PSR

Payment
Security
Report
2022

**Verizon
Cyber
Security
Consulting**

About the cover

Navigating the complexity of payment security is like steering a ship through unpredictable waters. It requires skill and strategic planning to negotiate changing currents, ebb and flow, unanticipated dangers, and the potential impact of evolving conditions. This navigation is about to take a new turn with the introduction of the Payment Card Industry Data Security Standard PCI DSS v4.0 with its customized approach and continuous compliance.

That's why the theme of the 2022 Payment Security Report (PSR) is preparing to successfully negotiate PCI DSS v4.0: how to determine the tools you'll need, identify and solve potential challenges, and choose the best path forward to determine and accomplish your goals.

Fittingly, our cover design is a circuit board with many interconnected channels. The white dotted line presents a course of unobstructed program progression within a well-organized security compliance management system.

The circuit board appears on a black background, which symbolizes absence of visibility, risk, the dark web and the vastness of our interconnected environments. To maintain an unobstructed course in such a deep abyss, security practitioners must plan for unexpected changes and unintended consequences. Today's data security planning and compliance requires choosing the right course, carefully mapping it and skillfully navigating around the obstacles.

Lateral movement—directed to a side—is relevant to a key metaphor in the report: one about a recent shipping fiasco in the Suez Canal. Lateral movement is also a method used by attackers in which a network is systematically infiltrated to access data and assets.

Even when traveling in a straight line through seemingly safe waters, one needs to prepare for unpredictable outcomes and side effects. Our metaphorical recounting of the container ship Ever Given's recent grounding and blockage of the Suez Canal (see page 11) highlights why chief information security officers (CISOs) and their teams need to apply a logical, coordinated process to evaluate requirements and constraints while navigating their ship into sound security and compliance waters.

No one engaged in PCI security should feel that their organization's approach to compliance is random—controlled by outside events, circumstances or other people. Numerous powerful solutions exist to help your organization take charge of its compliance program's destination. And that's exactly what we'll be exploring in this edition of the PSR. We'll introduce a toolbox of management methods, models and frameworks to help your organization negotiate the changing waters, whether you'll be traveling in a straight line or taking a less-predictable zigzagging course. This special set of management tools is designed to harness the combined capabilities within your organization and establish better management of your PCI security program by helping you plan, design, navigate, fix and maybe even rescue your security ship on its journey through unknown waters.

Table of contents

1

2

3

4

About this report:

Most security and compliance programs can do a lot better. Are you currently attaining your security and compliance goal? Do you know where to focus your efforts? What is keeping your strategy and program from progressing? What is keeping your control system from reaching its full potential? What exactly are the constraining factors? Everyone on your team has an opinion, but which is right? You can find the answers to these and more PCI security questions in this report, which distills a range of security and compliance subjects into valuable insights. We study various tools, tactics and methods applied by numerous organizations and explore why some companies accomplish more than others in their efforts to achieve sustainable and effective data security. We also distinguish between the approaches that separate busy security teams from productive ones and analyze the different ways decisions are made and how that can impact which strategies are formed and goals embraced.

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

Reader feedback:

Verizon's 2020 Payment Security Report—Focusing on strategy

"While PCI DSS forms the foundation of these reports and informs their content, the guidance is broadly applicable, and they could easily be rebranded as 'data security' reports. I hope everyone responsible for data security takes the opportunity to not only read this year's report but to also download the reports from prior years. Each report builds on the previous foundations, and the 2020 report provides an overall success strategy for CISOs and information security leaders.... The Verizon Payment Security Report remains one of the most valuable assets for developing and improving a data security environment. Whether providing key concepts such as the nine factors of control effectiveness, the five constraints, or this year's focus on strategy, the report is essential reading for security leaders. The 2020 report reads like a short textbook for a master's level college course for CISOs, and it is full of guidance for developing and improving security leadership."

— Anthony Israel-Davis, Tripwire[1]

"This report is a welcome wake-up call to organizations that strong leadership is required to address failures to adequately manage payment security. The Verizon Business report aligns well with Omdia's view that the alignment of security strategy with organizational strategy is essential for organizations to maintain compliance, in this case with PCI DSS v3.2.1 to provide appropriate levels of payment security. It makes clear that long-term data security and compliance combines the responsibilities of a number of roles, including the Chief Information Security Officer, the Chief Risk Officer, and Chief Compliance Officer, which Omdia concurs with."

— Maxine Holt, Senior Research Director, and Brian Curl, Omdia (previously known as Ovum)[2]

1   Anthony Israel-Davis, "Verizon's 2020 Payment Security Report: Focusing on Strategy," The State of Security Blog, Tripwire Inc., Jan 10, 2021, tripwire.com/state-of-security/regulatory-compliance/pci/verizon-payment-security-report-strategy/
    Reprinted by permission from Tripwire, Inc., ©2020-2021. Tripwire is a registered trademark of Tripwire, Inc.
2   Maxine Holt, "Only 1 in 4 Global Organizations Keep Cardholder Payment Data Secure," Omdia, Oct 6, 2020, https://www.verizon.com/about/news/cardholder-payment-data-secure

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

2014: Simplifying complexity
A review of the value of compliance, the impact of PCI DSS changes, the need for sustainability and how to improve scope reduction and compliance program management

2015: Achieving sustainability
A focused look at improving the sustainability of compliance, and a review of the state of scope reduction and payment security

2016: Developing proficiency
Developing data security 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 life-cycle 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 7 Constraints of Organizational Proficiency

2019: Evaluating program performance
Achieving high-performance security programs with sustainable and effective controls in a predictable manner, and addressing constraints that prevent continuous improvement of process and capability maturity

2020: The underlying reasons for low control effectiveness and sustainability
The value of a strategic approach to security compliance management, and how avoiding the Top 7 Strategic Data Security Management Traps contributes to reduced complexity and helps CISOs and their teams be more productive and successful
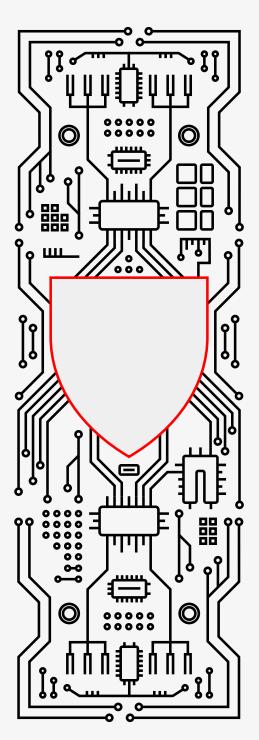
2022: A logical process for meeting PCI DSS v4.0 goals and requirements
How to navigate the changing requirements introduced by PCI DSS v4.0, with clear goals, a logical process and innovative models that eliminate core conflicts and constraints

Executive summary

For more than a decade, Verizon has documented compliance trends in the evolving payment security industry. The Payment Security Report (PSR) has tracked compliance ups and downs, while keeping a finger on the pulse of the changing payment security landscape. During this time, consumers and businesses substantially increased business activities conducted online. The COVID-19 pandemic escalated that trend and, as a result, the number of payment card transactions also increased. Meanwhile, the capabilities of threat actors continue to evolve and escalate, enabling the skillful exploitation of both existing and emerging threats and weaknesses within payment systems and processes. Additionally, digital transformations that rely heavily on cloud technologies are introducing new drivers that impact the payment security industry, further complicating the role of CISOs and other security managers and practitioners.

In response to these recent challenges, the PCI Security Standards Council (SSC) instituted a major rewrite of the PCI DSS v4.0. The latest update will help organizations ensure that data security controls remain relevant and effective in a shifting landscape. It's the most significant update to the PCI DSS since its initial release in 2004. If you feel overwhelmed by the amount of information you need to digest to understand the impact of PCI DSS v4.0 and want to simplify the complexity with the best-curated wisdom available, the 2022 PSR is essential reading.

The security management toolbox
A valuable set of models, methods and frameworks to simplify security compliance management:

The GRC²
The Security Management Canvas (TSMC)
  • Security business model (SBM)
  • Security strategy
  • Security operating model (SOM)
  • Security frameworks
  • The 9 Factors of Control Effectiveness and Sustainability
  • The 7 Constraints of Organizational Proficiency
  • The 4 Lines of Assurance
The Theory of Constraints and the Logical Thinking Process

An updated standard with higher expectations

Organizations worldwide should be gearing up to implement the changes required by PCI DSS v4.0. Planning and focusing attention of scarce resources on a set of design priorities for PCI DSS v4.0 is of utmost importance. If you don't design a bespoke program for your organization, you'll be violating one of the fundamental principles of security and compliance management that Verizon has promoted for over a decade: Success is achieved by design, not by luck.

It has been nearly 20 years since the introduction of the PCI security compliance regulation. That's plenty of time for every experienced CISO and management team to develop a security compliance management toolbox. Your tools should create structure and order and drive clear results. Not having a toolbox and merely taking a trial-and-error approach is a dangerous way to operate (design, implement and improve) a complex security and compliance program. CISOs attempting to manage programs without proper toolboxes are jocularly described as engaged in "six phases of a project":

1) enthusiasm, 2) disillusionment, 3) panic, 4) search for the guilty, 5) punishment of the innocent and 6) praise and honor for the nonparticipants.[3] With the correct approach—one that enables proper planning and execution—there's no reason for PCI DSS v4.0 projects to decline into panic. The design, implementation and management of PCI security strategy and program management is not an intractable problem.

Toward an efficient algorithm for achieving sustainable control effectiveness

A problem is tractable when a known, efficient algorithm solves it; it's intractable when an efficient algorithm for resolution is not known. Organizations fail to improve control environments and achieve the goal of sustainable control effectiveness for many reasons. We reviewed those reasons in the 2020 PSR's Top 7 Strategic Data Security Management Traps, (page 12).[4] The process of solving an intractable problem hinges on two primary elements: determining the critical root cause and determining the most effective next action. In this edition of the PSR, we review the tools needed to address those elements, while also avoiding the introduction of damaging unintended consequences.

"Most geniuses—especially those who lead others—prosper not by deconstructing intricate complexities but by exploiting unrecognized simplicities."[5]

—Andy Benoit

---

3 This list was used in computer science in the early 1970s and quickly spread to engineering and government projects. "Six Phases of a Big Project," Wikipedia, https://en.wikipedia.org/wiki/Six_phases_of_a_big_project

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

5 "Andy Benoit: Exploiting Unrecognized Simplicity," Farnam Street, 2016, https://fs.blog/2016/01/andy-benoit-unrecognized-simplicity/

What's in your management toolbox?

PCI security compliance is a business management discipline, not an information technology discipline. Organizations within the payment security industry need the knowledge and application of an appropriate set of management tools to deliver results within dynamic and complex environments: tools that support analysis, decision-making, coordination, alignment and control. The methods and techniques used to design and manage PCI security compliance goals, strategies and programs require careful consideration. There's no shortage of methods to choose from: management by objectives (MBO), total quality management (TQM), the observe-orient-decide-act (OODA) loop, business process management (BPM), Lean, Six Sigma, Drum Buffer Rope (DBR), balanced scorecard (BSC), management accounting, critical chain project management (CCPM), force field analysis (FFA), cost-benefit analysis (CBA), change management (CM), etc. Still, no silver bullet exists. And the more chaotic the environment, the less effective many management approaches become over time. With the additional changes afoot, how do you choose the best, most effective long-term methods?

This issue of the PSR focuses on goals. More specifically, it focuses on the importance of aiming for a clearly articulated security and compliance goal: how to formulate your goal and objectives, identify necessary requirements to meet them and remove constraints. Every decision, task and activity within your PCI security program should be aligned with a defined goal and its objectives.

"It is a simple thing to make things complex, but a complex task to make them simple."[6]

—Meyer's Law

The best path for your organization's journey

In his landmark book The 7 Habits of Highly Effective People,[7] Stephen Covey recommends starting "with the end in mind." If you don't know where you're going, then any path will do. Or, in the immortal words of Yogi Berra: "You've got to be very careful if you don't know where you're going, because you might not get there."[8] To find the best path, you need to define and refine your goals. Therefore, this issue of the PSR focuses on goals. More specifically, it focuses on the importance of aiming for a clearly articulated security and compliance goal: how to formulate your goal and objectives, identify necessary requirements to meet them and remove constraints. Every decision, task and activity within your PCI security program should be aligned with a defined goal and its objectives. This report hones in on a method for achieving the focus needed for your security team to do this while staying highly productive—not simply busy. This is why we're spotlighting the Logical Thinking Process (LTP) as an exceptionally valuable management tool that belongs in every CISO's and security professional's management toolbox.

6 Meyer's Law, https://www.just-one-liners.com/it-is-a-simple-task-to-make-things-complex-but-a-complex-task-to-make-them-simple/
7 Stephen R. Covey, "The 7 Habits of Highly Effective People: Restoring the Character Ethic," Simon and Schuster, 1989.
8 Barney Corkhill, "20 Great Quotes From … Baseball: Yogi Berra Special!!," Bleacher Report, https://bleacherreport.com/articles/58227-20-great-quotes-frombaseball-yogi berra-special

> "What's the use of running if you are not on the right road?"
>
> —German proverb

In the early 1990s, Eliyahu M. Goldratt conceived a multistage process for complex problem solving called the Logical Thinking Process (LTP). This structured process takes an undefined or ill-defined system problem and helps practitioners advance it to an effective, fully implemented solution. For over 20 years, the LTP has been one of the most effective, rigorous and comprehensive problem-solving methods. It defines clear, prioritized and achievable goals and offers visibility and structure; clarity and quality of communication; improved decision-making; and a solid foundation for continuous improvements.

The challenges organizations encounter with data security and compliance management have identifiable cause-and-effect relationships. Solutions can be applied at a process level, system level or both. While organizations experience different degrees of complexity with the systemic problem of protecting data 24/7, PCI DSS v4.0's customized approach—if implemented correctly—should move the needle forward in the direction of effective, sustainable control.

One of the major breakthroughs in understanding the complex world of organizations is the field of systems theory, which greatly influenced how we understand and change organizations. Systems thinking helps organizations examine and simplify complexity, recognize patterns and expand the range of choices for problem solving. A systems thinking application is ideal for data security and PCI security compliance challenges because they are important issues; the problems are chronic rather than one-time events; the problems are familiar with a known history; and organizations have unsuccessfully tried to solve the problems before.

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

Gall's Law: "A complex system that works is invariably found to have evolved from a simple system that worked. The inverse proposition also appears to be true: a complex system designed from scratch never works and cannot be made to work. You have to start over, beginning with a simple system."[9]

—John Gall, systems theorist

---

[9] John Gall, "The Systems Bible: The Beginner's Guide to Systems Large and Small: Being the Third Edition of Systemantics," General Systemantics Press, 2006.
Josh Kaufman, "What Is 'Gall's Law'?", Worldly Wisdom Ventures, 2005-2021, https://personalmba.com/galls-law/

The compliance landscape ....

Much has evolved in payment security since the PCI DDS was introduced nearly 20 years ago. The speed and scope of these changes created a tipping point within the security community, prompting the PCI Security Standards Council (SSC) to address the critical need for substantial improvements to the baseline Standard.

Central to that tipping point is the significant change in how we work: Many people work from home today, and securing home-based work computers is a growing challenge. More organizations are adopting cloud computing and the use of cloud native applications, and digital transformation is driving increased automation and interconnectedness. Meanwhile, cybersecurity threats are morphing and growing at a rapid pace, often stretching the limits of security programs. The threats organizations face are more cunning and evasive than they were even two years ago. Threat actors are breaking passwords once considered nearly uncrackable and even circumventing multifactor authentication (MFA). Ransomware is rampant; sophisticated phishing attacks are commonplace. The COVID-19 pandemic further complicated this complex mix, overwhelming CISOs and security experts already juggling mounting security alerts and scarce resources.

How are you and your organization preparing to meet these new requirements and improve the overall maturity of your control environment?

The pressure of these changes raises an obvious question: How are you and your organization preparing to meet these new requirements and improve the overall maturity of your control environment?

It's no secret that many organizations need to significantly update their data security, compliance strategy and overall security program. For organizations that lack resources, working harder on a strategy is not a viable option. The answer is, instead, to work smarter on the right tasks and activities. For starters, you need to clarify what you are aiming for to achieve the right goals in an evolving, increasingly interconnected security matrix.

For many years, Verizon has been exploring different methodologies and tools to help you accomplish the right security goals. Integrating the Logical Thinking Process into your security planning is the next essential step. This step-by-step systems approach to complex problem solving is based on the Theory of Constraints (TOC). Its application is easy to grasp, as it provides simple diagramming processes to identify the root cause of any undesirable effect in a control environment. As a valuable planning tool, it can even move a rusty needle to clarify goals and solve problems.

> If you want a significant change in results, then you probably need a significant change to your strategy, to your approach— how you pursue (design, execute and evaluate, improve, etc.) your objectives and goals at a project, program and strategic level. Working harder on your current strategy is unlikely to move the needle; you need to work smarter and pursue the right goals with focus.

