in an action plan to update the IR Plan, determine additional IR resource requirements, and identify internal IR stakeholder and tactical responder training needs.

Give participants 10 to 15 minutes to discuss.

Countermeasure worksheet

Workshop participants can enter their discussion notes on breach countermeasures here.

Phase	Countermeasure
1. Planning and preparation	
2. Detection and validation	
3. Containment and eradication	
4. Collection and analysis	
5. Remediation and recovery	
6. Assessment and adjustment	
0. Mitigation and prevention	

Figure 78. Breach simulation countermeasure worksheet

Scenario #1

PoS Intrusion—The Faux PoS

The situation

Reliance on third parties has increased significantly. The practice not only benefits the business financially, but also provides an opportunity for any organization to focus on its core business strengths while letting expert third parties handle selective domains.

As the Business Unit Leader for a large brick and mortar merchant in the APAC region, that was my expectation. I had worked with a third-party vendor, utilizing their point-to-point encryption (P2PE) solution to establish a more secure transaction flow between our point-of-sale (PoS) systems and our acquiring banks.

Figure 79. Payment card transaction flow

All was fine until our acquiring banks informed us of a suspected PCI data breach. Fraudulent transactions worth millions of dollars had occurred in various parts of the world.

The common point-of-purchase (CPP) analysis from the payment card brands had identified us as the likely source of the stolen payment card data. This reported data breach wasn't limited to a store or even a region, but was spread throughout our global store network.

I kept asking myself, "What could have gone wrong?" "Where had we been breached?" "Was it in our corporate network?" "Was it at our stores?" "Or perhaps it was one of our service providers?"

Notes

PoS Intrusion—The Faux PoS (continued)

Investigative response

We quickly established a "war room" and core team coordinating internal meetings and sessions with the acquiring banks and payment card providers. In parallel, we engaged the VTRAC | Investigative Response Team as the PFI for the PCI investigation.

The VTRAC | Investigative Response Team PFIs meticulously combed through the incident background information, payment transaction flow, CPP analysis data from payment card brands, our IT environment details, and our third-party access.

This was followed up with a game plan to collect and analyze the PoS servers and terminals at the CPP-identified stores, along with the in-scope business units and approximately a dozen third-party servers.

Unfortunately, valuable forensic artifacts were lost due to the actions of the vendor. It had restarted systems, executed antivirus scans, deleted existing local system accounts, changed passwords, deleted various logs and changed the systems. This had all been conducted without our approval and just prior to the evidence collection.

The VTRAC | Investigative Response Team PFIs soon identified a litany of issues. These included unrestricted ingress from the internet to the PoS servers, single-factor authenticated logons from unknown external IP addresses using a remote desktop protocol (RDP), a backdoor Trojan virus, RAM scraper and network sniffer software on the systems. They also found over 100,000 transaction log entries with primary account numbers (PANs) and full Track 1 and Track 2 information in clear text on the third-party server.

Based on the forensic analysis of the available evidence sources, coupled with an understanding of the payment card data transaction flow and the CPP analysis, it was confirmed that a data breach had occurred.

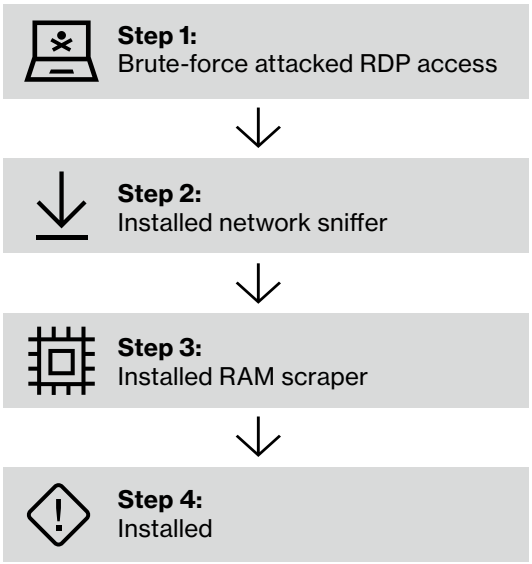


Figure 80. Third-party server attack stream

Notes

PoS Intrusion—The Faux PoS (continued)

This breach occurred first through a brute-force attack on RDP access, followed by installing a network sniffer, a RAM scraper and finally a remote-access Trojan (RAT) on the third-party payment card data processing server.

Now that the investigation was complete, I prioritized the remediation, recovery, prevention and mitigation actions.

The affected systems were cleaned and rebuilt, RDP access was restricted using source address-based filtering, and multi-factor authentication (MFA) was required for all remote login connections.

A thorough review of the security controls of the third-party service provider brought up gaping holes, not only from the PCI DSS perspective but also from basic hygiene security controls that ideally should be implemented for any secure enterprise.

We immediately initiated a process for regular, independent PCI DSS compliance assessments of our third-party service providers. We can't blindly rely on our service providers to always be doing the right thing.