The opening paragraph of the 2020 PSR[10] (see page 6) mentions that while data security is a complex problem, it need not be complicated. In response, readers asked for additional guidance on what they specifically need to do to assess the complexity, and on how to reveal and reduce the complicated interrelations between the components of their control environment. They requested a strategic approach to data security and compliance, a method to help them decide what to focus on, ways to determine what to aim for (goals and objectives) and post-implementation methods to measure success. This PSR focuses on Verizon's "True North" answers to their questions.

Understanding the TOC and application of the LTP are valuable additions to your toolbox, because they unlock the steps for designing and implementing a sustainable and effective security and compliance control environment. A strategic approach is essential. However, crafting an excellent strategy while pursuing goals that are unclear, lack alignment or are the wrong goals altogether is like bailing water from a boat that has a hole in the bottom. Not only is the process counterproductive and wasteful, it can also be very demoralizing.

We've done both the bailing and repair for you with a "navigational chart" that pinpoints the best course to take to define goals and objectives for your security and compliance strategy and program—and the necessary conditions to attain them. Having a chart with the best proven strategies will help your organization avoid unintended consequences, which can be cataclysmic to a security program.
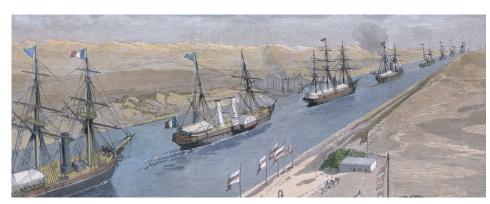
Unintended consequences: The Ever Given metaphor

The container ship Ever Given's misfortunate accident in the Suez Canal is a timely metaphor for the importance of considering unintended or unexpected consequences. Such consequences can occur when design, strategy and planning lack foresight and coordination.

"The questions you ask determine the answers you get."

—Anonymous

The Suez Canal was created to accommodate shipping traffic between Port Said on the Mediterranean Sea and Suez on the Red Sea. In 2015, engineers widened the canal in certain sections for two-lane traffic and for the increasing size and weight of container ships. In the past 15 years, the size and

Early days of steam ships passing through the Suez Canal.

10 2020 Payment Security Report, Verizon, 2020, https://www.verizon.com/business/resources/reports/payment-security-report/

weight of container ships has doubled—increasing container capacity from about 10,000 20-foot equivalent units (TEUs) to as many as 25,000 TEUs. In March 2021, one of the largest ships in the world, the Ever Given, became lodged sideways in the canal for six days and four hours, stalling tens of billions of dollars in trading per day.

Several converging factors caused the accident:

1) Human error and poor communication and coordination[12]

2) Limited regulation and/or coordination between the shipping industry and Suez Canal officials during the time container ships grew significantly in size[13]

3) A narrow section of the canal where the Ever Given—one of the longest ships in service—became wedged was not widened during the 2015 Egyptian canal redevelopment project

4) Hydrodynamics: Large container ships in shallow, narrow canals have a smaller gap between the hull, canal walls and canal floor, increasing the bank and squatting effects, making ships less maneuverable[14]

5) A dust storm and high winds apparently impacted visibility and maneuverability

What could planners have foreseen and implemented to avoid that disaster? Were unintended consequences at play? What regulations could have helped? Was there advanced warning, or was it a black swan event, unpredictable beyond what is normally expected of a situation with potential severity "characterized by their extreme rarity, severe impact and the widespread insistence they were obvious in hindsight?"[15]

What are unintended consequences?

The concept of unintended or unanticipated consequences was first coined by sociologist Robert K. Merton to describe outcomes of a purposeful action that are not intended or foreseen. His foundational work "The Unanticipated Consequences of Purposive Social Action"[11] defines three different types of unintended consequences:

- **Unintended benefit**
  A positive, unexpected benefit (sometimes called a windfall or serendipity)
- **Unintended drawback**
  Negative consequence with a positive benefit
- **Perverse result**
  Negative consequence with no positive benefit

Unintended consequences are sometimes categorized as both a drawback and perverse result. This is particularly relevant in cases with unexpected security or safety concerns.

11 Robert K. Merton, "The Unanticipated Consequences of Purposive Social Action," American Sociological Review, 1936, https://www.jstor.org/stable/2084615
12 Vivian Yee and James Gianz, "How One of the World's Biggest Ships Jammed the Suez Canal," The New York Times, Jul 17, 2021, https://www.nytimes.com/2021/07/17/world/middleeast/suez-canal-stuck-ship-ever-given.html
13 The Impact of Mega-Ships, The Organisation for Economic Co-operation and Development (OECD), International Transport Forum, 2015, https://www.itf-oecd.org/sites/default/files/docs/15cspa_mega-ships.pdf
14 Marc Vantorre, et. al., "Maneuvering in Shallow and Confined Water," Encyclopedia of Maritime and Offshore Engineering, Apr 20, 2017, https://doi.org/10.1002/9781118476406.emoe006
15 "What is a Black Swan?" Investopedia, Mar 22, 2021, https://www.investopedia.com/terms/b/blackswan.asp#

> "The best laid plans of mice and men often go awry."[16]
>
> —Robert Burns

In 2015, The Organization for Economic Co-operation and Development (OECD) raised the following concerns about the shipping industry:[17]

- Container lines typically are not consulting regulatory, government or shipping agencies before building larger container ships

- Appropriate discussion forums are needed "between liners and transport stakeholders ... including governments, regulators, port authorities and all interested constituents ... to facilitate an exchange of views, an understanding of objectives and plans, and ultimately better coordination"

- Attention is needed on "insurability of mega-ships and the costs of potential salvage in case of accidents"

- Data is showing the potential cost savings to carriers as "fairly marginal," while infrastructure upsizing costs "could be phenomenal"

- Many ports and countries "accidentally or on purpose, encouraged the development of mega-ships"

- Countries and ports "frequently make decisions that seem positive on an individual level, but could be detrimental at a collective level," and an extensive cost/benefit analysis is needed

Cargo ship Ever Given being unlodged from the banks of the Suez Canal in March 2021.

Failure to deal with constraints

When completed in 1869, the Suez Canal was 102 miles long, 26 feet deep and 200 feet wide at the narrowest point, with maximum capacity for a loaded ship weighing 5,000 tons. The canal was later expanded to 120 miles long, 79 feet deep and 656 feet wide at its narrowest point, with maximum capacity for a ship weighing 240,000 tons. The 1,312-ft Ever Given is significantly longer than the canal is wide and became stuck where the canal is about 985 feet wide.

The Ever Given fiasco shows how important it is to pinpoint constraints in a design. This is particularly relevant today at a time of rapid evolution and complexity with digital transformation. All possible constraints (based on a risk assessment) need to be considered when building security frameworks. After the fiasco, the Egyptian government acknowledged the lack of foresight and, in May 2021, announced plans to widen and deepen the canal in the stretch where the Ever Given lodged.

---

16 "The best laid plans of mice and men often go awry," SAP Community Blogs, 2010, https://blogs.sap.com/2010/01/07/the-best-laid-plans-of-mice-and-men-often-go-awry/

17 The Impact of Mega-Ships, The Organisation for Economic Co-operation and Development (OECD), International Transport Forum, 2015, https://www.itf-oecd.org/sites/default/files/docs/15cspa_mega-ships.pdf

The Top 7 Strategic Data Security Management Traps

In the 2020 Payment Security Report, we included the Top 7 Strategic Data Security Management Traps to help CISOs streamline planning processes. Knowing these traps is valuable when considering how unintended consequences can be overlooked in planning stages. With the Ever Given accident, they include:

Trap 3: Lack of resourcing capabilities	Were feasibility studies performed by enough entities? Were planners, designers and engineers given ample resources to analyze potential problems and complete the entire design? Did they struggle with time and resource constraints?
Trap 4: Falling short on sound strategic design	Was it planned properly in the design stages?
Trap 5: Deficient strategy execution	Was the plan sufficient, but alignment between various entities insufficient?
Trap 7: Communication and culture constraints	Was there ample communication? Did it focus on the most complex, crucial and cultural issues?

When implementing design changes, CISOs and security experts should consider the "precautionary principle," which emphasizes that burden of proof should be defined as being able to show lack of harm, rather than to prove harm. The approach is often used by policy makers when conclusive evidence is not yet available and redesigning and decision-making can result in harm. "The precautionary principle forces us to ask a lot of difficult questions about the nature of risk, uncertainty, probability, the role of government and ethics. It can also prompt us to question our intuitions surrounding the right decisions to make in certain situations."[18] When designing for change, such considerations can help organizations avert costly data breaches.

---

18 "The Precautionary Principle: Better Safe than Sorry?" Farnam Street, June 2021, https://fs.blog/2021/06/precautionary-principle

Digital risk management and predictive technology

Making even minor changes to complex systems can result in unforeseen outcomes. Anticipating and planning for all possible repercussions in the design process is essential, but complex interdependencies can make predicting outcomes difficult. This is why payment security requires a comprehensive, well-researched design approach. This is especially true when combining the new customized approach of PCI DSS v4.0 with the multiple drivers of digital transformation.

Digital risk management (DRM) is central to security and enterprise risk for evolving organizations that are increasingly dependent on digital processes. DRM strives to build digital resiliency so that an organization's security systems can detect and respond to digital threats, thereby reducing financial disruptions and losses.[19] Many of these risks will emerge in new forms as innovative digital processes, services and products are introduced to already well-established frameworks.

2020 proved to be a year when threat actors launched particularly surreptitious attacks in response to companies scrambling to adapt to and survive the COVID-19 pandemic. Shortly after COVID-19 became widespread, 69% of boards of directors accelerated their digital business initiatives, according to the "2021 Board of Directors Survey" by Gartner Group, conducted May through June 2020 in the United States, Europe-Middle East-Africa (EMEA), and Asia-Pacific (APAC) regions. The study also found that 67% expected budget increases in technology and a nearly 7% increase in 2020 IT budgets.[20]

Predictive technologies are expected to become increasingly helpful with risk management and adverse unintended consequences. However, organizations need to take the necessary steps to prepare for integration of algorithms, analytics and artificial intelligence (AI) as viable means of risk management.[21] (See "Appendix D: AI and ML in the payment card industry" on page 159 for more details.)

The psychology of risk compensation

In addition to focusing on digital risk, CISOs and security experts need to be mindful of risk compensation:

the tendency to allow risky behaviors to increase when implementing security controls because of the false sense of security the controls create. Insurance companies are factoring this tendency into their security assessments. Risk compensation is a common syndrome in traffic psychology, where the presence of new safety measures creates a tendency for people to exhibit riskier behaviors. For example, introducing safety features such as seat belts, helmets and anti-lock braking systems in vehicles resulted in an increase in driving speed.[22] According to a 1994 study, motorists drove faster and with less caution when wearing seat belts. In similar risk compensation theory studies, when a vehicle was equipped with anti-lock braking systems, drivers drove closer to the vehicles preceding them.[23]

19 "What Is Digital Risk Management?" Digital Risk Management Institute, https://www.drminstitute.org/what-is-digital-risk-management/

20 "Gartner Says 69% of Directors Accelerated Their Digital Business Initiatives Following COVID-19 Disruption," Gartner, Sep 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-30-gartner-says-sixty-nine-percent-of-boards-of-directors-accelerated-their-digital-business-initiatives-folloing-covid-19-disruptions

21 Nitin Nohria and Hemant Taneja, "Managing the Unintended Consequences of Your Innovations," Harvard Business Review, Jan 19, 2021, https://hbr.org/2021/01/managing-the-unintended-consequences-of-your-innovations

22 Peter Berlich, "Risk compensation," Network World, IDG Communications, Inc., Mar 9, 2008, https://www.networkworld.com/article/2237441/risk-compensation.html

23 "Anti-lock braking system," Wikipedia, https://en.wikipedia.org/wiki/Anti-lock_braking_system

2

Commentary

Charting the best strategic method for your organization

Pretend you are a CISO asked to deliver a compelling, three-minute narrative on how your company is effectively meeting data security compliance requirements. Many CISOs would struggle to do so because there's so much information to cover. CISOs frequently spend too much time explaining technical details and being involved in the time-consuming task of managing a multitude of security vendors. To successfully deliver that compelling narrative, you need a framework that distills a response down to the most essential components: clarity on goals, requirements (their success factors and necessary conditions) and constraints.

Too many CISOs are still stuck in approaches from 20 to 30 years ago. They are decades behind in the way they should operate, much as Rolf M. von Roessing pointed out in 2010:

> "Information security professionals continue to find themselves reacting to issues within the enterprise rather than taking a proactive stance. This constant firefighting leaves little time for innovation, strategic thinking and planning. Security professionals revert to applying controls to problems as they arise, often with an over reliance on technology. This is often accompanied by a lack of historical data, so problems continue to occur, even though they have been 'fixed' at some previous point."[24]

This does not have to be the case today. CISOs and security departments can overcome constraints that are impeding success by applying the correct frameworks and overall approaches. By rethinking and reframing your approach to data security and compliance, methods, and priorities—and how you communicate them to executive teams and boards of directors—you gain control of the security direction of the organization and areas of internal operational investments.

24   Rolf M. von Roessing, The Business Model for Information Security, ISACA, 2010, https://www.isaca.org

Year after year, Qualified Security Assessors (QSAs) conducting compliance validation assessments discover that controls are not kept in place. Organizational failure to apply systems thinking to diagnose and solve reoccurring control and program performance issues is a major contributor to the problem. For some organizations, it's a condition of "learned helplessness." Learned helplessness is a psychological condition "in which a person has a sense of powerlessness, arising from a traumatic event or persistent failure to succeed."[25]

While a PCI DSS compliance assessment could be viewed as a "traumatic event" for some (we hope not!), the definition of "persistent failure" is what's most significant in this context.

Security teams may incorrectly perceive low sustainability of the PCI DSS control environment as an intractable problem that no efficient algorithm can solve. Solving an intractable problem hinges on two primary elements: determining the critical root cause and determining the most effective next action.

This helplessness occurs in the face of two primary criteria: when there is the perception of no clear cause of the lack of sustainable control effectiveness (the problem), and when there is no clear next action—a next logical step to address a control system that lacks effectiveness and sustainability.

You need a method.

If you're struggling to develop your security and compliance strategy and create a strategic plan that you are confident will deliver the required objectives and goal, you may be missing an effective method.

Why is it important to create a method or proven process for designing a strategic plan? Some of the most successful, sustainable products and procedures incorporate a proven process. Dentists adhere to a series of fail-proof steps when filling teeth. Builders prepare the land and have a secure method for building a foundation before constructing a house. Why wouldn't security professionals apply a method of control design for security systems? What many organizations lack is a logical method to deconstruct the complexity of establishing clear goals and objectives, and the capacity to achieve them. Applying logical thinking is the ability to achieve progress in incremental, clear and predictable steps.

Defining goals is the first step in dealing with a complex problem.

For a surprisingly large number of organizations across the payment card industry, it's not immediately obvious what they need to achieve with their data security and compliance programs. For many, this will become increasingly important with PCI DSS v4.0, which is why we are introducing a cohesive method to separate the most essential from the peripheral. In short, organizations need an LTP to clearly

---

25 "Learned helplessness," Oxford Lexico, https://www.lexico.com/en/definition/learned_helplessness

establish their goals, requirements and constraints. Developing the capability to determine root causes and formulate solutions to factors (constraints) that negatively influence the performance and outcome of the environment is an increasingly essential and unavoidable management task in the evolving security matrix. For more detailed information on goals, requirements and constraints, see page 21.

Focusing on your goals provides mastery over the problem.

It's common for security teams to be spread thin and feel overwhelmed—as if they're always just treading water. Increasing staffing can be difficult and is often only part of the solution. There seems to be too little time to focus on strategy and goals.

"A wealth of information creates a poverty of attention!"[26]

—Herbert A. Simon, economist, psychologist and Nobel prize winner

The reality is that strategic planning, coordination and execution at an operational level have become paramount for security and compliance approaches and programs to succeed—and avert costly data breaches. We're not talking about annual task lists outlined by executive management. We're referring to focus: application of scarce resources on

clearly prioritized activities to drive outcomes that are of strategic, long-term benefit to the organization. Security teams need to remain focused on clearly defined goals with very specific objectives and stop being busy with tasks that don't promote sustainable control effectiveness. Of course, this is easier said than done. The reality for most security teams is the daily battle of people and departments pulling them toward distractions and chipping away at the time available to work on activities that have higher long-term value and contribute to security and compliance strategic goals.

"There is nothing as useless as doing efficiently that which should not be done at all."[27]

—Peter F. Drucker

Focus often means knowing when and how to say "no" to competing activities and tasks. Achieving focus requires avoiding distractions. For many security teams, this requires a deliberate reduction in scope of what others expect them to undertake. The security team's attention must be diversified enough to cover the broad scope of security and compliance responsibilities, yet concentrated enough to maintain consistent progress

toward the achievement of objectives. It requires the development of the team's collective decision-making skills to triage requests based on risk (impact, probability and asset value) and relevance to the accomplishment of the strategic objectives. It's imperative to focus on core strategic data security objectives, stay alert to unwarranted distractions, categorize secondary and tertiary objectives, and prioritize activities that contribute most to the sustainable effectiveness of the control environment.

Ideally, you should have a one- to five-year plan to focus on, though many organizations benefit from strategies that map out a program over an even longer period—up to 10 years. Strategies should be revisited several times throughout the year—even monthly—to make both large and incremental improvements. For additional information on security strategy, see page 43 of the 2020 PSR.[28]

---

26 "A Wealth of Information Creates a Poverty of Attention!" influencepeople, Oct 15, 2018, https://www.influencepeople.biz/2018/10/wealth-information-creates-poverty-attention.html

27 Peter F. Drucker, "Managing for Business Effectiveness," Harvard Business Review, May 1963. Reproduced with permission from the Drucker 1996 Literary Works Trust.

28 2020 Payment Security Report, Verizon, 2020, https://www.verizon.com/business/resources/reports/payment-security-report/

Optimizing limited resources by strengthening the weakest link

With the right resources—experienced teams and ample funding—it's theoretically possible to improve every part of an organization. The reality is that even the largest and most prosperous organizations have limited resources—time, budget and skilled people—available to invest in making the changes needed to improve all the systems, processes and capabilities within their organization.
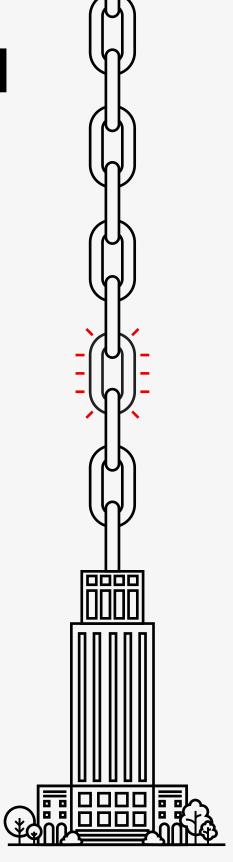
When security and compliance teams continue to experience an acute shortage of skilled professionals across the globe, how does a CISO and security steering committee decide where and when to focus time and scarce resources to remain effective? What's needed in many organizations is a reliable method to focus on and differentiate between the "many" components—the various systems, processes, documents, capacity, capabilities, etc.—that "can" be improved from the "few" that "must" be improved in order to achieve the security and compliance objectives and goal.

Continuous compliance and increased expectations of ongoing improvement are part of the PCI DSS v4.0 requirements. The key to achieving ongoing growth and stability of security and compliance program performance is to find a way to focus resources on only the parts within the control environment that are currently limiting or blocking further improvement—the weakest links, system constraints or leverage points.

PCI security compliance environments, and control environments in general, are complex systems. However, they are governed by inherent simplicity. In most cases, the majority of poor performance issues are caused by very few underlying causes (the Pareto principle—also see the general truism of Price's Law).[29]

Performance improvement of PCI security compliance programs, and compliance of the control environment, is not equal to the sum of improving all the components. Focusing on improvements by targeting the weakest links—the most important constraints in a few components—can improve the performance of the whole system (see the note on "systems thinking" on page 71).

The strength of any chain is limited by the weakest link. Similarly, the effectiveness and sustainability of a control environment is limited by the performance of the weakest link (system constraint). Improving less-weak links (i.e., focusing on any link that is not the weakest) will not improve the performance of the environment, while improving the weakest link will always result in improvement to the environment as a whole.[30]

---

29 "Understanding the Pareto Principle (The 80/20 Rule)," Better Explained, https://betterexplained.com/articles/understanding-the-pareto-principle-the-8020-rule/
    Price's Law: Only a handful of people produce half of the results in any given field or company. Fifty percent of work is done by the square root of the number of people who participate in the work. If a company has 10 employees, three of them will do 50% of the work and the other seven will do the rest. With 100 employees, only 10 will account for 50% of the work. https://dariusforoux.com/prices-law/
30 Alan Barnard, "What is Theory of Constraints (TOC)," Goldratt Research Labs, http:www.https://goldrattresearchlabs.com/about/

Applying an easy-to-understand method based on sound analysis and reasoning offers a much-needed breakthrough. The LTP lays bare erroneous assumptions about what teams focus on and what they do not. It's a practical method to help differentiate between all the parts that can be improved and those few that must be improved to achieve more with fewer resources.

For an overview of the benefits of applying the Logical Thinking Process to improve the performance of PCI security programs, see page 69. For a more detailed discussion of how to apply the Theory of Constraints, see page 64.

The GRC² Model = The Goals, Requirements and Constraints x Governance, Risk Management and Compliance

The 2020 PSR highlighted the critical importance of organizations taking strategic action to drive investment in the development and enforcement of security and compliance programs. In many cases, it's a survival skill to combat growing complexity. In addition to a sound security and compliance strategy, the success of PCI security compliance programs often depends upon the extent to which the program is integrated with governance and

risk initiatives/activities into the broader control environment. A direct relationship exists between the amount of time and effort organizations invest into the design, execution and ongoing management of their governance, risk management and compliance (GRC) program, and the effectiveness of their PCI security programs.

The term GRC is an established acronym that has been in existence for about 20 years. It's an umbrella term for a management discipline and operational framework. To assure the realization of organizational goals and objectives, GRC requires an integrated, organization-wide approach to establish clearly defined, measurable standards of performance.

In other words, the main purpose of GRC as a business practice is to develop and maintain a well-coordinated and integrated collection of capabilities to support predictable and reliable performance at every

level of the organization. It's a structured approach to align IT with business objectives, while effectively managing risk and meeting compliance requirements. Organizations should develop this essential capability to achieve goals and strategic objectives and meet stakeholder needs.

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

Regulation is the biggest driver for GRC. The past two decades saw a substantial increase in demands from third-party stakeholders for greater transparency. Stakeholders increasingly demand (and contractually require) evidence of high-performance GRC capabilities. A significant internal

G² = The goals, requirements and constraints of governance

Governance is the way an organization is directed and controlled to reach goals. In GRC, governance is necessary for setting direction (through strategy and policy), monitoring performance and controls, and evaluating outcomes. Governance can be defined as the combination of processes that facilitate decision-making. The processes are established, executed and supported by all levels of management. This should be reflected in the organization's structure. Activities performed under this category are carried out in order to clearly define and communicate control mechanisms that ensure that decisions and directives made by management are properly carried out. The processes are designed to include ongoing support of the governance function to ensure that critical, relevant management information—which is accurate, sufficient and complete—reaches the management team on a timely basis (clear visibility).

driver is the need to manage costs associated with addressing risks and compliance requirements to prevent them from spinning out of control.

These demands resulted in an industry of exponential growth in the selection of GRC tools (software applications) to support the automation, management and reporting of GRC activities. Having a tool alone isn't enough to guarantee effective GRC, as technology does not have ethics—people do. Hence, GRC must be addressed from a systems-thinking, people-and-process perspective even before technology is considered.

Complexity adds no value. Organizations need to apply a framework—a powerful method for simplifying the overall approach needed to achieve results in a highly structured and predictable manner.

The three practices that make up GRC share common and interrelated tasks, with overlapping areas of responsibility and processes. They are more effective when integrated and dealt with as combined practices.[31]

GRC involves bringing the right groups of people together, supported by appropriate technology; clarifying performance expectations and outcomes (goals); determining the necessary resource commitments (requirements) needed to ensure that those goals are achieved; and evaluating what could get in the way (constraints).

Although the concept of governance, risk management and compliance (GRC) is no longer an emerging field of

study within the information assurance community, understanding its successful design and implementation still requires some demystification

and exploration. That's why the author formulated GRC², pronounced "GRC squared." GRC² stands for the multiplication of each individual

R^2 = The goals, requirements and constraints of risk management

Risk management anticipates risks that could potentially cause harm or loss or hinder the organization from successfully managing and achieving its goals. It ensures that the organization promptly identifies, analyzes and controls risks that can derail the achievement of strategic objectives. The processes include identification and classification, assessment and communication, mitigation, and reporting on the containment of risks.

C^2 = The goals, requirements and constraints of compliance

Compliance refers to a defined process and consistent accounting of organizational practices for ensuring that policies, standards and guidelines are employed and followed. Depending upon the context, compliance ensures that the organization takes measures and implements controls to assure that internal and external compliance requirements are consistently met. It sets measurable standards of performance for an organization's policies and procedures on practices and individual behavior that need to conform to the expectations of a broad range of internal and external stakeholders. This typically includes compliance requirements from third-party contractual obligations and external government and industry regulations—such as PCI security.

The compliance process includes recording all components that must be complied with, assessing the state of compliance of the organization and cost-benefit analyses to evaluate the possible impact of noncompliance with the rules. Compliance activities usually involve documentation of processes and the risks of compliance and noncompliance; identification, definition and documentation of compliance controls in place; assessment of the effectiveness of the controls; remediation of compliance issues; and disclosure and certification of compliance processes.

---

31 For a deeper understanding of GRC, refer to:
    "Governance, risk management, and compliance," Wikipedia, https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance
    "Governance, Risk And Compliance (GRC)," CIO Index, https://cio-wiki.org/wiki/Governance,_Risk_And_Compliance_(GRC)

governance, risk management and compliance component with its respective goals, requirements and constraints. This presents an enhanced model for the logical step-by-step design, implementation, management and evaluation of a GRC approach.

Many organizations isolate their PCI security compliance programs from broader governance programs, not realizing the effectiveness and efficiency of a synchronized approach, which avoids overlap and repetition of tasks between various programs. A unified compliance approach to meet various regulatory requirements under a single corporate governance umbrella has significant compliance and risk management benefits. Organizations should, at least annually, revisit the goals, requirements and constraints of their governance program. We include definitions of GRC below, which you can reference when constructing the articulation of your strategic goals and objectives.

PCI DSS compliance focuses on managing risk associated with the storage, transmission and processing of payment data by defining the requirements within and between PCI security programs and enterprise risk management programs.

GRC² Model

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

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

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

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

GRC: A management model that promotes criteria unification, communication and collaboration between different stakeholders in the management and control of the organization
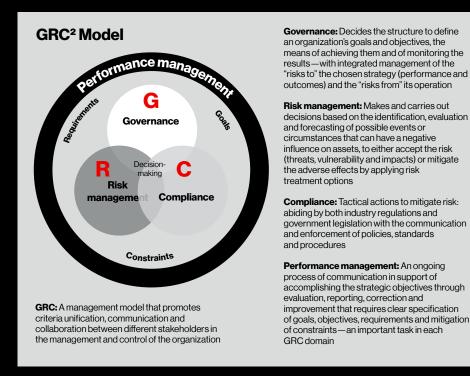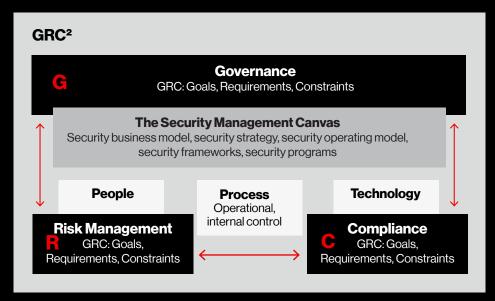
Figure 1. The interactions of the GRC² Model

GRC²

Figure 2. GRC² Model = Managing the GRC (Goals, Requirements and Constraints) of GRC (Governance, Risk Management and Compliance)

This process (compliance) should be very familiar to any organization that has completed a PCI DSS assessment.

In the 2020 PSR, we highlighted Verizon's Top 7 Strategic Data Security Management Traps, which range from inadequate leadership (often rooted in the organizational structure) to communication and culture constraints. Readers concerned about compliance issues would benefit from reviewing those traps (see page 12 of the 2020 PSR).

Deconstructing GRC[2]

Various options exist for defining the design and implementation of a GRC approach within your corporate security and compliance strategy. GRC involves a range of different organizational activities, from setting up roles and responsibilities, business processes, and arranging periodic compliance assessments, to establishing internal continuous control monitoring and reporting procedures. Observing how organizations approached the implementation of GRC over the last 20 years offers valuable lessons in strategic and critical success factors. Many factors determine the successful outcome of GRC initiatives; in the majority of cases, organizations pay far too little attention to defining what they actually aim to achieve, the necessary requirements (capabilities) and critical constraints that stand in their way. In other words, too many organizations gloss over goals, requirements and constraints in relation to governance, risk management and compliance.

Goals
Define what you aim to achieve, an obvious but often overlooked step that can determine success or failure. The solution is to gather together key stakeholders and project staff, brainstorm what GRC means to your organization, and generate priorities based on specific needs. Make sure you determine which goals (for governance, risk management and compliance) should have top priority. (See page 25 for further explanation on goals.)

Requirements
Identify the necessary conditions to meet objectives and goals once you've identified, clarified and documented what governance, risk management and compliance mean to your organization, and the overall goals for each. Also determine what the requirements are for each. What are the objectives to reach the goals and respective requirements—the necessary capacity, resource inputs and capabilities? Which requirements should be prioritized as most logical and beneficial? Which method should be used to determine where to focus team energy and prioritization? How do you identify the requirements that will benefit your approach to GRC the most—particularly in light of the changes brought about with PCI DSS v4.0? (See page 42 for further explanation on requirements.)

Constraints
Take stock of your current situation and capabilities, because every complex system, including PCI security compliance and data security, consists of multiple linked activities that act as a constraint upon the entire system. A constraint is anything that limits a system from achieving higher performance in relation to its goal. It can be a step or process that is producing less than what's demanded of it. At least one constraint exists in every system.

Systems are analogous to chains. Your payment card security and compliance system consist of a chain of processes. Each system (chain) has a weakest link (constraint) that ultimately limits the success of the entire system. If you want to improve the system (strengthen the chain), where is the most logical place to focus your efforts? The weakest link! A constraint can be elevated to the point where it's no longer the system's limiting factor. This is called breaking the constraint. The limiting factor is now some other part of the system, or may be external to the system (an external constraint). This approach can be applied to PCI DSS compliance environments to break constraints that prevent the control environment from achieving the required level of effectiveness and sustainability. (For further explanation on constraints, see the 6 Constraints of Organizational Proficiency on page 45 of the 2020 PSR, the updated 7 Constraints of Organizational Proficiency table on page 68 and the risk of unintended consequences on page 11 of this report).

Goals: The security and compliance rudder

Point 1:
The fundamental importance of goals

No CISO can hope to truly succeed with data security and compliance without knowing three things:

- What the ultimate goal is
- Where they currently stand in relation to that goal
- The magnitude and direction of the change needed to move from the status quo to where they want to be (the goal)[32]

CISOs and their security teams are understandably busy. Focusing on the complexity of data security and compliance requires time. The day-to-day operations always appear to be more pressing and given higher priority than taking the time for proper introspection and foresight.

Figuring out exactly what the right goal is—and creating a navigation chart to get there—can be daunting for those very reasons. Some CISOs erroneously think that devoting the proper amount of time to planning a goal is not a top priority, despite knowing that the goals of a data security and compliance program are far more achievable and effective with a strategy in place. A strategy applies focus and prioritization to obtain carefully chosen, defined goals.

It's not the amount of technology, resources or policies that help improve the effectiveness and sustainability of a control environment. It's the decisions behind the formulation of the goals that make the difference.

Organizations are investing an unprecedented amount of money to secure sensitive data and meet compliance requirements. Yet, it's not the amount of technology, resources or policies that help improve effectiveness and sustainability in a control environment. More important is the quality of decisions behind the formulation of the goals—the data and analytics behind the decisions. Those goals are integral to the security business model, security strategy and security operating models (see The Security Management Canvas, page 33). They determine the quality of security governance and how the CISO, steering committee and board of directors can turn the tide.

32   H. William Dettmer, "Goldratt's Theory of Constraints: A Systems Approach to Continuous Improvement," American Society for Quality (ASQ) Press, 1997.

Do not underestimate the value of effective goal setting.

Organizations should not be surprised when they struggle to achieve sustainable control effectiveness if it's not an explicit goal supported by a strategy that directs resources toward prioritized objectives.

Too often, PCI security program team members chase off in different directions. All participants and stakeholders should have the same vision of the end point. When program participants work toward different end points, even inadvertently, it often becomes impossible to completely correct the misalignment and pull them all together at the end. All team members should follow the same strategy and navigation points for successful achievement. Even minute differences in interpretation of the success criteria can lead to quite dissimilar outcomes.

Point 2:
Differentiating goals from objectives

Goals specify the desired results, outcomes and destinations of the organization's mission and ambitions into specific, quantifiable terms with measurable results. Your primary security and compliance goal statements should be quantified in advance of strategy implementation. Their achievement (or nonachievement) should be specifically measured throughout the implementation and operation of the tasks and processes along the journey.

Clear communication of goals helps you conduct day-to-day operations with a sense of purpose and direction. It promotes accountability, as team members can be held responsible for their tasks to the collective team.

"It is more important to know where we are going than to get there quickly. Do not mistake activity for achievement."[33]

—Mabel Newcomer

Organizations should not be surprised when they struggle to achieve sustainable control effectiveness if it's not an explicit goal supported by a strategy that directs resources toward prioritized objectives.

33 Mabel Newcomer, "Vassar Welcomes Class of '39 at Convocation," The Vassar Miscellany News, Oct 2, 1935, https://news.hrvh.org/veridian/?a=d&d=vcmisc19351002-01.2.7

Good communication lays a foundation for collaborative work toward proclaimed goals. Setting clear goals for PCI security compliance can affect individual performance by:

- Directing action and effort toward goal-related activities and away from unrelated activities, which is greatly needed to deal with the changes PCI DSS v4.0 will introduce
- Energizing employees, leading to higher employee effort
- Motivating employees to apply existing knowledge to attain a goal, or to acquire knowledge necessary to do so
- Triggering persistence through frequent reminders of goals—again, employees may exert more effort

Can you keep your compliance ship straight?