Lessons learned

For us, the investigation highlighted several procedural and technical issues that led to this incident. Further, the investigation was very complex and arduous due to the unavailability of some crucial digital evidence. Among their findings, the VTRAC | Investigative Response Team PFIs made these recommendations.

Countermeasure solutions

Detection and response

- Proactively discover undetected code modifications by regularly performing integrity checks on sensitive code; implement tools to track and monitor website changes; implement a change control process for modifications
- Help detect unusual elevated account activity by periodically reviewing logs of accounts accessing critical and sensitive systems
- Implement a file integrity monitoring (FIM) solution

Mitigation and prevention

- Regularly review and update firewall configurations and access control lists (ACLs)
- Assess the complete payment process (not just the P2PE solution); implement further controls with a defense-in-depth approach
- Implement system-based controls to help prevent unauthorized access; make it a policy and practice to use admin accounts (with MFA) only when needed

Notes

Scenario #2

An E-Commerce Breach—The Flutterby Effect

The situation

The call center was receiving a high call volume from online customers having issues paying for products. Specifically, there appeared to be a consistent issue with "frozen pages" when attempting to submit payment on our checkout webpage. As the Incident Commander for an online retailer, I was alerted immediately as this could have a potentially negative impact on our online sales.

This issue couldn't have come at a worse time. Due to the holiday season, our IT staff wasn't permitted to change the web application or the production environment.

My initial thoughts were this issue was likely related to some bug within our P2PE setup as it dealt with payment card data at the point of checkout. Payment card data was encrypted prior to being received by our systems, which relaxed any concerns of potential payment card-related fraud.

As a first step, we tested the checkout process within our nonproduction development environment. After repeated attempts, we observed no issues with the checkout process; the data inputs and outputs looked normal.

This was perplexing, as our development checkout process should've been a perfect replica of our production instance. There were no changes logged in our change management platform and no employees had changed the production platform in several weeks.

We then focused on the production environment, attempted the checkout process "live" and received the frozen page. We hash-checked the development pages associated with checkout process against those pages in production. If something was different between development and production, a hash check would reveal an affected page. Sure enough, the hash differed in the checkout webpage and contained a JavaScript code involved in the processing of payment cards.

A quick comparison revealed five lines of code had been inserted into the production page. A preliminary review of the code suggested that it used a simple regex string to look for payment card data strings and sent it to an external domain.

Investigative response

Prior to this discovery, our CISO had notified the VTRAC | Investigative Response Team. Their investigation revealed an attacker had gained access to our payment processing application.

After gaining access, the attacker modified the payment processing code on the application. During the checkout process, this JavaScript code then redirected the payment card data via the web browser to a remote internet domain. So, although we were using P2PE, the solution was irrelevant for these attacks as the theft occurred before the data ever made it to our systems or the payment processor.

Notes

An E-Commerce Breach—The Flutterby Effect (continued)

However, the malicious code failed to execute cleanly, causing the Internet Explorer browser to hang. We cleaned up the malicious sections of code and implemented stronger access controls for future code updates.

Lessons learned

One thing we realized from the start of this incident was that policy-based restrictions don't prevent unauthorized users from breaking them. We had written policies restricting personnel from modifying the production environment. However, there was no actual system or logical restrictions preventing access and later changes to critical and sensitive systems.

We were lucky to catch this early on. Given this attack occurred during our busy season, this could have hurt a large part of our customer base. With this in mind, when the dust settled, we compiled a list of actions to undertake as part of our After-Action Review (AAR).

Countermeasure solutions

Detection and response

- Proactively discover undetected code modifications by regularly performing integrity checks on sensitive code; implement tools to track and monitor website changes; implement a change control process for modifications
- Help detect unusual elevated account activity by periodically reviewing logs of accounts accessing critical and sensitive systems
- Implement a File Integrity Monitoring (FIM) solution

Mitigation and prevention

- Regularly review and update firewall configurations and Access Control Lists (ACLs)
- Assess the complete payment process (not just the P2PE solution); implement further controls with a defense-in-depth approach
- Implement system-based controls to help prevent unauthorized access; make it a policy and practice to use admin accounts (with MFA) only when needed