The goals of your data security compliance program are like the rudder on a ship. The rudder sets the direction and determines where you go. If you commit to one specifically defined set of goals, or perhaps even a single well-articulated goal, then the rudder stays put. You continue moving forward on course. If you flip-flop between vague or conflicting goals, the rudder moves all around, and it becomes easy to find yourself going in circles (or getting stuck in the Suez Canal).

However, other parts of the ship are just as important as the rudder; for example, the engine and the hull. If the rudder is your goal, then the engine is your process for achieving it. While the rudder determines your direction, it's the power and speed of the engine and

Goals: A goal is an end result you want to achieve with your data security and compliance strategy and program. It's typically a general and overarching idea expressed clearly, concisely and descriptively. Goals for your organization should be aligned with your organization vision, mission and ideals. They are both long-term and time-sensitive indicators of what should be accomplished and where your organization expects to be in the future. Goals are normally singular and expressed as a single sentence or short paragraph articulating the desired outcome, the anticipated date it is to be achieved and the resources required.

Objectives: While goals are usually broad, objectives are much more specific, clear and actionable. Objectives are smaller, specific targets within the general goal. They articulate how a goal is attained, with specific actions and steps to take to achieve a goal. Objectives are time-bound and have more immediate deadlines than goals. Objectives include measurable performance factors, challenging but approachable deadlines, and clearly stated costs and quantities.

Goals express a wide-range vision. Objectives focus on the individual, achievable outcomes with concrete deliverables. Progress toward objectives helps measure advancement to reaching the larger end goal.

the captain's skill in steering the ship to navigate the environment (river, canal, ocean and weather) that determine progress.

When outlining a security plan, understanding the difference between goals and objectives is important. A goal describes a broad, overarching destination: "We want to improve the robustness of all cardholder data system components in two years."

Or a goal to improve the resiliency of PCI DSS compliance: "We want the ability to detect all controls that fall out of place, prior to the PCI DSS compliance validation assessment."

A goal does not define how to achieve these objectives; it does not describe a strategy to get there or offer the specific tasks necessary to achieve the strategy. It simply specifies a target destination to work toward.

Security and compliance objectives are specific, measurable activities you need to engage in to attain broader security and compliance goals. For example: "To achieve the goal of maintaining sustainable control effectiveness of the payment card data environment, we will review, report and improve the capacity of the compliance team to support the program every two months." Or, "All PCI DSS controls that are found not in place during internal compliance validation assessments will be corrected within 30 days."

The objectives focus on particular deliverables that can be divided into a series of moves, including groundwork, analyses and creating the capacity that enables security and compliance teams (across all 4 Lines of Assurance; see page 44 in the 2020 PSR)[34] to support the objectives. On the security field, goals and objectives are a lot harder to achieve without mapping out a strategy.

Strategy: The navigation plan for successful goals and objectives

Strategy is the central plan that connects objectives with goals. The CISO and team should strive to create a security business model, strategy, and supporting security operating model and frameworks that are integrated and embodied into the security and compliance program, to help move toward an overarching set of organization-wide goals.

The challenge of customizing goals and objectives

In many security organizations, the performance appraisal and planning process involves identifying goals and objectives for an upcoming time frame. However, people often don't know the difference between a goal and an objective and conflate the terms. A helpful approach is to break down the goals and objectives into steps and stages. For example, define one to three statements that describe a destination for each individual in your security and compliance team, and for each additional key stakeholder that can impact the security of payment card data. These are your individual goals, at a team level. Each goal statement should be supported with a description of the high-level approach needed to achieve it.

Envision the goal as a final destination at the end of the field, and the objective as the various plays, maneuvers and actions needed to reach that goal. Resist the temptation to confuse the goal with the objectives needed to reach that post and, more importantly, instruct your team on the difference.

In our example above, to achieve the goal of reducing the number of PCI DSS controls that are not in place during compliance validation assessments by 50% within six months, the security and compliance team should adopt a strategy and define the specific sets of actions (objectives) necessary to realize the strategy that will propel them toward the goal. "We will increase the number of control environment reviews conducted internally to measure and report the performance of controls across the compliance environment."

A goal is supported by a clear strategy that is broken down into objectives and tactics for measuring progress. This high-level strategy statement is part of a simplified plan that is then refined to be specific about the resources, priorities and focus needed to accomplish the objectives and goal. A strategy statement frames the major actions but stops short of describing specifically how those actions will be implemented.

> "Success is doing a thousand little things the right way ... over and over again."[35]
>
> —Charles R. Walgreen, Sr

Point 3:
The circular journey between goals and strategy

The value of taking a strategic approach to data security and compliance was covered throughout the 2020 PSR. Since the release of that report, more organizations are aware of The Security Management Canvas. We also explained what strategy is, its components and how to evaluate the strength of a security strategy.

When a CISO is asked about their security and compliance strategy, the response is often a list of activities and description of various operational metrics. The list often fails to summarize how they are progressing against the primary goals. When a strategy cannot be articulated clearly and concisely, it's often an indicator that there probably isn't an effective, executable strategy in place. This is often a symptom of "strategy development sessions" where participants focus on a narrow set of key performance indicators. No matter how much enthusiasm is at the table, they are likely to emerge with a list like this:

- Improve information security
- Optimize the investments in security and compliance
- Increase security awareness and training
- Improve security configuration management, etc.

These are vague statements of intent. While they may contain what might be called goals, objectives or actions, they are not easily attainable. Participants often jump into developing solutions, burrow into the details and quickly lose sight of the actual goal. They lose the birds-eye view and get stuck in fix-it mode.

While goals, objectives and clear targets are not a substitute for strategy, they are essential to strategic development.

Which comes first, goals or strategy?

Don't confuse strategy with goal setting. They are not the same, and it's important to understand the difference. Set the goal first, then decide how best to reach it through strategy and tactics. Innovation requires a goal to get started. As Stephen Covey said, "Begin with the end in mind."[36]

For security strategy and programs to be viable, stakeholders must agree up front on the goals, objectives and success criteria. This is a necessary condition for project success, not a sufficient condition. Unfortunately, nothing absolutely guarantees success. But without clearly defined goals and carefully chosen tactics that support your goals, you can't gauge progress and make adjustments to a strategic plan.

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

Goal → strategy → tactics

Properly set data security and compliance goals provide a clear vision for teams and individuals involved in or able to influence the security of the control environment—particularly for the teams within each line of assurance. It's recommended that people across all 4 Lines of Assurance participate in the development and execution of goals, strategies and tactics. Clear communication of goals helps them conduct day-to-day operations with a sense of ownership, purpose and direction. They invest in the learning, success and failures.

---

35 John U. Bacon, "America's Corner Store: Walgreen's Prescription for Success," John Wiley & Sons, Inc., 2004.
36 Stephen R. Covey, "The 7 Habits of Highly Effective People: Restoring the Character Ethic," Simon and Schuster, 1989.

The pursuit of goals and execution of strategy is often not linear, but circular. As you progress through the execution of your strategy, it can reveal new—and better—goals.

"How do the goals of cybersecurity differ from other goals?" is a logical question. More specifically, "What are the goals of cybersecurity?" And "What are the goals of information and data security?" Or even more specifically, "What is the goal of PCI DSS compliance?"

A very basic response is "to protect payment card data from being compromised by maintaining strict control over the confidentiality, integrity, authenticity, availability and utility of all systems and components that process, transmit or store payment account data and its surrounding environment, in accordance with PCI Standards."

While this is true, oversimplifying goals is dangerous. Which is one reason why it's worth clearly defining your goals to internal and external stakeholders before working on how to achieve them.

Compliance is one of the components of an organization's governance (GRC) that is concerned with protecting stakeholder value by managing business risk. Therefore, the objectives and goals of a PCI security compliance program should be to align with the primary goals pursued by the organization's GRC strategy. It's widely recognized that the goals of PCI security compliance are not to implement a baseline set of security controls for the purpose of passing a compliance validation assessment.

Point 4:
Goals specific to PCI security

Key to this concept are:

- **Security assurance:**
  The grounds for and measure of confidence that the security practices, procedures, architecture and features of an information system meet objectives accurately, mediate and enforce the security policy

- **Security assurance levels (SALs):**
  Provide a qualitative approach to address goals, their requirements (necessary conditions) and constraints to plan, design, manage and maintain the performance of the security control environment at a specified confidence level

- **Sustainable security control effectiveness:**
  An essential organizational capability based on a target level of assurance. This ensures that the control environment and critical components within it have the broader organizational capacity and support to avoid prolonged negative deviation from operating standards and objectives. This requires demonstrable evidence of assurance by measuring, recording and reporting the actual quality of robustness and resilience of all critical components within the control environment. This is essential for early detection and correction of control performance deviations

As mentioned before, the effectiveness and assurance that a PCI security program offers is directly proportional to the extent it's integrated into and supported by broader GRC initiatives.

"Effective goal setting requires consideration of the system that surrounds you. Too often, we set the right goals inside the wrong system. If you're fighting your system each day to make progress, then it's going to be really hard to make consistent progress. There are all kinds of hidden forces that make our goals easier or harder to achieve. You need to align your environment with your ambitions if you wish to make progress for the long-run."[37]

—James Clear

37 James Clear, "Goal Setting: A Scientific Guide to Setting and Achieving Goals," JamesClear.com, https://jamesclear.com/goal-setting

When poorly designed goals fail

If a simple formula existed, goal setting would be easy. Designing your goals with the necessary motivation to reach them is hard. However, there are methods and known factors you can adjust to vastly improve your goal-setting skills.

CISOs, security teams, security professionals and management in general benefit from having and applying a goal-setting standard. A goal-setting standard is a repeatable and harmonized process (an agreed-upon norm) for documenting your end goal and specifying how to achieve it in a detailed, relevant, measurable and time-bound manner. Avoid any process that will result in establishing vague ambitions for your PCI security compliance program, and your overall data security and compliance strategy and efforts. These ambitions (goals) can be hard to define. Clearly defined goal-setting standards are pointless if they don't actually help you reach your goal. For example, implementing PCI DSS requirements merely for the sake of meeting baseline compliance requirements, without a sincere attempt to establish an effective and sustainable control environment, is nearly useless if it doesn't actually help you reach that goal. If you take anything away from this report, remember the importance of developing sound goal-setting standards.

Aligning goals between business and security compliance interests
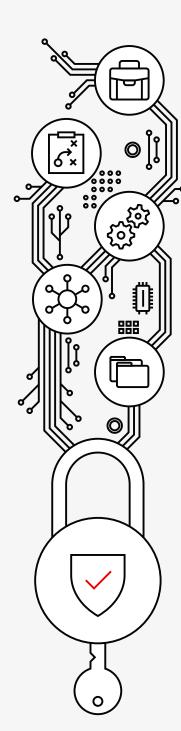
Involving stakeholders is essential. Clear goals, objectives and targets should be designed with input from all stakeholder groups. This may, in many cases, be best accomplished one stakeholder group at a time. Once accomplished, you have a significant cornerstone to build a smart security and compliance strategy for each group.

Collaboration between the CISO and board enables the organization to be in the best position to oversee necessary strategy changes and hold all stakeholders accountable. Accountability should include the effort to make sound decisions for organizational planning and management, and performance measurement of security and compliance. Not surprisingly, many CISOs and boards aren't prepared to assume this responsibility; in many cases, that's because they lack an actionable framework that will empower senior executives and board members to become stewards of their organization's data security and compliance activities.

The responsibility for satisfying security and compliance goals rests with the managers of the system, from the chief executive officer down to the front-line supervisor. If you're a manager, how do you know what the system's goals are? Frequently, managers directly involved in security and compliance have different ideas than business executives in other parts of the organization. For more information on goals, see "Appendix A: Primer for crafting security and compliance goals," page 146.

Next, we review The Security Management Canvas (TSMC)—a management tool and vital component that can be integrated into your goal-setting standard to tie strategy and operations together.

The Security Management Canvas

The Security Management Canvas (TSMC) is a template and strategic management framework that allows managers to visualize and assess all management activities on a single canvas. This one-page document template contains five boxes that represent the five most important and fundamental elements of security management. All information security activities that an organization undertakes are encapsulated.

The five pillars of The Security Management Canvas

1. **Security business model (SBM):**
Communicate a strategic SBM that ties all security management elements together to convey the value of GRC, and to secure the investment needed

2. **Security strategy:**
Communicate a refined security strategy with clear goals and objectives to all stakeholders, and that includes sustainable control environment effectiveness as an explicit objective or goal

3. **Security operating models (SOMs):**
Communicate the current and target SOMs in a set of visualized operational maps essential for effective management to help diagnose constraints and drive progress

4. **Security frameworks:**
Integrate supplemental programs and governance frameworks; avoid selective application and instead fully implement them to achieve their intended benefits

5. **Security program:**
Manage the program and supporting frameworks collectively as an integrated GRC program (the maturity and support of your security program is supported by the other elements of the canvas)

We will briefly review the five components of TSMC (introduced on pages 15 to 17 of the 2020 PSR) and follow with an explanation of the two important but lesser-known elements: the SBM and SOM.

The Security Management Canvas

Security business model	Security strategy	Security operating model	Security frameworks	Security program
• **Value proposition** • **Stakeholders** • **Goals and objectives** • **Architecture and structure of core process** • **Resources** • **Culture** • **Regulations** • **Risk management** • **Governance**	• **Stakeholders** • **Priorities** 　– Goals 　– Objectives • **Focus** 　– Exclusion of activities • **Application of resources** 　– In-house 　– Third-party • **Top 7 Strategic Data Security Management Traps**	• **Visual presentation of operations** 　– Stakeholders and relationships 　– Organizational chart 　– Geographical map 　– Organizational process map 　　▫ Core 　　▫ Supporting 　– Security process map 　– Functional responsibilities 　– Capability map 　– Constraints map	• **Adopted security frameworks and standards** 　– PCI DSS 　– ISO 27000 　– NIST CSF 　– CoBIT • **Coverage** 　– Scope of implementation 　– Coverage of systems components 　– Partial vs full implementation of frameworks 　– Coverage of framework elements	• **Program management** 　– Charter 　– Program management office • **Program scope** 　– 9 Fs 　– 7 Cs 　– 4 Ls • **Project management** • **Maturity models** 　– Process 　– Capability • **Performance** 　– Metrics 　– Reporting

Figure 3. The fundamental elements of effective security and compliance management

The security business model

The SBM is an overarching model that ties all the elements together to obtain business support for security strategy. This model defines the objectives and how core processes are structured to deliver maximum value, and supports how the organization's frameworks and models are aligned. (We described this concept on page 12 of the 2020 PSR.) The SBM precedes all other security management activities — for good reason. It appears first because you need it to secure investment in the other activities, and it ties the other elements of the canvas together to present the perspective and input needed for decisions and activities in each of the four pillars that follow.

Data security and compliance must be addressed at a strategic management level. For the strategy to get off the ground and succeed (which, in broad terms, means the achievement of sustainable control effectiveness across the control environment), it requires investment in resources. Resources include the time, budget and people to develop processes, capabilities and documentation. Unless

a CISO can secure resources, time and efforts spent on developing a security strategy, improving the security operating model, and implementing security frameworks and programs will be and will remain an uphill battle that is neither sustainable nor effective. Securing investment from the business is an essential first step and requires a compelling case made by the CISO that clearly articulates the value proposition of security and compliance. Some CISOs need to make this case once a year or less, while others may need to do so more frequently. To do so with confidence requires consistency of quality input. It requires groundwork. This is why it's so essential to have an up-to-date SBM strategy and SOM, as well as a target security operating model (TSOM).

The SBM documents how the core elements of the security organization will serve the business and stakeholders to improve value. The typical components of the SBM include a documented description of the following:

Value proposition
Spells out the offer or promise that the security and compliance team is making about the projected outcomes and returns on investment to the mission stakeholder, and the core strategy for profitably doing business.

Goals and objectives
Provides strategic and program goals and objectives that support sustainable security control effectiveness and efficiency of operations.

Strategy
References the security and compliance strategy that defines the focus — the application of resources to achieve prioritized goals and objectives.

Resources
Describes the in-house and third-party resources and stakeholders with whom the organization will interact, highlighting the mission stakeholders. It includes a description of the security and compliance products or services, anticipated expenses and resulting financial model (income statement and balance sheet), taking into account size and growth ambitions and constraints.

Architecture
Documents the structure and organization of security and compliance in relation to the rest of the business, and references the selected operating model (such as POLISM, explained below), support and frameworks.

Operations
References the SOM and TSOM, and the organized and concerted activities that will make it possible for the organization to deliver on the strategy and value proposition.

Culture
The pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things and their influences on security and compliance.

Regulations
Voluntary vs mandatory regulations and legislation; direct and indirect alternatives of compliance.

Risk management
Describes how the business culture, and the chosen risk management approach, mitigates the causes that introduce risk that impact the SBM. Defines how the operating model supports risk management, i.e., the execution of decisions based on the identification, evaluation and forecasting of possible events or circumstances that can have a negative influence on assets and compliance with regulations.

Governance
References the governance of security and compliance — the way an organization is directed and controlled to reach goals. Specifies the limits in which security and compliance teams operate. Implements processes to monitor performance, ensuring that goals and objectives are determined and defined, ascertaining that risks are managed appropriately and verifying that business resources are used responsibly.

A well-documented and well-presented SBM is indispensable in helping to address the security program at the strategic or business level. The model allows security managers to gain a broad view of what is happening in the enterprise, enabling them to better treat information risk and improve decisions, while assisting senior management in meeting its goals.

The security strategy

The corporate security strategy is ultimately concerned with formulating and communicating the careful selection and prioritization of defined goals and objectives and the allocation of resources toward their achievement. This, in turn, guides the approach to the design, execution and management (operation) of security and compliance program activities. Therefore, security strategy sits between the business model and operating model for a reason. The strategy defines the focus—the application of resources to achieve prioritized objectives. The operating model then makes it possible for the organization to deliver the strategy and value proposition. Security strategy is seldom effective without support from a SBM and SOM. Input from a documented security business model is essential to the development of an effective strategy. What is missing in many organizations is the communication of the business model for security and compliance to the stakeholders. Many security strategies are not supported by a sound security business model that ties the design, strategy and operations to the core processes, which in turn ties the people, processes and technology together. CISOs need to get better at defining the business model and their strategy, to explain to the board how data security and compliance generate value for the organization. Therefore, the strategy must be properly aligned with the security business model. This helps to secure needed investments and resources for long-term sustainability.

Lack of this alignment is the first issue with strategy execution. The process of aligning an organization's structure, resources, decisions and actions with its strategy and business environment is needed to support the achievement of strategic goals. Just having a strategy isn't enough; by itself, it may have no real effect on the performance of your security program.

Most organizations can and should improve their capability to design, integrate and execute security strategies. Reviewing strategies only one day per month is not sufficient to properly engage the right people on strategy design and execution. Organizations can benefit from spending a lot more time on strategic security-management capability development. This helps prevent strategic management from being an oversimplified process that results in prioritizing the wrong objectives: not knowing how to accurately determine which approach and controls will provide the best protection to support the robustness and resilience of the control environment.

The security operating model

The SOM is the coordinated collection of security capabilities, organizational structure, assets, people, technology, partnerships and governance used to effectively deliver the data security strategy. An operating model[38] focuses on the delivery element of the business model and strategy. It's the connective fiber between strategy and execution, and a visual representation of how an organization structures its processes to deliver value to its internal and external stakeholders.[39] Operating models, which may also be called value chain maps, are created to help employees visualize and understand the role each part of an organization plays in meeting the needs of other components. There are common taxonomies to present the elements that make up an operating model in different ways, such as: 1) PPT = People, Process and Technology; or 2) POT = Process, Organization and Technology; or 3) POLISM = Processes, Organization, Locations, Information, Suppliers and Management systems.

These models support the diagnosis (what is causing the performance problems) and solutions (where, what and how to change). Operating models are useful tools for helping managers understand how changes to one part of the organization might impact the value to other parts. Therefore, the SOM is one of the tools a CISO and steering committee should use to help them formulate and execute the security strategy.

---

38 For a better understanding of operating models, see: "Operating model," Wikipedia, https://en.wikipedia.org/wiki/Operating_model
39 "What is operating model?" WhatIs.com, https://whatis.techtarget.com/definition/operating-model

Well-defined operating models should include six elements ("POLISM"):[40]

- **Processes and activities.**
  A clear specification of the work that needs to be done
- **Organization and people.**
  The people doing the work and how they are organized
- **Locations, buildings and other assets.**
  The places where the work is done and the equipment that supports the work
- **Information.**
  The software applications and databases needed to support the work
- **Sourcing and partners.**
  Those outside the organization supporting the work
- **Management systems.**
  The planning and performance management of the work

The following adapted description of an operating model is defined by Hult Ashridge executive education:[41]

- The core processes that are needed to create and deliver the products or services that provide data security and compliance to the stakeholders
- The people needed to do the work, and the offer that will attract and retain these people
- The organization structure, decision rights and accountabilities needed to govern and support the people
- The information systems needed to execute and support these core processes

Security operating model presentation

1. **Stakeholder map**
2. **Stakeholder relationships**
3. **Organization chart**
4. **Geographical map**
5. **Organizational process map**
6. **Security sevices processes**
7. **Network architecture map**
8. **Capability map**
9. **Data management map**
10. **Functional responsibility map**
= **Combined operating diagram**

Figure 4. Components to include in SOM visualization (maps)

- The processes needed to support the core processes, such as financial or Human Resources processes
- The suppliers needed to support the processes, and the supplier agreements needed to keep the most important suppliers engaged
- The calendar of management meetings and scorecard needed to run the organization
- The cultural context that will help the people be effective
- The locations, buildings and ambiance where the core and support processes will be executed

For more information on the business model canvas and operating models, see the Verizon 2020 PSR, page 52.[42]

40 "Designing Operating Models," Ashridge Strategic Management, Sep 9, 2019,
    https://execed.economist.com/ashridge-strategic-management-centre/designing-operating-models-2019-09-09
41 For more information on the business model canvas and operating models see: "Business Models and Operating Models," Andrew Campbell, Hult Ashridge Executive
    Education, Feb 24, 2014, http://ashridgeonoperatingmodels.com/2014/02/24/95/ and Andrew Campbell, Mikel Gutierrez and Mark Lancelott, Operating Model Canvas,
    Van Haren Publishing, 2017, www.operatingmodelcanvas.com
42 Verizon 2020 PSR, page 52, which explains the benefits of a SOM.

Security frameworks

Security frameworks present a support guide for the security and compliance management system. The selected frameworks drive the structure of the security program and its projects. Many organizations do not fully implement the frameworks. Refer to page 55 of the 2020 PSR for details on a selection of control, program, risk and governance frameworks.

Recognizing that data protection is not an IT issue, leadership should ensure that the enterprise develops, adopts and implements appropriate sets of security frameworks. It's common for organizations to adopt more than one framework in order to meet various required governance, risk and compliance initiatives.

Security program and projects

The security and compliance management program delivers the outcomes through the collective oversight and management of projects. Establishing and maintaining management at a program level (as opposed to individual project management) helps to direct and ensure the achievement of long-term goals and objectives that can only be realized when they are collectively managed as a program. We devoted the 2018 PSR to reviewing the components and success factors of security management programs.

In the goals section above, the importance of goals is reviewed. When formulating your security compliance goals, it's very helpful to understand the scope and elements of security management—which is why The Security Management Canvas is introduced for perspective. It frames the scope of activities (incorporated as objectives) and the requirements for establishing the conditions needed to achieve your goal.

Systemic change for lasting success

The approach that organizations take with security and compliance has to evolve to meet today's sophisticated threats. To be prepared to meet these new requirements, organizations need to develop a rich, contextual picture outlining what they want in terms of security and compliance. The development of mature data security and compliance processes and capabilities needs to speed up—significantly.

Framework types

The four main types of security frameworks are:

1 Control frameworks, such as NIST 800-53; CIS Controls (CSCs); PCI DSS with a catalog set of baseline security controls

2 Program management frameworks, such as ISO 27001; NIST CSF

3 Risk management frameworks, such as NIST 800-39, 800-37, 800-30; ISO 27005; FAIR

4 Governance frameworks, such as ISO/IEC 27002, COBIT, COSO

The PCI DSS is a security control framework. It is not a program, risk management or governance framework.

Several security and compliance issues that organizations suffer from today can be traced back to the origin of the PCI compliance regulation. During the first 10 years of PCI DSS (2004 to 2014), the need to comply with PCI DSS was perceived as a significant disruption for many organizations, and in many cases met with resistance. At the time, many organizations did not have well-developed models for their security and compliance into which they could simply integrate PCI DSS requirements. Many still do not have this capability today. They lack established GRC practices, where PCI compliance can be achieved by integrating the baseline set of PCI DSS controls into an existing mature control environment.

Most organizations' strategy and program management approaches seem to have evolved organically, without a deliberate and focused attempt to design a security and compliance operational model that includes crafted frameworks for governance and management.

During the first 10 years of PCI DSS, a high degree of training and education was needed merely to understand compliance requirements and interpret them correctly. A common approach was, and still is, for a project manager to be appointed and tasked with initiating and managing a PCI compliance project. That person then assigns tasks to people inside the organization and tracks progress.

But project managers can quickly find themselves overwhelmed by the sheer volume of back-and-forth communication, the amount of time needed for team education and the pressure of keeping internal assessments, remediation and the development of compliance evidence on track. They are also often burdened with repeatedly evaluating compliance evidence, providing feedback, improving low-quality and insufficient evidence, etc. The need for automated compliance management and structured, ongoing scope reduction inevitably becomes obvious.

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

When first-order changes do not suffice

Many security experts note that the superjacent and underlying reasons why organizations don't achieve sustainable control effectiveness never seem to change. The same problems and challenges keep recurring, and the fixes don't stick. Interventions that solve an immediate problem often cause other problems elsewhere in the system, or they don't last. Within PCI compliance and control environments, multiple causes often contribute to the issues organizations experience. The conclusion is that first-order changes will not suffice, and higher-order changes are needed.

The introduction of PCI DSS v4.0, with its greater emphasis on objective-based, evidence-backed continuous improvement, may change this situation over the next decade. Organizations will need to make changes to improve their data security and compliance. Some of those changes will be minor and incremental; others will be major, requiring substantial effort and causing disruption. How change is approached can determine whether it is perceived as a positive, much-needed investment or as a harmful and disruptive imposition.

While all improvements are changes, not all changes are improvements.

What is the level of change that your organization wants versus the level of change needed?

That depends on the goal that you are after.

First-, second- and third-order changes to achieve continuous improvement

Here is a brief summary of the distinctions between first-, second- and third-order changes.

First-order changes
These changes work within an existing structure and include changes consistent with the currently existing, already present operations model. You could view it as tinkering with the system—doing more or less of something, making an existing process better or more accurate, and creating incremental changes. For example, making an existing PCI security process and component better or more accurate. First-order changes are easier to make because people are tempted to look at the symptoms and the single, immediate cause of a problem, rather than consider the system as a whole. Sometimes first-order changes work and the efficiency of the system improves. They are most likely to be successful where the problem has a single cause. However, implementing a new security and compliance strategy and achieving continuous improvement requires complex second- or third-order changes.

Second-order changes
Second-order thinking is an umbrella term for considering the downstream consequences of first-order thinking to the second, third and nth order. In the game of chess, this would be akin to thinking many steps ahead, considering the options for moving pieces on the board and how alternative actions could bring about better outcomes. Any misstep, such as going straight for the king, will have a ripple effect of consequences for the rest of the game.

With first-order changes, every action has a consequence. In second order, every consequence has its own consequence. These changes are transformational and seek to alter the operations model. They involve seeing your control environment differently, challenging assumptions and working from a new and different viewpoint. They can be disruptive or discontinuous. Inevitably, they trigger new ways of doing things, evolution of values and goals, and often structural changes in the organization. In many organizations, second-order change attempts are designed to "phase in" updated security operations models and "phase out" others. Changing some aspect of a complex system always introduces second-order effects (consequences). When second-order changes are made, the secondary consequences may seem obvious, but systems are almost always more complex than expected. In an information security control environment, as in a game of chess, the possibility of space is huge. We can consider a simple scenario where we pretend that any change to a cardholder data environment (CDE) security control or control system has only three possible consequences. Thinking about consequences of consequences means we have to consider nine possibilities. Thinking one order higher grows our possibility space exponentially. In the real world, every action has many more possible consequences than three, so every consequence has even more consequences to consider. Second-order consequences include "unknown unknowns," so there is no way to account for every possibility. There will always be unanticipated consequences, no matter how hard we try. But it is beneficial to recognize possible second- and third-order consequences early in the decision process, and implement changes accordingly.

Third-order changes

These changes operate from questions rather than answers—when an organization is willing to question and change its beliefs and culture. Continuous improvement is essential in a constantly evolving world, and this is even more important with the introduction of PCI DSS v4.0. Continuous improvement, by definition, is a process and not merely a state change. Depending on the implementation, a second-order change may still result in merely substituting one state for an improved one. However, an organization committed to continuous improvement requires third-order changes, which are process and systems changes, not merely a state change. A third-order change aims to help the organization's members develop the capability and capacity to identify and effectively change their own strategy and operations model as they see fit, to achieve optimal performance and expected results.

While a second-order change requires a consultant (such as a QSA) to advocate a particular interpretation of requirements, events and downstream consequences, a third-order change requires the consultant to help the organization develop the ability (with the application of proven methods and techniques) to determine when second-order change is needed and then to help implement it.

Thinking is hard. People do quite a lot to avoid it.

Leadership skill requirements

Wise security professionals, particularly CISOs and security steering committee members who know how to present themselves and their data security and compliance situation well, get buy-in for the investments they need to develop and advance their security strategy and programs. They obtain leverage when they know how to evaluate their security strategy and program strengths and communicate them well. These are leadership skills. Individuals and teams that fall short in presenting their success in managing data protection generally fall behind and lose opportunities.

Maintaining up-to-date security business models and security operating models, and mapping out the 7 Constraints, are essential steps to presenting a clear, logical visualization of the control environment. They enable organizations to analyze data security compliance complexities and formulate a coherent, logical and tight strategy that addresses the root causes of poor security and compliance performance. Organizations that apply a structured, logical approach, with second- and third-order changes based on sound reasoning, will be able to define the steps needed to achieve their goals and create a rigid process to expose faulty assumptions and conflicts. In short, they'll develop the ability to uncover and explain root causes and formulate solutions.

The application value of TSMC

CISOs and compliance program managers require clear visibility into the progress of their efforts, and how it relates to the accomplishment of objectives and the stated security and compliance goal. They are often guided (and in some cases misguided) by the dashboards, models and frameworks chosen to frame their view of the control environment and order the steps toward the goal. The methods applied to structure the workload significantly impact the strategy and program engineering and how the performance is measured. Remember

the saying "What is measured gets done?" That includes the goals, related objectives and requirements for meeting those objectives. The frameworks, methods and "dashboard metrics" applied to security and compliance are immensely important, yet many organizations don't give this sufficient thought. A lack of research and insights in this area can make it difficult to determine the range of available options and define best-in-class approaches.

CISOs require simple, effective methods to organize the most important facts into manageable structures and zero in on the ones that enable them to find answers and make sound decisions. This is why Verizon strives to advance research on management methods and promotes models, methods and techniques to simplify and optimize the management process, clarify options, and bring order, structure and repeatability. Our goal is to make the path, the processes and program performance transparent and predictable.

The Security Management Canvas (TSMC) enables teams and individuals to identify the main components and subentities or properties of security and compliance management in one overarching framework. This canvas view helps CISOs understand and clarify relationships among these entities. It reveals how the entities are integrated into a coherent whole, representing either an ideal type or an exemplary security strategy and

program construction. The Canvas view enables individuals to grasp what would otherwise be an overwhelming flow of seemingly disjointed objectives. Such frameworks are much needed, as individuals can process only a limited amount of information at any given time. The frameworks show which components of security management are essential, translating them into objectives and activities and by implication, which objectives to ignore or postpone. For example, TSMC helps teams focus attention on collective issues and ask pointed questions about how they can contribute. It facilitates the designing of strategies and programs, resulting in the ability to pivot to new concerns and diagnose the root causes of performance issues. And it explores how they can be resolved to improve security ROI and compliance.
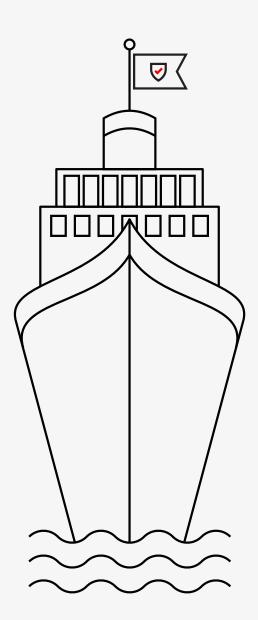
Focus on defining and documenting all five elements of your Security Management Canvas

1. Clearly communicate your security business model—keep it strategic

2. Clearly define and communicate your security strategy—goals and priorities should include sustainability and effectiveness objectives

3. Clearly define and present your documented current and target security operating model

4. Avoid selective application of security frameworks—fully implement them to achieve their benefit

5. Make sure the maturity and support of your security program is underpinned by the other elements of the canvas

Do not neglect these basic steps.

Requirements: The security and compliance hull

PCI DSS v4.0 is the most substantial update made to the Standard in the 17 years since the release of PCI DSS v1.0 in 2004. At first glance, organizations will notice several significant changes introduced by PCI DSS v4.0. While PCI DSS v4.0 doesn't alter the fundamental structure of the Data Security Standard, and it still has the familiar Control Objectives and 12 Key Requirements introduced in 2006, the new version reflects evolving objectives and requirements. This includes wording changes, updates to existing requirements, several new requirements and future-dated requirements.