Notes

Appendix D

PCI DSS compliance calendar

By Dyana Pearson, Senior Consultant, Verizon PCI Security Practice

PCI req	PCI sub-req	Activity	BAU	Daily	Weekly	Quarterly	Bi-annually	Annually	After changes	Prioritized approach milestone	N/A
ES	**ES**	Perform PCI DSS assessment scoping confirmation activities.						•			
1	1.1.7	Perform router and firewall rule set reviews with documented evidence of results every six months.					•				6
2	2.x	Maintain updated configuration standards (supported versions of operating systems, devices, and applications).	•								3
2	2.4	Maintain an inventory of system components that are in scope for PCI DSS.	•								2
3	3.1	Ensure that stored CHD does not exceed defined retention policies and validate secure deletion purge processes.				•					1
3	3.5.1	Service providers only: Maintain a documented description of the cryptographic architecture.	•								5
PCI req	**PCI sub-req**	**Activity**									
3	3.6	Retire or replace keys as necessary, in alignment with documented key management procedures.	•								5
4	4.x	Monitor transmission encryption protocol configurations and mechanisms.	•								2
5	5.2	Monitor antivirus configuration and performance.	•								2
6	6.1	Use reputable external security resources to identify new security vulnerabilities and assign a risk rating.	•								3
6	6.2	Ensure that all system components and software are protected from known vulnerabilities, by installing vendor-supplied patches. Install critical security patches within a month of release.	•								3
6	6.4.6	Upon completion of a significant change, implement all relevant PCI DSS requirements on all new or changed systems and networks, and update documentation.								•	6
6	6.5	Train developers at least annually in up-to-date, secure coding techniques, including how to avoid common coding vulnerabilities.						•			3
6	6.6	If not using a web application firewall, review public-facing web applications, at least annually, and after any changes.						•		•	3
8	8.1.3	Immediately revoke access for any terminated users.	•								2
8	8.1.4	Remove or disable inactive user accounts within 90 days.				•					2
8	8.2.4	Change user passwords and passphrases at least once every 90 days.				•					2

Appendix D (continued)

PCI DSS compliance calendar

PCI req	PCI sub-req	Activity	BAU	Daily	Weekly	Quarterly	Bi-annually	Annually	After changes	Prioritized approach milestone
8	8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.								2
9	9.5.1	Store media backups in a secure location—preferably an off-site facility—such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.						•		5
9	9.7.1	Properly maintain inventory logs of all media, and conduct media inventories at least annually.						•		5
9	9.9.1	Maintain an up-to-date list of devices. The list should include the make, model, location, serial number or other unique identifier of device.								2
9	9.9.2	Periodically inspect card readers to detect tampering.								2
9	10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.		•						4
10	10.6.1	Review logs and security events of all CDE components.		•						4
10	10.6.2	Review logs of all other system components periodically, based on the organization's policies and risk management strategy.								4
10	10.8	Detect and report on failures within critical security control systems.			•					4
11	11.1	Test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.								4
11	11.1.1	Maintain inventory of authorized wireless access points.				•				4
11	11.2.1	Perform quarterly internal vulnerability scans.				•				2
11	11.2.2	Perform quarterly external vulnerability scans.				•				2
11	11.2.3	Perform internal and external scans and rescan as needed, after any significant change.							•	2
11	11.3	Review and consider threats and vulnerabilities experienced in the past 12 months.						•		2
11	11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification.							•	2
11	11.3.2	Conduct scans of the internal and external networks after any significant change.							•	2

Appendix D (continued)

PCI DSS compliance calendar

PCI req	PCI sub-req	Activity	BAU	Daily	Weekly	Quarterly	Bi-annually	Annually	After changes	Prioritized approach milestone
11	11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls and methods.								2
11	11.3.4.1	Service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls and methods.					•		•	2
11	11.5	Perform critical file comparisons at least weekly.			•					4
12	12.1.1	Review the security policy at least annually and update the policy when the environment changes.						•		6
12	12.2	Perform a formal, documented analysis of risk, at least annually.						•		1
12	12.3.9	Activate remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.								6
12	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.						•		6
12	12.6.1	Educate personnel upon hire and at least annually.						•		6
12	12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.						•		6
12	12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.						•		2
12	12.10.2	Review and test the incident response plan, at least annually.						•		2
12	12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	•							2
12	12.10.4	Provide appropriate training to staff with security breach response responsibilities.	•							2
12	12.11	Service providers only: Perform reviews at least quarterly to confirm that personnel are following security policies and operational procedures.				•				6
12	12.11.1	Service providers only: Maintain documentation of quarterly review process to include results of the reviews, and review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.				•				6

Appendix E:

CISO responsibilities

CISO

Leading change

Commercial & strategic focus
Collaboration & influencing
Driving innovation
Driving change

Managing finance

Budgeting
Business case

Managing the supply chain

Commercial negotiations
Supplier management

Core behaviors

Resilience
Flexibility & pragmatism
Focus on results
Initiative
Difficult decision making
Cultural awareness

Leading people

Inspiring leadership
Org design
Team management
Talent development
Driving behavioral change
Engaging comms

Building relationships

Stakeholder engagement
Stakeholder communications
Conflict management
Simplify the complex

Strategy, leadership and governance

Information security governance body

- Terms of reference
- Ensuring relevance of content
- Member engagement

Organization design

- Operating model
- Roles and responsibilities
- Org design
- Team cohesion
- Org change management
- Talent sourcing
- Talent development:
  - Cyber apprenticeships
  - Team development
  - Succession planning