PCI DSS release timeline

Prior to PCI DSS v4.0, the longest duration between releases of updates to the PCI DSS was PCI DSS v2.0 in October 2010 and the release of PCI DSS v3.0 in November 2013.

	Release	Version	Pages
2004	December	1.0	12
2006	September	1.1	17
2008	October	1.2	73
2009	July	1.2.1	74
2010	October	2.0	75
2013	November	3.0	112
2015	April	3.1	115
2016	April	3.2	139
2018	May	3.2.1	139
2022	March	4.0	360

Historic PCI DSS release timeline

PCI DSS v4.0 is the 10th edition of the PCI Standard. With the release of PCI DSS v4.0 in March 2022, it is nearly nine years since the last major update (PCI DSS v3.0) and four years since the interim update in 2018 (PCI DSS v3.2.1), which made minor changes to the Standard.

These updates reflect significant changes within the payment card industry and account for risks in an increasingly complex, ever-changing threat landscape. In this technological sea change, PCI DSS v4.0 provides new navigation points to help organizations achieve sustainable control effectiveness across control and compliance environments.

PCI DSS v4.0 specifically supports the use of key technologies, including cloud and serverless computing. Organizations that currently apply compensating controls to meet DSS requirements may benefit from determining whether the new PCI DSS customized implementation method is suitable for their specific security needs.

The updated PCI Standard also introduces more flexibility into the wording of the requirements and adds intent statements. On pages 46, 48 and 52, we explore the three most significant updates in PCI DSS v4.0, which are continuous compliance, customized controls and control environments.
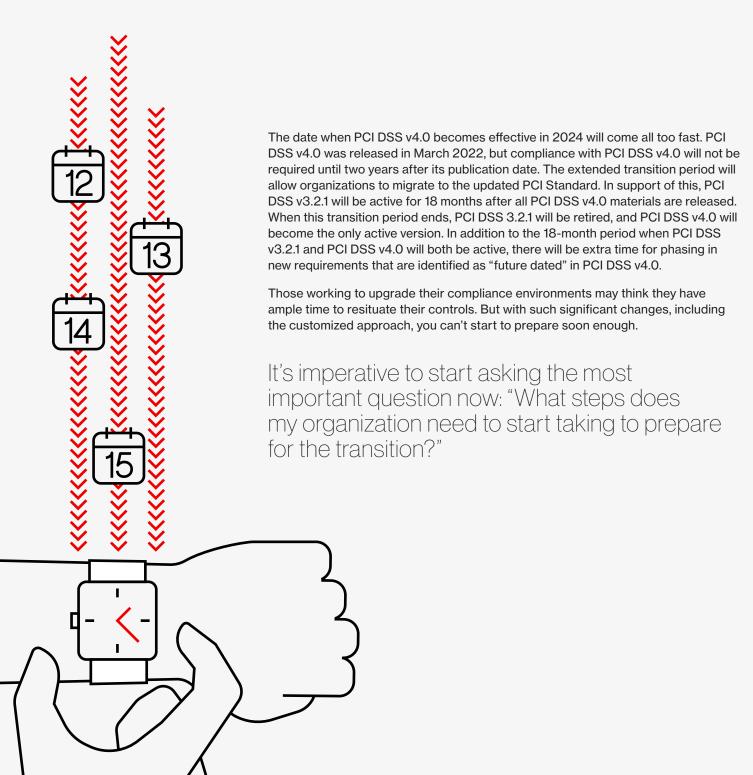
In summary, the most significant reasons why the PCI DSS was updated are to:

- Ensure that the Data Security Standard continues to meet the security needs of the payments industry

- Create flexibility and support of additional methodologies to achieve security

- Address ongoing technology developments in payment systems, mobile, cloud, etc.

- Address ongoing changes in the threat landscape, such as improving protocols and methods associated with validation

- Promote security and compliance as an ongoing process

This revision of the Standard is considered so significant that between 2019 and mid-2021, the PCI SSC fielded an unprecedented amount of feedback from participating organizations and assessors on the PCI DSS v4.0 draft. For past revisions of PCI DSS, formal feedback opportunities for the participating payment card community were limited to a single period. For PCI DSS v4.0, the PCI SSC expanded the feedback opportunities to maximize collaboration and stakeholder involvement in updating the Standard.[43]

---

43 See PCI Security Standards Council, PCI DSS v4.0: Anticipated Timelines and Latest Updates,
    https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates
    https://www.pcisecuritystandards.org/about_us/press_releases/pr_10242019
    https://www.pcisecuritystandards.org/get_involved/request_for_comments

Preparing for
PCI DSS v4.0 ....▶

The date when PCI DSS v4.0 becomes effective in 2024 will come all too fast. PCI DSS v4.0 was released in March 2022, but compliance with PCI DSS v4.0 will not be required until two years after its publication date. The extended transition period will allow organizations to migrate to the updated PCI Standard. In support of this, PCI DSS v3.2.1 will be active for 18 months after all PCI DSS v4.0 materials are released. When this transition period ends, PCI DSS 3.2.1 will be retired, and PCI DSS v4.0 will become the only active version. In addition to the 18-month period when PCI DSS v3.2.1 and PCI DSS v4.0 will both be active, there will be extra time for phasing in new requirements that are identified as "future dated" in PCI DSS v4.0.

Those working to upgrade their compliance environments may think they have ample time to resituate their controls. But with such significant changes, including the customized approach, you can't start to prepare soon enough.

It's imperative to start asking the most important question now: "What steps does my organization need to start taking to prepare for the transition?"

Supporting data security by aligning your goals

The PCI SSC created the standardized compliance requirements to help organizations develop habits of data security best practices. The intent of the PCI DSS is for requirements to be consistently followed to better align, design, prioritize, implement and maintain goals that result in an effective, sustainable control environment. This intent may be more explicit than what was recommended in previous versions of the PCI Standard.

Since the release of PCI DSS v1.0 in 2004, most organizations continue to struggle with achieving and maintaining effective, sustainable payment card data security. Those that succeed in maintaining all their PCI DSS requirements year-round—rather than ongoing remediation for the sake of passing an annual assessment— implement a strategy and design based on sustainable, well-developed goals. That's because once you clarify your goals, you can more easily implement a custom control and validation design.

PCI DSS v4.0 places increased emphasis on this transition to security as a business-as-usual culture, including increased gathering of validation information over a period of time to encourage continuous security processes.

Correcting the slow implementation of sustainable control environments

Payment card data is one of the most highly sought after data types by external and internal threat actors, because it's one of the easiest data types to monetize. Yet, even within these highly sensitive environments, organizations remain slow to implement strategies that result in sustainable control effectiveness.

Many move into action only when:

- There is a real pressure to improve, typically in the aftermath of a confirmed payment card data breach

- It finally becomes obvious to organization leadership that there's no remedy within their existing security and compliance paradigm; they have tried everything else without results

- Professional help is introduced to help the CISO and steering committee accomplish first steps, with a clear outline of a how-to strategy that focuses on the right things, in the right manner, at the right time

Managers and their teams are generally so overwhelmed with security and compliance challenges that they tend to concentrate on corrective actions they know how to take—not necessarily ones that should be corrected. But PCI DSS v4.0 introduces requirements for ongoing compliance and improvements.

For the application of PCI DSS v4.0 to improve processes and be effective, organizations must first know what to change. Many different approaches to designing the management of a compliance program exist. The key question is: Which is most effective and efficient?

To make those decisions, teams need a high-quality, repeatable process with a clear understanding of the correct priorities, and the requirements and conditions necessary to achieve the objectives that lead to the end goal.
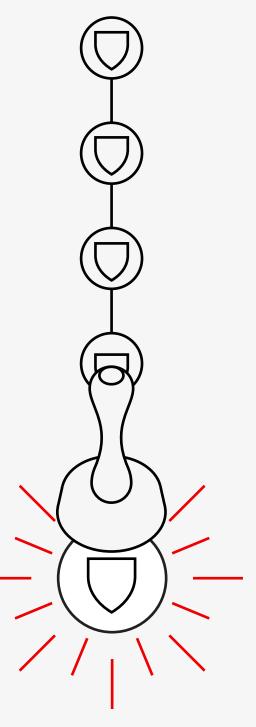
As discussed in the previous section, it's very important for organizations to carefully consider the actual goals of their GRC program, their security and compliance program strategy, and supporting programs. It requires time and effort to design goals and communicate them with clarity. This leads to the next important step in the process: the requirements for achieving the goals. Without clarity on what the success factors and necessary conditions are to attain the goals, organizations are far less likely to achieve them. On page 86, we discuss what the goal of a PCI security compliance program should be.

The lack of clear goals and a keen strategic defense plan leads to permeable security design. CISOs and security managers need to take time to mull over their organization's specific needs and problem-solve solutions, rather than rush straight into implementing the new requirements. Each new and updated requirement should be carefully examined. Before project managers assign tasks to resources, they need to understand

Developing sustainable control design solutions

the scope of the project—the goals and objectives, their requirements and constraints.

Well-designed data security and compliance solutions too often become secondary or tertiary considerations as security planners and technicians scramble to address staffing shortages and a plethora of email alerts. Annual compliance validation projects may be perceived as successful simply because controls not in place were remediated to receive the coveted final annual DSS Report on Compliance (ROC). This approach falls far short of meeting the intent of the PCI DSS.

Enhanced validation methods and procedures

Major changes introduced by PCI DSS v4.0 include enhanced validation methods and procedures, which evolved from a defined-only approach to include an objective-based customized approach. The PCI SSC announced the plan to introduce these enhanced validation methods and procedures into PCI DSS v4.0 at the 2019 Community Meetings.

The traditional defined approach is the familiar method where required security controls must be implemented when applicable. Requirements need to be met in a very specific manner and validated, sometimes regardless of the actual control outcome, such as whether or not the control system in question is actually effective and sustainable. This method for validating PCI DSS won't be going away with PCI DSS v4.0. But the new customized approach allows organizations to use security methods that differ from traditional PCI DSS requirements, as long as they can demonstrate that they meet the intent of the relevant PCI DSS requirements and can validate its effectiveness.

Within a PCI DSS compliance assessment, organizations can choose either or both of the approaches on any of the key requirements. For example, PCI DSS v4.0 allows organizations to take a hybrid approach: They are allowed to meet some requirements by following the defined approach and other requirements by following the customized approach. Even within a single DSS requirement, the defined approach and customized approach can be split to meet different aspects of the requirement, as long as the organization meets the security objective of the requirement. However, be aware that some requirements explicitly cannot be met using the customized approach.

The defined approach

The defined implementation refers to the existing traditional approach to security control implementation and compliance validation that has existed since the introduction of the PCI Standard. The sets of requirements, controls and test procedures are fairly prescriptive. The PCI Standard includes descriptions of the controls that need to be in place and how the validation testing procedures should be met.

The defined approach simply means that organizations follow the current requirements and familiar testing procedures as written in the PCI DSS. This approach remains valid. All organizations can continue to benefit from its prescriptive directions. Many organizations may not see any need to follow a customized approach to meet the control objectives.

The customized approach

The customized implementation allows organizations to follow a tailored process to custom-design security controls or adopt other controls outside of the familiar defined list of requirements. This new approach of validating PCI DSS controls focuses on an outcome-based approach, rather

than a must-implement-based one. As mentioned earlier, all customized controls must still meet the stated security objective of the requirement.

Requirements and validation options in PCI DSS v4.0 focus on security objectives and support organizations using different methodologies to meet the intent of PCI DSS requirements. The PCI Standard includes objective statements that clearly identify the security outcomes that customized implementations must meet. The control intent statements specify and clarify what needs to be achieved, with greater flexibility in how the organization completes the desired security outcomes.

The customized approach's greater flexibility allows for implementation of security solutions and technologies that don't require waiting for the PCI DSS

to catch up. Validation methods focus more on specific security outcomes, giving organizations the ability to prove the effectiveness of their approach.

This alternate approach allows organizations to customize their approach and develop security controls by meeting several criteria:

- Determine the controls for a given security objective
- Submit detailed documentation to the QSA, outlining the approach to achieve compliance and demonstrate the effectiveness of the approach
- After the QSA reviews the evidence, the QSA makes a final decision on the effectiveness of the control, based on the analysis of the documentation submitted

A customized approach typically requires additional documentation effort for:
- Control design, with evidence that it meets the control objective and intent
- Internal control testing
- Control risk
- Control performance
- Control effectiveness
- Control maintenance
- External control compliance validation testing procedures

The impact of a customized approach

Customizing security controls should be done in a very structured way that delivers measurable and predictable outcomes.

Organizations with mature control environments are more likely to embrace the new customized validation approach with confidence. They should also find it easier to rewrite how their systems can be tested to validate how they meet the latest PCI DSS requirements.

The new validation method will likely result, at least initially, in additional assessment work for organizations to develop and prepare documentation, control design, evaluations and risk assessment data that a QSA will need to evaluate.

Although this new validation approach offers more flexibility in how the PCI DSS 12 Key Requirements can be met, there's an explicit expectation that organizations ensure that each of their customized implementations of PCI DSS requirements meet respective control objectives and fulfill the intent.

As such, a customized approach requires adopting a robust method of designing and managing security controls and maintaining the control environment. It requires higher levels of process and capability maturity of control design, control risk evaluation, control implementation and monitoring.

Organizations need to collaborate with the QSA or Internal Security Assessor (ISA) to agree on and develop tailored testing procedures. Some organizations are likely to experience unintended consequences from the design and implementation of their customized controls. It's critical to be aware of blind spots and seek out cause-and-effect relationships between controls, control systems and the control environment. You need to understand your capability and competency to design, implement, maintain and monitor customized controls, as well as your capacity to maintain all the requirements associated with your approach. The new alternative approach may not be for everyone. It's best suited for organizations with fairly mature security, compliance and risk assessment processes in place.

When choosing to follow the customized approach, organizations that don't have a robust control environment backed by reasonably mature compliance management processes and capabilities are advised to improve their level of maturity and implement changes in small, incremental steps. This avoids making changes to substantial portions of the control environment, which can lead to unintended consequences— a range of good, mixed and bad unexpected outcomes.

For an overview of capability maturity and metrics, revisit the Verizon 2019 Payment Security Report, pages 21 to 29.[44]

The new alternative approach may not be for everyone. It's best suited for organizations with fairly mature security, compliance and risk assessment processes in place.

---

44   2019 Payment Security Report, Verizon, 2019, https://enterprise.verizon.com/en-au/resources/reports/payment-security/

Examples of unintended consequences

Unintended benefit: The creation of email

Described as windfalls, good fortune, luck or serendipity, unintended benefits result from an unexpected positive outcome in which no significant, clear-cut drawback or perverse result occurs. For example, when the internet was first designed, email programs were never intended to become extensive communications channels. However, their extreme popularity, practicality and ability to be sustained definitely pegs this innovation as an unintended benefit.

Unintended drawback: LED traffic lights

The world's first electric traffic signal was put into place in Cleveland, Ohio, on August 5, 1914.[45] Today, traffic lights are one of the most common and effective traffic-control tools available. But they can also cause accidents when they go out.

Recently, cities around the globe sought to increase the energy efficiency of traffic lights by switching from incandescent bulbs to long-lasting light-emitting diode (LED) bulbs, only to discover a new set of problems. It's an apt example of how proposed changes to controls should be carefully studied; environmental factors must be taken into account to uncover unintended consequences.

Local and state governments in the U.S. began replacing incandescent traffic-signal light bulbs with LED lighting in response to the United States Energy Policy Act of 2005 minimum standards for energy efficiency for traffic and pedestrian lights. While the efficient and longer-lasting LED bulbs improved energy costs by 90%, when incandescent bulbs burn out, they go out completely without warning. On the other hand, LEDs often go out in parts, leaving part of the string of LEDs inside the traffic light operative and emitting light. Drivers then alert the authorities, who send out a crew to replace the failing light.

However, since LED lights don't emit heat, they don't melt snow the way incandescent light bulbs do. The changing directional lights can become obscured with snow and ice buildup, according to a 2014 U.S. Department of Transportation Federal Highway Administration study. Partial or complete covering of the signal with snow and ice resulted in at least one fatality and numerous vehicular accidents. Drivers unfamiliar with an intersection may not notice the covered lights, which can lead to potentially devastating collisions.

Efforts were made to address the problem by installing weather shields and snow scoops to reduce or resolve accumulation. Some city workers also used compressed-air devices to blow the snow off and manually scraped the lights. Local and state governments argued that drivers should respond to such obstructed LED lights in the same way they do for a power outage—by treating the traffic signal as a four-way stop.[46] While some might argue that the environmental and energy-saving benefits outweighed the unintended drawbacks, the main purpose of the LED lights was to protect human lives and avoid accidents. Therefore, the LED lights also could be viewed as having a perverse result.

---

45   "First electric traffic signal installed," History.com, Nov 2009, https://www.history.com/this-day-in-history/first-electric-traffic-signal-installed.

46   David Noyce, "Traffic Signal LED Module Specification Workshop and Informational Report for Snow Conditions," U.S. Department of Transportation, Federal Highway Administration, Jan 2014, https://ops.fhwa.dot.gov/publications/fhwahop13010/index.htm

Unintended drawback/perverse result: Passenger-side airbags

Sometimes an unintended consequence crosses over and cannot be clearly identified as either a benefit, drawback or perverse result. An example is passenger-side airbags created as a safety device in cars in the mid-1990s. The devices inadvertently led to an increase in child injuries and fatalities. When the air bags automatically deployed in a crash, small children were injured or killed from the impact. Child seats were then moved to the back seat of the vehicle to avert this outcome, but that led to an increase in the number of children being left unattended in extreme temperature conditions. While passenger-side airbags definitively save lives, the perverse result on small children cannot be ignored.[47]

Perverse result: The cobra effect

Colonial Delhi, India, was suffering from a proliferation of cobras, so the local government placed a bounty on them. Ironically, this resulted in an increase in the species. As the cobra population fell, people started raising cobras in their homes, which they would then kill to collect the bounty.
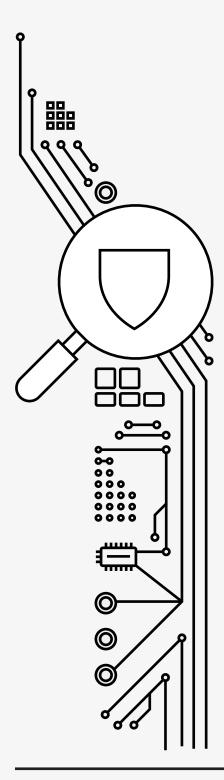
Local authorities eventually realized that while very few cobras were evident in the city, a bounty was still being paid on large numbers of snakes. So, they canceled the bounty. In response, the people raising cobras in their homes released all of their now-valueless cobras back into the streets. In the end, Delhi had a bigger cobra problem after the bounty ended than it had before it began. The unintended consequence of the cobra eradication plan was an increase in the number of cobras.[48]

47 "Airbag," Wikipedia, https://en.wikipedia.org/wiki/Airbag
48 Antony Davies and James R. Harrigan, "The Cobra Effect: Lessons in Unintended Consequences," Foundation for Economic Education, Sep 6, 2019, https://fee.org/articles/the-cobra-effect-lessons-in-unintended-consequences/

Continuous monitoring, internal assessments and validation

A key component of PCI DSS v4.0 is the importance of continuous monitoring of the control environment, and continuous compliance with PCI DSS requirements. Organizations need to develop performance metrics to measure effectiveness and resilience of their security controls and the control environment. In terms of control resilience, a clear capability must exist and be exercised for all security controls to be continuously monitored across the cardholder data environment (CDE) to ensure they are operating effectively and as intended. All failures in security controls must be rapidly detected and promptly responded to in order to restore the security control, identifying the cause(s) of failure and addressing any security issues that arose during the failure of the security control. Evidence that this process is effective needs to be presented during compliance validation assessments. Critical to those procedures are standards of evidence (evidence criteria) and evidence assessment.

Evidence assessment

A typical evidence review process conducted by an assessor involves:

1. Designing the independent (QSA) assessment procedures or tests. For customized control implementation, this includes the evaluation of the tests and procedures that are specifically designed to validate customized control implementations—in terms of risk analysis, meeting the requirement objective and its ongoing effectiveness, and evaluating the validity of the evidence presented to support this

2. Gathering evidence and carrying out the independent assessment procedures or tests

3. Analyzing evidence and evaluating it against evidence validity criteria (see page 54), evaluating DSS requirements performance against the assessment validation criteria, drawing conclusions; making decisions about whether additional information is required and can be obtained (go back to Step 1 above) or if sufficient, appropriate evidence exists to determine with reasonable assurance the compliance condition of the DSS requirement in question

PCI DSS compliance validation evidence assessment and acceptance

The assessor is required to critically evaluate evidence of compliance. This requires set standards to enable the consistent evaluation of evidence against established evidence acceptance criteria. Validation procedures for compliance evidence typically include documentation that explains the design of the security control, its operation, and a documented set of tests designed to confirm the effectiveness of the control's ability to meet the intent of the relevant control objectives. Test procedures preferably should be developed jointly, approved and agreed upon by the assessed entity and the QSA, prior to the assessor's evaluation of each customized control.

The QSA will make firsthand observations of the control environment, conduct interviews and request documents from the assessed entity. The assessor will then abstract the information to obtain evidence to support the conclusions of the assessment findings. The strength of the evidence will depend on the evidence type—distinguishing between primary (firsthand) and secondary (secondhand) sources of information. The documentation

collection and review generally includes policies, standards and procedure documentation, documented control design profiles, asset inventories, configuration files, audit logs, data files, training records, etc. Ideally, there should be documentation for all elements of the security operating model (see page 35) and The Security Management Canvas (see page 33).

Evidence validity criteria

Assessors are required to exercise professional judgment and skepticism when evaluating the quantity and quality of evidence, and thus their sufficiency and appropriateness. Determination of the adequacy with which a control conforms to the intent of its relevant control objective(s) is based on evidence presented that meets evidence validity criteria. Evidence can be considered valid when it consists of data that is judged to be both appropriate and sufficient—both measures of the quantity of evidence. The sufficiency and appropriateness of evidence are interrelated. The evidence collected has to be enough. How much is considered enough depends on standards of evidence provided by the PCI SSC (such as sampling standards included in the DSS), standards established by the assessor and the circumstances of the engagement. In general, the higher the

quality of evidence presented, the less may be required. Merely obtaining more evidence may not compensate for its poor quality.

The basic criteria and main test to determine if evidence is acceptable is the triangulation between the validity, reliability and accuracy of the evidence presented. Therefore, evidence collected is considered appropriate when it's evaluated by the assessor and determined to be 1) relevant to the assertion being tested, 2) from a reliable source and 3) accurate. Each of those evidence validity criteria with their associated qualities is further explained below.

Evidence validity

1. Relevance

Evidence presented during a PCI DSS compliance validation assessment must have credible relevance to the DSS requirement, or relate to dependent compliance requirements (the control system in question). The evidence should be evaluated in the context of the CDE and overall control environment. Evidence that has no relevance or relation to the control system in question and the CDE is deemed unacceptable. In other words, the artifacts (evidence) presented must support the existence of any fact that is of consequence to the determination of compliance status of a control and control system (i.e., in place, not in place, compensated, not applicable, control effectiveness, etc.) and substantiate the effectiveness of the operation and management of the control system, its robustness and its resilience. This fundamental test of the relevance of an artifact and its associated facts is that its inclusion must make the determination of compliance status more probable when included, and less probable when excluded. This is especially important for creating test procedures for the validation of PCI DSS v4.0 customized controls to help establish the lower and acceptable upper boundaries of the amount of evidence that can be considered "sufficient."

2. Reliability

The ability to test the reliability of evidence must exist: the origin, accuracy, authenticity, age, ownership, trustworthiness and dependability of the artifact/data. Reliability is the extent to which the assessor can confidently rely on the source of the data and, therefore, the data itself. Reliable data should be considered dependable, authentic, trustworthy, genuine, reputable and consistent. Evidence is considered more reliable when it's obtained from independent sources, in documented form (original documents) and corroborated from different sources, as compared to evidence that is obtained indirectly or by inference. Therefore, the reliability of evidence is influenced by its source and nature, and its dependence on the individual circumstances under which it's obtained.

3. Accuracy and completeness

Accuracy refers to the degree to which the evidence presents data, measurement, calculations or specification with true, precise values. The evidence presented must be clear and complete. The evidence must be reasonably free from mistakes and errors and conform to the correct values in terms of detail, such as dates, numbers, names, locations, etc. The reliability of the data obtained from a sample will increase as the sample increases in size toward that of the whole population. In general, it's the size of the sample that determines its accuracy: The size of the population is less relevant. In terms of statistics, doubling the size of the sample will not double the reliability of the information. Accuracy is proportional to the square root of the sample size. So, to double the accuracy, the sample size must be increased fourfold—which will greatly increase the cost of the sample survey.[49] This is an example of the so-called law of diminishing returns (or diminishing marginal utility). It explains why most samples are relatively small.

---

49 Roger Pierce, "Research Methods in Politics: A practical guide," SAGE Publications, Ltd., 2008,
    https://www.sagepub.com/sites/default/files/upm-binaries/17810_5052_Pierce_Ch07.pdf
    Also see ISO 18414:2006—Acceptance sampling procedures by attributes
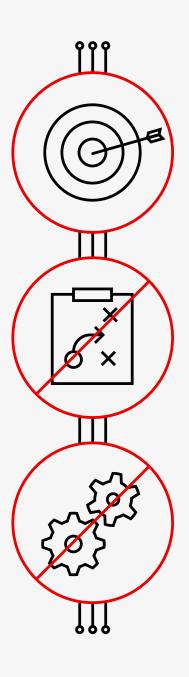
Burden of proof: Positive confirmation vs negative confirmation

The evidence should reflect the whole story. It's not enough to collect evidence that just shows one perspective. The focus of the assessor (validation QSA) is to request supporting evidence from the assessed entity that clearly and convincingly substantiates how and why all compliance requirements are met (positive confirmation), and not to start from a position of assuming full compliance, and then trying to determine where discrepancies may exist, indicating noncompliance (negative confirmation). This is an important distinction on the focus of the assessment approach.

In general, the burden of proof during compliance validation lies with the assessed entity, since it is required for merchants and service providers to provide sufficient evidence to support their claims that all PCI DSS requirements are, indeed, in place. The burden is not on the assessor to attempt to gather evidence of noncompliance. As mentioned, assessors should not generally assume an initial position that the assessed entity is fully compliant, and then attempt to demonstrate noncompliance — instead, the evidence presented should convincingly assert the claim of compliance.

The introduction of a customized approach for control design and validation under PCI DSS v4.0 may depend on the involvement of a remediation QSA in the design and validation of customized controls. It also may introduce a bilateral burden of proof, where some aspects of the burden of proof are shared between the remediation QSA and the assessed entity to produce evidence that the design of customized controls are effective and meet the intended objectives.

The three stages of PCI DSS compliance program failure

Managing the changes introduced by PCI DSS v4.0 can be a demanding exercise, but it need not be a frustrating experience. Insufficient planning is one of the major reasons why projects spin out of control. It can lead to unintended consequences and even compliance program failure. The application of a suitable, comprehensive framework will ensure that expectations are set and assumptions identified, and it will help create a predictable winning outcome, rather than risk and uncertainty.

A program is a cluster of projects and ongoing operations that has a common goal and is managed in a coordinated way so that benefits are achieved, which would not happen by managing the projects individually.

Security and compliance programs can fail in many ways. Multiple reasons exist for poor performance and failure. Program managers must identify and prevent or overcome numerous potential risks prior to and during program execution. PCI security compliance programs demand effective program management to ensure firm control and to maintain alignment between the five components of The Security Management Canvas (discussed on page 32).

Avoid misalignment on goals.

Business and security teams should not have different expectations regarding the goals of security and compliance. Shared knowledge, common understanding and alignment of goals are of utmost importance. All parties must act as a team with a singular vision for success.

The 3 stages of failure[50]

The challenges organizations encounter, and the mistakes that occur during the planning and execution of PCI security compliance programs, can generally be divided into three stages of failure:

Stage 1: Failure of vision
These are "why" mistakes. Participants in PCI security programs fail to understand why they are engaged in PCI security compliance, and what the overall goals are. These "why"-related mistakes occur when leadership doesn't establish a clear direction for security and compliance with a clearly articulated vision of the goals and objectives necessary to achieve the required outcomes. This vision is about achieving and maintaining focus on executing the correct prioritized objectives toward an aligned common goal.

Stage 2: Failure of strategy
These are "what" mistakes. They occur when the CISO and team follow a security and compliance strategy that fails to be designed and executed in a manner to deliver the results they desire. The team may know why they are engaged in a PCI security compliance program and how to do the work, but they still choose the wrong "what" to make it happen. Revisit The Security Management Canvas (see Figure 3, page 33) to help you position the overall approach, and individual components and elements within each of the five domains.

Stage 3: Failure of architecture and design
These are "how" mistakes. They occur when the security team fails to build systems and a security and compliance control environment where sustainable control effectiveness is built into the design and not bolted on afterward. This type of failure also happens when you forget to measure performance and get lazy with the details. A failure of architecture and design is a failure to execute on a good plan (strategy and program) and clear vision. For additional insights, revisit the 9 Factors of Control Effectiveness and Sustainability and review how they should be applied (see the 2018 PSR, page 4).

Generally speaking, program success hinges on two fundamental concepts: a high-quality plan and effective implementation. A PCI DSS v4.0 implementation plan that remains on the drawing board is little more than a concept until the organization implements and moves it from "concept design" to a tangible solution with measurable results. It takes as much specialized expertise to effectively implement as it does to develop the plan. The organization must have the internal program implementation competence or turn to a specialized program implementation partner for support.

Proficiency: Skill and experience matter.
It's common for organizations that undertake the management of large, complex security and compliance programs internally to lack deep knowledge of program management and implementation. Program management and implementation is a highly specialized, technical discipline that usually requires experts to help ensure success. Organizations often don't have this expertise or in-house training because their core business operations are focused elsewhere. If an organization chooses to build and support this core competency internally, intensive education in program management and implementation—including the processes and technical tactics for success—is necessary.

---

50 James Clear, "The 3 Stages of Failure in Life and Work (And How to Fix Them)," JamesClear.com, https://jamesclear.com/3-stages-of-failure

PCI DSS v4.0
navigational points..................

1. **Do not delay.**
   Organizations should not delay preparations to meet the requirements of PCI DSS v4.0. It would be a mistake to believe that it's not necessary to start your preparations early, even if your organization is fully compliant with PCI DSS v3.2.1.

2. **Start strong—meet PCI DSS v3.2.1 requirements.**
   Start from a position of strength. Determine the extent to which you are, or aren't, following the defined approach for each requirement applicable to your CDE. Evaluate the robustness and resilience of your control systems. Improve your capability to very quickly detect and correct control failures. Determine if each of the requirements is truly meeting the stated security objective of the requirement.

3. **Understand the PCI DSS v4.0 requirements.**
   Review all the PCI DSS v4.0 requirements carefully, taking note of changed controls, controls that were removed, new controls, renumbered controls and future-dated controls. Ensure that you understand the control objective and intent of each requirement in the context of the entire PCI Standard. The biggest impact is within Key Requirements 12, 11, 10 and 8 (ranked in order of impact).

4. **Choose your control design and compliance validation option wisely.**
   Selecting the customized approach may initially require an increased workload to prepare for the compliance validation of tailored security controls. It could potentially increase control risk, but also offer a more robust, permanent security control solution when compared to a defined approach with compensating controls that require documented justification of a business or technical constraint. (Refer to the 2018 PSR, pages 23 and 41, for examples of how to measure control effectiveness.) Customized controls, as with traditional defined controls, need to show consistent operating effectiveness over long periods of time, without interruption, to meet the objective and intent.

5. **Take care when selecting a customized approach.**
   If you opt to follow the customized approach for any portion of your environment, you need to be prepared to manage the scope of work it requires. Controls should be designed to be effective and sustainable within their operating environment. Also, customization requires structured and detailed documentation. Documented evidence should be maintained to substantiate that controls meet the intent of the relevant security objective(s). Whoever gets the job of internally reviewing control effectiveness prior to external validation should be proficient and look at competence, maturity and testing as three key elements. This work is needed for the actual achievement of the task—for controls to be validated and approved.

6. **Use control design and management templates.**
   The importance of assessing control effectiveness regularly is obvious. Creating control design documentation in a structured manner is immensely useful but can be time consuming. Developing and consistently applying a standardized control template that generates a control design profile for each required security control or control system is a best practice recommendation for all organizations, particularly if you're opting to implement a customized control approach. (See additional details under "The necessity and value of control design templates" below.)

7. **Do early validation of control designs.**
   Control designs should be shared with assessors (ISAs and QSAs) at the earliest opportunity during the design process to determine if the controls are acceptable to meet the related requirements and security objectives. Without thorough documentation that details the "what," "when" and "how to" of the design, function, operation, maintenance and evaluation of controls, the approval of a customized control approach could be delayed.

8. **Prepare for ongoing compliance.**
   It's important to define the requirements and constraints for your security team to support the design, implementation and maintenance of ongoing compliance. This requires capacity planning and commitment for teams to support this process, to regularly evaluate, document and report on the control status of the environment throughout the year. The internal recording of evidence of compliance with the PCI DSS should be an ongoing business-as-usual activity.

The necessity and value of control design templates

The use of tailored security control design templates to create and maintain documented control profiles is not, surprisingly, a common security architecture and management task followed by organizations. Using templates provides substantial benefits for control system improvement, including the ease, transparency and consistency they provide in designing, deploying, operating and maintaining controls. Templates assist in the clarification of functional control specification, and early detection of control design and control operation issues. A complete set of documented security control profiles also contributes toward the effectiveness and strength of the control environment, providing much-needed perspective on control purpose, function and operational limitations.