Strategy and business alignment

- Maturity assessments and benchmarking
- Security strategy definition and articulation
- Security program:
  - Tactical quick wins
  - Long-term roadmap

Metrics and reporting

- Operational and executive metrics
- Key risk indicators
- Validation of metric effectiveness

Stakeholder relationships

- Executive board and non-executive directors
- Corporate strategy alignment
- Updates to leadership and staff
- Conflict management
- Innovation, value creation
- Expectations management
- Coordination with others: CSO, CRO, DPO, General Counsel

Finance

- Business case and ROI
- Alignment with wider portfolio
- Budgeting and tracking

Risk and controls

Risk management framework

- Control frameworks:
  - COSO/SOX
  - COBIT
  - ISO27000
  - NIST, FAIR, CIS
- Control assurance
  - Management risk, control reviews and reporting
  - Internal and external audit

Cyber risk insurance

- Broker and underwriter engagement
- Covered scenarios
- Limits and self-insured retentions
- Pre-breach risk and control maturity assessments
- Post-breach engagement

Risk assessment, treatment and acceptance

- Risk assessment plan
- Risk ownership and governance
- Risk articulation and management review
- Risk acceptance processes

Continuous improvement

- Security health checks:
  - Testing
  - Tech risk landscape
  - Remediation roadmaps
- Incident readiness assessments
- IT controls assessments
- Penetration tests
- Threat detection capability assessments
- Prioritized remediation planning

Legal and compliance

Compliance assurance

- External assurance: ISAE3402/ SSAE18/SOC1/SOC2
- Internal assurance:
  - Internal Management Review
  - Internal Audit

Externally-imposed compliance requirements

- NIST/FISMA/HIPAA/HITECH
- China CSL
- PCI
- Sarbanes Oxley
- Data protection regulations
- Government certifications:
  - Privacy shield
  - Cyber essentials +

E-discovery and legal hold

- Preparation of data repositories for e-discovery
- Enforcement of legal hold
- Internal compliance requirements

Security policies and standards

- Project NFRs
- Publication and awareness
- Supply chain compliance

Data retention and destruction

- Data retention policies
- Retention schedules
- Enforcement within business functions

Securing new initiatives

Integrating security and risk in SDLC/PMO

- Waterfall, Agile and DevOps

Design

- Secure coding training and review
- App development standards
- Security requirements and NFRs

Security testing and assurance

- Code reviews
- App vulnerability testing

CISO responsibilities (continued)

- Penetration tests
- Continuous assurance
- Certification and accreditation requirements

Securing the supply chain

Pre-contract due diligence
- Self-assessment
- Audits
- Independent assurance
- Contracts

New contracts
- Contract renewals
- Reviews and assurance

Self-assessment
- Audits:
  - Right to audit and remediation
- Independent assurance

Securing the business

On-boarding and termination
- Staff
- Business partners/clients
- Suppliers

Securing the customer and business initiatives
- Product/customer security
- Identification of new initiatives
- Engagement with new initiatives

Business continuity planning
- Security of BC plans
- Cyber attack scenario planning

Employee behavior
- Employee awareness/risk culture:
  - Awareness and training
  - Phishing simulation tests
- Investigations and forensics

Mergers and acquisitions
- Risk management: before, during and after acquisition
- Integration of acquired targets
  - Identity integration
  - Technology integration
  - Business culture integration

Security operations

SOC design – outsourced/ MSSP/co-sourced
- Knowledge transfer
- Resource commitments
- Metrics and KPIs
- Supplier management
- SOC design – in-house

Recruitment
- Development, retention and promotion
- Knowledge retention
- Team and shift management
- Continuous training

Vulnerability management
- Identification:
  - Scoping and asset discovery
  - Supplier liability and operational risk of scanning
- Remediation:
  - Approach to fixing vulnerabilities
  - Verification
  - Metrics and baselines

Threat management
- Alerting from security tools
- Log analysis, correlation, SIEM Netflow analysis
- Open source and commercial threat feeds
- Threat hunting: automated and manual
- DNS, social media and dark web

SOC operations
- SOC procedures and runbooks
- Metrics and KPI reporting
- SOC/NOC/Svc desk integration
- Partnerships with info sharing and analysis centers
- DR exercises

Security platform operations
- Platform lock-down, operations and monitoring
- Technology upgrades

Incident management
- Participation of all stakeholders:
- Executive board
- IT, HR, legal, comms/marketing/ media relations
- Clients/customers, suppliers
- Incident process
- Runbooks for critical incident types: ransomware and customer-facing breaches
- Incident testing
- Crisis plan: cyber-attack scenario
- Security orchestration/SOAR
- Managed detection and response/MDR
- Integration with related plans
- Crisis plan
- Personal data breach plan
- Business continuity plan
- Forensics and 24x7 support

Securing the technology

Infrastructure and server OS security
- Service continuity and disaster recovery
- Hardening
- Patching
- Anti-malware and APT protection
- Backups, replication, multiple sites
- HIPS
- Security monitoring

Application security
- Data access governance:
  - Information ownership and custodianship
  - Application access controls
  - Role-based access controls
- Security monitoring
- File integrity monitoring

Identity and access
- Credential and password management:
  - Password strength/complexity
  - Password self-service resets
  - Multi-factor authentication
- Starters, movers, leavers:
  - Account creation and approvals
  - Account reviews
  - Account removal
  - HR process integration
- Single sign-on
- IAM SaaS solutions
- IAM data analytics
- Identity repository and federation
- Mobile app access control
- IOT device identities

Network security
- DDoS protection
- Firewalls, IDS, IPS
- Secure remote access
- Proxy/content filtering
- Secure wireless networks
- Network function virtualization and SD-WAN

BYOD security
- Policy considerations
- Commercial opportunities
- Personal data privacy
- HR, financial and tax
- Data security
- Policy enforcement

Innovation – exploiting emerging tech
- AI, ML and robotics
- Crypto currencies
- Blockchain
- 5G
- Drones
- VR and AR
- Wearables
- Autonomous vehicles

Physical security
- Landlord services
- Physical access control and monitoring
- Intrusion detection and response
- Theft prevention
- Environmental controls/power and HVAC
- Fire detection and suppression
- Redundancy
- BCP/work area recovery sites

Cloud security
- SaaS strategy:
  - Governance and compliance enforcement
  - Cloud specific DR and BCP
  - Supplier risks
  - SLAs and performance management
  - Data ownership, liability, incidents, privacy compliance
  - Security assurance
  - Management of shadow IT
- Cloud security controls:
  - Cloud security architecture
  - Cloud identity/CASB
  - Virtual machine security
  - Virtualised security appliances/ cloud-to-cloud integration
  - Monitoring/log integration
- Access to corp data from non-corp devices

Email security
- Anti-spam control
- Phishing and impersonation protections
- Email encryption

Endpoint security
- Hardening
- Patching/software updates
- Anti-malware
- HIPS/EDR
- Security monitoring/UBA
- Encryption
- PIN/password enforcement
- Apps inventory and deployment control
- Containerization/data segregation
- Lost/stolen devices
- Cloud storage of data
- Device tracking

Data security
- Data and process mapping
- Data analytics security
- Encryption and masking:
  - PKI
  - Encryption at rest
  - Encryption in transit
- Business partner access:
  - Access approval
  - Access reviews
  - Access removal
  - Identity federation and access automation
- Data loss prevention:
  - DLP and data classification policy
  - Data loss channels
  - DLP enforcement technologies

IoT/operational technology security
- IoT risks:
  - Connected office devices
  - Connected medical devices
  - At home
  - Planes, trains and automobiles
  - Industrial control systems, SCADA, PLCs, HMIs
- IoT Security:
  - IoT Frameworks
  - Vulnerability management
  - Comms protocols
  - Device authentication and integrity
  - Network segregation
  - Device protection
  - Over The Air updates

Figure 81: "The CISO Role," what the CISO does for a living, adapted from an infographic by Louis Botha. Based on http://rafeeqrehman.com

Appendix F:

Terminology

Cybersecurity	Protection of digital data and information systems against electronic attacks. The measures taken to protect information systems that store, process or transmit electronic data against the unauthorized access, use, disclosure or harm. Cybersecurity is limited to the protection of electronic and digital data and information only, and excludes protection of physical data.
Information security	The ongoing process of exercising due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, disruption or distribution. It includes the design, implementation and evaluation of countermeasures that provide confidentiality, integrity and availability to counter, prevent, detect and document threats to digital and non-digital information assets.
Information assurance	The overarching approach for identifying, understanding, evaluating and managing risks through an organization's use of information and information systems. It is concerned with the lifecycle of information through the objectives of maintaining the following attributes: confidentiality, integrity, availability, non-repudiation, authentication, possession and utility. Information assurance is the practice of assuring information and managing risks related to the use, processing, storage and transmission of information or data and the systems and processes used for those purposes.
Privacy	The ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. It is the requirement to maintain control over one's personal information to determine when, how and to what extent information is communicated to others. Privacy concerns exist wherever uniquely identifiable data relating to a person are collected and stored, in digital form or otherwise, how data are collected, stored, and associated, and who is given access to information. Other issues include whether an individual has any ownership rights to data about them and/or the right to view, verify, challenge and correct that information.
Data protection	The act of protecting the possession, confidentiality, integrity and authorization of personal and corporate data, where controls are implemented to ensure consent and choice, collection limitation, data minimization, use, retention, limitation of disclosure, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, purpose legitimacy, and information security. Data protection focuses on the protection of sensitive personal and corporate data that is collected, accessed, updated, stored and disposed of by people and information systems. It includes, inter alia, names, contact information such as physical addresses, phone numbers and email addresses, medical history, banking details, credit ratings, employment records, and religious and political opinions. Therefore, data protection goes well beyond information security. It is a more comprehensive term that is inclusive of all data elements and selective security measures. It is usually covered by various data protection laws applicable to a specific region, such as the European Union's General Data Protection Regulation (GDPR). Data protection, although mostly focusing on personal data, can also be extended to include the protection of sensitive corporate data that, when compromised, can harm a corporate entity.
Security event	Anything that happens that could potentially have information assurance implications. A security event can be any event such as access, use, disclosure, disruption, modification or destruction of data, information or information systems and other actions that can impact information assurance with the potential to compromise the confidentiality, possession, control, integrity, authenticity, availability and utility of information systems or data. For example, a security event can be a system crash, packet floods, unauthorized use of system privileges, etc.
Security incident	Any observable occurrence in a system or network that violates an organization's security or privacy policies, or compromises the integrity, confidentiality, availability, possession or utility of an information asset. For example, a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, modification or destruction of data of a system component.

Terminology (continued)

Security breach	An act from outside an organization that bypasses or contravenes security policies, practices or procedures. A similar internal act is called security violation. A security breach can be any confirmed security incident that involves access, use, disclosure, disruption, modification or destruction of restricted information systems. A security breach differs from a data breach.
Data breach	When the security or privacy of data that should be protected is compromised due to the unauthorized acquisition, access, use, or disclosure of protected data, or its accidental or unlawful destruction, loss or alteration. It includes all security incidents where sensitive, protected or confidential data was confirmed to be copied, transmitted, viewed, stolen, used or altered by a system or individual not unauthorized to do so. A data breach is an incident that results in the confirmed compromise—not just potential exposure—of data to an unauthorized party, as a result of accidental or unlawful breaches of security. It is a violation, transgression, infringement, gap, or breakthrough of restrictions and trust placed on the data and/or the information systems that store, process or transmit the data.
Data compromise	See Data breach—The terms data compromise and data breach can be used interchangeably. Data compromise refers to the exposure of data to elements that violates the restriction placed on data to ensure the trust in its confidentiality, availability, integrity, use, possession, control, authenticity and utility.
Sustainability	A security control and a control environment can be considered sustainable when an organization demonstrates the capacity, capability, competence, commitment and communication needed to consistently maintain the required level of configuration, functionality and performance of security controls to meet control design specifications and data protection objectives over extended periods of time. The level of sustainability can be measured by monitoring the amount of deviations from the established standard of control operation and performance, and tracking the amount of effort and resources (cost, people and time) required to maintain the required status (i.e., performance and effectiveness) of data protection operations. (See Control robustness and Control resilience.)[48]

48 Verizon 2018 Payment Security Report, "Control robustness" and "Control resilience," pages 14–17

Appendix G:

Suggested reading

This suggested reading list (more than 45 books in total) is a gold mine of information for security professionals tasked with managing data protection compliance programs. One of the best ways to develop proficiency in data protection compliance management is to absorb the wealth of information that has accumulated from the experts over the past two decades.

The particular focus of this list is on guidance for CISOs in program management, security principles, risk management and developing mature control environments. Without well-educated and inspired management leadership, a compliance program will likely lag or be inadequate. CISOs need to brush up regularly on guidance from the best and brightest.

This list is merely a starting point and is by no means complete. Some books are 20 years old and may appear out of date, but we believe they still have value. Their content remains insightful and offers an understanding of how a subject has evolved during the past two decades.

Book categories:

- CISO guidance
- Security controls and frameworks
- General security principles and management
- Program management
- Risk assessment and management
- Security measurement and metrics
- Security maturity development

CISO guidance

Year	Title	Author	Publisher	Pages	ISBN
2003	The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program	Gerald Kovacich	Butterworth-Heinemann	361	9780750676564
2005	The CISO Handbook: A Practical Guide to Securing Your Company 1st Edition	Michael Gentile, Ron Collette, Thomas D. August	Auerbach	352	9780849319525
2005	Data Protection and Information Lifecycle Management	Tom Petrocelli	Prentice Hall	288	9780131927575
2013	CISO and Now What?	Michael Oberlaender	Createspace	102	9781480237414
2013	Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework	Robert Moeller	Wiley	304	9781118626412
2015	Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats	Scott Donaldson, Stanley Siegel, Chris Williams, Abdu Aslam	Apress	586	9781430260820
2016	CISO Desk Reference Guide: A Practical Guide for CISOs	Bill Bonney, Gary Hayslip, Matt Stamper	CISODRG	366	9780997744118

Suggested reading (continued)

Security controls and frameworks

Year	Title	Author	Publisher	Pages	ISBN
2008	IT Compliance and Controls: Best Practices for Implementation	James J. DeLuccia	Wiley	274	9780470145012
2015	Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework	Lynford Graham	Wiley	416	9781118996218
2016	Security Controls Evaluation, Testing, and Assessment Handbook	Leighton Johnson	Syngress	678	9780128023242

General security principles and management

Year	Title	Author	Publisher	Pages	ISBN
2003	Principles and Practice of Information Security	Linda Volonino and Stephen Robinson	Pearson	256	9780131840270
2004	A Practical Guide to Managing Information Security	Steve Purser	Artech House	259	9781580537025
2004	Executive Guide to Information Security: Threats, Challenges, and Solutions	Mark Egan, Tim Mather	Addison-Wesley	288	9780321304513
2009	Beautiful Security: Leading Security Experts Explain How They Think	Andy Oram, John Viega	O'Reilly Media	304	9780596527488
2016	Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour	Leron Zinatullin	IT Governance Ltd	128	9781849287890
2017	Principles of Information Security 6th Edition	Michael E. Whitman, Herbert J. Mattord	Cengage Learning	656	9781337102063
2018	Management of Information Security 6th Edition	Michael E. Whitman, Herbert J. Mattord	Course Technology	672	9781337405713

Suggested reading (continued)

Program management

Year	Title	Author	Publisher	Pages	ISBN
2005	Data Protection and Information Lifecycle Management	Tom Petrocelli	Prentice Hall	288	9780131927575
2008	Fundamentals of Effective Program Management: A Process Approach Based on the Global Standard	Paul Sanghera	J. Ross Publishing	344	9781932159691
2013	Implementing Program Management: Templates and Forms Aligned with the Standard for Program Management and Other Best Practices 3rd Edition	Ginger Levin, Allen R. Green	Auerbach	328	9781466597716
2014	The Handbook of Program Management: How to Facilitate Project Success with Optimal Program Management	James T. Brown	McGraw-Hill Education	304	9780071837859
2017	The Standard for Program Management Fourth edition	Project Management Institute	Project Management Institute	176	9781628251968
2018	Program Management: A Practical Guide	Sorin Dumitrascu	Independent	621	9781976928581

Risk assessment and management

Year	Title	Author	Publisher	Pages	ISBN
1999	Risk Management for Security Professionals	Carl A. Roper	Butterworth-Heinemann	304	9780750671132
2001	Information Security Risk Analysis	Thomas R. Peltier	Auerbach	281	9780849308802
2002	Managing Information Security Risks: The OCTAVE	Christopher Alberts & Audrey Dorofee	Addison-Wesley	512	9780321118868
2005	Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments	Douglas Landoll	Auerbach	473	9780849329982
2006	A Practical Guide to Security Assessments	Sudhanshu Kairab	Auerbach	498	9780849317064
2009	The Failure of Risk Management: Why It's Broken and How to Fix It	Douglas W. Hubbard	Wiley	281	9780470387955
2011	Security Risk Management: Building an Information Security Risk Management Program from the Ground Up	Evan Wheeler	Syngress	340	9781597496155
2012	Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis	Mark Talabis & Jason Martin	Syngress	258	9781597497350
2014	Measuring and Managing Information Risk: A Fair Approach	Jack Freund & Jack Jones	Butterworth-Heinemann	408	9780124202313
2016	IT Security Risk Control Management: An Audit Preparation Plan	Raymond Pompon	Apress	311	9781484221396

Suggested reading (continued)

Security measurement and metrics

Year	Title	Author	Publisher	Pages	ISBN
2005	The Chief Information Security Officer's Toolkit: Security Program Metrics	Fred Cohen	Fred Cohen & Associates	228	9781878109354
2007	Security Metrics: Replacing Fear, Uncertainty, and Doubt	Andrew Jaquith	Addison-Wesley	336	9780321349989
2007	How to Measure Anything: Finding the Value of "Intangibles" in Business	Douglas Hubbard	John Wiley	287	9780470110126
2007	Complete Guide to Security and Privacy Metrics – Measuring regulatory compliance, operational resilience, and ROI	Debra S. Herrmann	Auerbach	824	9780849354021
2009	Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement	W. Krag Brotby	CRC Press	223	9781420052855
2011	Security Metrics, a Beginner's Guide	Caroline Wong	McGraw-Hill	397	9780071744003
2013	Pragmatic Information Security Metrics	W. Krag Brotby & Gary Hinson	Auerbach	512	9781439881521
2014	Measures and Metrics in Corporate Security	George Campbell	Elsevier	145	9780128006887
2015	Measuring and Communicating Security's Value: A Compendium of Metrics for Enterprise Protection	George Campbell	Elsevier	226	9780128028414
2016	How to Measure Anything in Cybersecurity Risk	Douglas Hubbard, & Richard Seiersen	Wiley	304	9781119085294

Security maturity development

Year	Title	Author	Publisher	Pages	ISBN
2008	CMMI Distilled: A Practical Introduction to Integrated Process Improvement 3rd Edition	Dennis M. Ahern, Aaron Clouse, Richard Turner	Addison-Wesley Professional	288	978-0321461087
2010	CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience 1st Edition	Richard A. Caralli	Addison-Wesley Professional	1056	978-0321712431
2011	CMMI for Development: Guidelines for Process Integration and Product Improvement (SEI Series in Software Engineering) 3rd Edition	Mary Beth Chrissis, Mike Konrad, Sandra Shrum	Addison-Wesley Professional	688	978-0321711502
2011	Open Information Security Management Maturity Model (O-Ism3)	Editor	Van Haren Publishing	152	978-9087536657
2016	Risk Maturity Models: How to Assess Risk Management Effectiveness	Domenic Antonucci	Kogan Page	320	978-0749477585
2018	Capability Maturity Model: A Clear and Concise Reference	Gerardus Blokdyk	5STARCooks	124	978-0655175063

Verizon professional security services

Payment card industry (PCI)

Threat and vulnerability (T&V)

Cyber risk program (CRP)

Governance, risk and compliance (GRC)

Product and solutions testing and certification (ICSA Labs)

Payment card industry (PCI) and payment security

- PCI DSS Assessments
- PCI DSS Readiness Assessments
- PCI Consulting Services
- PCI Payment Application Data Security Standard (PA-DSS)
- PCI Point-to-Point Encryption (P2PE & PA-P2PE)
- PCI PIN Transaction Security (PIN)
- PCI 3-D Secure (3DS)
- EI3PA
- SWIFT Customer Security Program (CSP)
- EU PSD2 & SecuRePay

Threat and vulnerability (T&V)

To bolster your security, you need to understand where your weakest points lie. Our team can help you to prioritize your defenses.

- Application/Network Vulnerability Assessment
- Penetration Testing
- Secure Source Code Review
- Wireless Vulnerability Assessment
- Data Discovery
- Development and Penetration Testing Training

Cyber risk programs (CRP)

Managing compliance and risk is challenging in today's connected world and regulatory environment. Although you may not be able to plan for every possibility, you can use historical trends and continual analysis as a guide to help you improve your security posture.

- Security Management Program (SMP)
- Cyber Risk Programs (CRP)
- Verizon Risk Report (VRR) Level 3: Culture & Process
- Application Security Certification Program (AppCert)

Governance, risk and compliance (GRC)

Our GRC team will guide you through assessments, programs and advisory services that can strengthen your security.

- Business Security Assessment – BSA (NIST CSF, ISO 2700X, GDPR)
- Healthcare Security (HIPAA, HITRUST)
- Fed/Gov (FedRAMP, FISMA)
- OTACS (SCADA, ICS, IoT)
- Risk Assessment
- Security Architecture Review (SAR) Assessments

Product and solutions testing and certification (ICSA Labs)

You want to assure customers that your security products and services will help keep their organization running smoothly. Verizon's ICSA Labs can help.

- Device security certifications: Anti-Malware, IPSec, Network (firewall, IPS...), SSL-TLS VPN, WAF, IoT
- Mobility and custom: IoT, mobile device, app
- Advance threat defense: Periodic testing
- Health IT testing, certification and maintenance

Verizon Threat Response Advisory Center (VTRAC)

VTRAC uses cyber intelligence to enable Verizon, its security services, and their customers to prevent, detect and respond to security incidents.

Our security assurance team has:

- Over 180 consultants in 30 countries
- Provided security consulting services since 1999
- Offered PCI compliance services since 2003
- Conducted over 16,800 assessments since 2009

Verizon 2019 Payment Security Report

Published November 12, 2019

Editorial team

Lead author
Ciske van Oosten

Co-authors
Anne Turner, Cynthia B. Hanson, Dyana Pearson, John Grim

Contributors
Abdelkrim Aoued Ahmed Bacha, Ashish Thapar, Clarence Hill, Eric Soper, Franklin Tallah, Gabriel Leperlier, John Galt, Michelle Wire, Neal Maguire, Rein van Koten, U.S. Secret Service Criminal Investigative Division, William Gooy

Data analysts
John Grim, Sundeep Paderu, Geena Richards, Noel Richards, Saravanan Thangam, Ron Tosto, Anne Turner

Security assurance practice

Managing director: Rodolphe Simonetti

PCI and Payment Security consulting practice
Global lead: Ron Tosto

PCI managers
APAC region: Sebastien Mazas
Americas region: Franklin Tallah
EMEA region: Gabriel Leperlier
Global intelligence: Ciske van Oosten

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 this 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.

Download the Payment Security Report at: https://enterprise.verizon.com/resources/reports/payment-security/

Verizon welcomes more organizations to participate and contribute to this research.

Team email: paymentsecurity@verizon.com

Contributing organizations:

ControlScan, Inc.

Foregenix, Ltd.

MegaplanIT, LLC

Schellman & Company, LLC

United States Secret Service

verizon business ready