In general, a PCI DSS control profile document should be prepared for each control system and critical individual controls. Typically, it includes the following 12 items:

1. **Control objective**
   Defines the applicable control objective(s) of the control or control system and its contribution toward the overall goal

2. **Control owner**
   Assigns ownership of, accountability for and responsibilities over the control or control systems

3. **Control function**
   Describes the control function, such as management, procedural, or technical and functional boundaries

4. **Control type(s)**
   Describes the applicable control types, such as preventative, detective, corrective or directive—or a combination

5. **Architecture**
   Defines the control architecture, such as system-specific, common or hybrid, and its contextual application

6. **Control risk**
   Describes key risks that the control mitigates, such as using control-to-risk matrix or mapping

7. **Control testing**
   Describes or references all applicable, related control test procedures and standards for the control and control system

8. **Implementation**
   Specifies implementation scope, control, procedure and dependencies—listing the primary PCI DSS controls and all dependent PCI DSS controls

9. **Operation**
   Documents control operation specifications and defines scope, processes, operational dependencies, supporting processes and control support requirements, as well as component impacts on people, systems, processes and third parties

10. **Maintenance**
    Defines control maintenance specifications, scope, and maintenance standards and processes

11. **Performance metrics**
    Provides a list of PCI DSS key performance indicators (KPIs) and other metrics to measure control performance

12. **Governance**
    References related policies, standards, frameworks and regulations

(For more details on documenting control profiles, see the 2018 Payment Security Report, page 12.)[51]

51 2018 Payment Security Report, Verizon, 2018, https://www.verizon.com/business/resources/reports/payment-security-report/

Maintaining control design profiles can have a substantial positive impact on the quality of controls and the control environment. Clear control design and operation specifications establish context and perspective on control performance expectations; identify and communicate design limitations; and list the operating and maintenance requirements of key control systems. Without clearly documented and communicated control profiles, security and compliance teams may lack sufficient direction for early detection and correction of deviations, which could result in control failure. In general, the more detailed the design profiles, the tighter (consistent and robust) the control, and more predictable the performance.

The overall outcome of a managed control design process is to enable and promote control effectiveness in terms of consistent, complete, reliable and timely operation.

Worth repeating

Control design requires a systematic method. The PCI DSS defines a set of dependent and interdependent controls that requires customization to every unique control environment in order to be truly effective and sustainable. Without a deliberate and systematic method for control design, the strength of each implemented control depends mostly on the enthusiasm and limited capabilities of the team or person tasked with its implementation, not the actual establishment and measurement

of control strength and sustainability requirements that conform to industry and internal standards.

Gaps typically exist in areas of control dependency. There is no single PCI DSS control that operates and achieves its objectives independent of all other controls in the Standard. This point is so important that it's worth repeating. The problems associated with organizations implementing out-of-the-box PCI DSS controls are well known. People assume that controls will work well and do not need design, refinement and management as part of a control system. Yet, things often have to go wrong before organizations take action and actually evaluate control designs and implement supporting processes to make sure the controls operate as intended and in a sustainable manner.

Procedures often have to fail before organizations take action and actually evaluate control designs and implement supporting processes to make sure the controls operate as intended and in a sustainable manner.

When conducting a compliance validation assessment, QSAs are often surprised by how organizations willingly tolerate routine security control operation and design errors. In such cases, management often continues to accept low but persistent levels of control and compliance errors as inevitable and acceptable, even when they are not difficult to avoid.

Project management is key for a successful transition to PCI DSS v4.0.

In the 2020 PSR, we emphasized that no PCI security program should be implemented without having a strategic plan in place. It's essential to develop, define and clearly communicate the sense of purpose of the program— the prioritized goals and objectives, and how resources will be directed toward a clear goal. All stakeholders should operate with clear direction and consistent coordination among teams.

Surprisingly, what we see in organizations that fail to maintain their PCI DSS controls, even those assessed multiple years, is that maintaining firm control over program and project management is still a challenge. Since PCI DSS v4.0 will require widespread changes for most organizations, all are advised to apply and adhere to fundamental project management principles. In the past, with each

major update to PCI DSS, the risk of producing work based on invalid assumptions was increased, such as misinterpretation of DSS security controls, duplication of efforts, etc. This can and should be avoided.

It's puzzling to learn how common it is for many organizations to initiate annual PCI security projects with little to no change implementation plan. A change implementation plan—which isn't separate from the project plan but is part of it—increases cooperation across all teams, supports buy-in and ensures change actions are undertaken by relevant people.

Also in the 2020 PSR, we discussed at length Trap 4, "Falling short on sound strategic design," and Trap 5, "Deficient strategy execution." A good strategic plan for your security compliance program won't do any good without appropriate structure, process and organizational alignment to ensure leadership support, real commitment and adequate communication. The initiation of a PCI security project should be preceded by confirmation of the overall security and compliance goals and objectives, followed by a revisiting of security and compliance strategy (the approach to direct resources to achieve the goals) and alignment with supplemental frameworks. All PCI security projects should be managed as part of a long-term program.

At a high level, four basic program and project management steps are sometimes overlooked that can help support a successful PCI DSS v4.0 implementation.

Step 1: Sponsorship and accountability

The accountability for the success of a PCI DSS project should not reside in one individual acting as the sole sponsor. Every manager with direct reports that participates in the project or is impacted by the project should share responsibility and proportional accountability for the success of the project. Commitment and active participation are of vital importance to the functioning of a project team. A change implementation plan should have an explicit strategy for securing a formal level of commitment at the beginning, middle and end of the project life cycle.

Step 2: Readiness

Project readiness measures and reports the state of preparedness to ensure a project is primed for development, implementation and execution to completion as planned. Building readiness is not a check-the-box activity that gets crossed off your list and forgotten. A project readiness management plan provides the disciplined, systematic, process-driven management practice required to ensure that teams are ready to perform their activities. Sources of resistance to changes by project participants often differ at various stages of the project (start, middle, end), requiring different strategies and tactics.

Step 3: Communication

A communication plan is not the same as a complete implementation plan—it's just one component. Communicating realistic, clear and measurable goals and objectives, and their requirements, plays a critical role for participants to all be on the same page to avoid misunderstandings. Putting sufficient effort into a PCI DSS v4.0 project communications plan to clearly define, document and communicate project deliverables, priorities and milestones is also essential. Include feedback loops to gather reactions to both the content of the change and how the change is being implemented.

Step 4: Reinforcement

It's vital to understand the symptoms and root causes of a project in trouble. Project management reinforcement and support processes help identify troubled projects in the early stage of their execution. A reinforcement strategy helps sponsors and project participants apply timely reinforcement at the local level for implementation. This helps with project resource capacity management and task prioritization, and avoids milestones getting pushed out.

Constraints:
The security and compliance shoal . . . .

A PCI security compliance management program is a complex system with many moving parts. A complex control environment consists of multiple linked activities. Events that occur in one area affect other areas of the system. Examples abound of these interlinking systems within every PCI security control environment, with many interconnections and dependencies between PCI DSS requirements and controls, and system components (people, documents, processes, and IT devices and networks). The decisions made often have unpredictable effects. The chain of causality is not easy to track. At any given time, an organization is limited from achieving its highest goal by at least a single constraint.

Constraints can show up in many ways. These can be anything that limits the system from achieving higher performance. There is at least one, but at most only a few significant constraints in any given system that require attention. One always acts as a constraint upon the entire system—the constraint activity is the weakest link in the chain. It can be a step or process producing less than what's demanded of it. The whole process itself can be the constraint, and, as an example, even senior management and other departments can be considered the constraint.

This means that processes, organizations, etc., are vulnerable because the weakest person or part can adversely affect the outcome. This is a harsh reality for data security and compliance, which security teams deal with daily. No meaningful improvement exists unless time and effort are spent to reduce and remove constraints that limit system performance.

"Not every change is an improvement but certainly every improvement is a change."[52]

—Eliyahu M. Goldratt

No meaningful improvement exists unless time and effort are spent to reduce and remove constraints that limit system performance.

---

52 Eliyahu M. Goldratt, Wikipedia, https://en.wikipedia.org/wiki/Eliyahu_M._Goldratt

Identifying the most important constraint

The introduction of PCI DSS v4.0 places a much greater impetus on organizations to demonstrate the capability to continuously improve their control environment. However, constraints, when approached correctly, can be key to unlocking improvements in productivity.

You can—and need to—elevate a constraint to the point where it's no longer the system's limiting factor. This is called breaking the constraint. In a PCI DSS compliance environment, breaking the constraint helps the control environment achieve the required level of effectiveness and sustainability.

Once you break a constraint, you will uncover the next most-limiting constraint. No system exists without constraints where its performance can go to infinity. Another constraint will constrain the system's performance. In other words, the limiting factor is now some other part of the system or is external to the system (an external constraint).

How do you sort out the important few constraints from the trivial many? A method is needed to identify and prioritize them according to their impact on the goal. Whatever the constraints may be, much can be done to reduce their impact.

Introducing the Theory of Constraints

The Theory of Constraints (TOC) is a proven process management methodology for identifying the most important limiting factor (constraint) that stands in the way of achieving a goal, and then systematically improving that constraint until it's no longer the limiting factor. This approach to improvement views any manageable system as limited in achieving its goals by a very small number of constraints. This makes the TOC a very powerful tool.

The TOC originated in manufacturing and soon proved usable in other environments. In 1984, Eliyahu M. Goldratt, a physicist turned business consultant, articulated the Theory of Constraints in his book, The Goal: A Process of Ongoing Improvement.[53] Goldratt simply defined the TOC as "a process of ongoing improvement" and a thinking process that enables people to invent simple solutions to complex problems. In 1986, he created the Avraham Y. Goldratt Institute to teach the theory. Many businesses around the world have adopted this methodology to help them better understand the factors keeping them from their goals.

The TOC helps you look closely at a process or step and then see the step in the context of the entire line, process or organization. This holistic perspective is key to the TOC, because it views organizations as a chain of departments and functions.

Applying the TOC to PCI security compliance management

The speed and efficiency used to complete the numerous tasks that are necessary to achieve and maintain security and compliance is mostly dictated by the slowest process in the control environment operations chain. The TOC's application to PCI security compliance, and data security in general, offers a prioritization method and a way of looking at a complex system to uncover and address underlying root causes that prevent control environments from being efficient, effective and sustainable. Its structured and logical approach can be applied system-wide to break limiting factors, get more out of existing processes and resources, and continually achieve goals.

The holistic view and continuous search for constraints enables better control over processes and exposes additional capacity—often without the need for further investments. In other words, the TOC forces you to use what you already have, rather than spend money on new equipment or more resources. This is exactly the solution many organizations need to improve their PCI security compliance capability.

---

53 Eliyahu M. Goldratt and Jeff Cox, "The Goal: A Process of Ongoing Improvement," North River Press, 2004.

The TOC benefits

In sum, the Theory of Constraints (TOC) helps individuals and teams understand that:

- Constraints analyses focus improvements on where they can have the most impact

- The concept of a constraint makes it easier to find what is slowing the advancement of the whole environment, or even the whole organization

- The holistic view of the environment (or organization) and the continuous search for constraints gives you better control over your process so that you can anticipate backups and events that reduce performance

In the context of its application to PCI security, this approach helps organizations by:

- Providing information needed to understand the scope and nature of data security and compliance goals and strategy

- Diagnosing issues, which may necessitate redefinition of the problem and recommendations based on the diagnosis

- Facilitating the capability to plan, develop and implement a structured approach to identify the correct solution (solve the right things in the right manner)

- Assisting with the implementation of recommended solutions and supporting consensus building around corrective action

- Facilitating learning — that is, growth in understanding, capability and processes to resolve similar problems in the future

- Continuously improving elements of organizational effectiveness

- Exposing additional capacity and optimizing existing resources

The method for achieving continuous improvement for PCI security compliance

To reiterate, your payment card security and compliance system consist of a chain of processes. If you want to improve the system (strengthen the chain), where is the most logical place to focus your efforts? The weakest link! Systems are analogous to chains, and each system has a "weakest link" (constraint) that ultimately limits the success of the entire system. In most cases, the most productive approach is to start with strengthening the weakest link. A chain will break at the weakest link, no matter how strong the other links are made. Therefore, efforts spent to improve nonconstraints will not produce the most beneficial improvement in your security and compliance system capability – its effectiveness, robustness and resilience.

For many organizations, the weakest link in the performance — strictly from a basic PCI DSS control requirement perspective — is found under Key Requirement 11: Test security of systems and networks regularly (specifically Controls 11.2 and 11.3). Other related weak links within the system are Key Requirements 12 and 6. When you increase the strength (control robustness and resilience) and address the weakest link, it should not be the weakest link anymore. While the chain became stronger, it's not indefinitely stronger — since some other link is now the weakest one, and the overall strength of your security program is now limited by the strength of that link. The primary constraint migrated to a different component.

From a broader perspective, organizations need to determine and address the weakest links in management capabilities. A generic management problem that exists across many organizations within the payment card industry is the design and implementation of a strategy that ensures ongoing improvement of the compliance environment and its follow-through.

If you decided on the goals of your security compliance strategy and program, and the necessary conditions for attaining them, are you achieving those goals right now? If not, you could be doing better. Now, consider these additional questions:

• What is keeping your strategy and program from doing better, in light of the fact that security and compliance are processes in part of the overall control environment?

• What is keeping your control environment from doing better—and reaching its desired full potential?

• What exactly do you think are the constraining factors (everyone in your team will likely have their opinions, but who is right)?

• Where in the chain of processes is the most logical place to focus your efforts to improve your payment card security and compliance system (where you can strengthen the chain)?

Now consider four basic questions about change that every manager needs to ask:

• Why change (what is the goal)?

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

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

• How to affect the change (how do you implement it)?

It's important to remember that these are system-level not process-level questions. While the answers to these questions have an impact on individual processes, efforts should be focused on system improvement.

"Processes are important, but our organizations ultimately succeed or fail as systems. What a shame it would be to win the battle on the process level, only to lose the war at the system level!"[54]

—H. William Dettmer

A control environment is a continuous managerial process with structures and standards that provides the basis for carrying out internal control across the organization. Within an effective control environment, competent people understand their responsibilities and the limits of their authority. They are knowledgeable, mindful and committed to doing what is right and doing it the right way.

An effective control system rapidly detects and discloses where failures are occurring and what or who is responsible for the failures. It ensures that corrective action is taken and that performance is measured, reported and continuously improved.

54 H. William Dettmer, "Goldratt's Theory of Constraints: A Systems Approach to Continuous Improvement," American Society for Quality (ASQ) Press, 1997.

Identifying and addressing constraints and core conflicts

PCI security management can only succeed when its set of baseline requirements is supported by a comprehensive set of actions taken by management to establish an effective control environment. The environment should never be subjected to random internal changes. Organizations are expected to firmly manage internal influences and have the capacity to deal with external influences, which one typically has much less control over.

As an industry, the need for ongoing improvement at a system level is not up for debate. A process of ongoing improvement is an absolute necessity. To improve means to change. As mentioned earlier, for an organization to have a process of continuous improvement, certain basic questions need to be answered faster and more effectively. Those fundamental questions are: "Why change?" "What to change?" "What to change to?" and "How to cause the change?"

What to change?

The changes are not simply limited to PCI DSS requirement changes. They go well beyond that. PCI DSS controls perform poorly within control environments for reasons that, after nearly two decades of PCI security

compliance, are well known and documented. The factors that influence the sustainability and effectiveness of the environment are known. The main security and compliance management mistakes are known—we refer to them as the Top 7 Strategic Data Security Management Traps, discussed on page 12 of the 2020 PSR. As are the nine primary factors, which we call the 9 Factors of Control Effectiveness and Sustainability (see the 2018 PSR for details).[55] Additionally, the most common constraints are known: The 7 Constraints of Organizational Proficiency (see next page).

All PCI security compliance environments can and should have known lists of observable symptoms with known cause-and-effect relationships between system components. How to identify the underlying common cause, the core problem, for all of the symptoms within the environment is a skill every security team can learn and master. With the correct approach, every organization can achieve full-compliance sustainability and effectiveness with the ability to keep 100% of PCI DSS requirements in place, and to be proficient at rapidly detecting and correcting any control that falls out of place.

For those who have not yet reached that level of operational capability and maturity, the core problem is inevitably an unresolved conflict that keeps the organization trapped and/or distracted in a constant tug of war. This goes back to unresolved issues

in the Top 7 Strategic Data Security Management Traps. This conflict is called a core conflict. Core conflicts within PCI security compliance environments have devastating effects on the performance (robustness and resilience, and therefore sustainability and effectiveness) of the control environment. Organizations attempt to treat those negative effects by creating policies. However, these are usually Band-Aid fixes, since they don't treat the core conflict.

---

55   2018 Payment Security Report, Verizon, 2018, for more details on documenting control profiles,
     https://www.verizon.com/business/resources/reports/payment-security-report/

The 7 Constraints of Organizational Proficiency (the 7 Cs)

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

The table below presents a categorized list of primary constraints. These are common constraints preventing organizations from developing the process and capability maturities needed to achieve a sustainable and effective control environment that operates with consistent performance and predictable outputs. It's certainly not an exhaustive list, but rather a useful frame or "mental model" that can facilitate categorization of limitations and restrictions within the control environment.

Constraints	Inhibitors	Specifics
1 Capacity	The required number of resources (people, processes, technology, time) not available to cover the scope of security assignments	• Ineffective capacity planning • Lack of assigned governance and leadership responsibilities • Time spent elsewhere, not on security issues (lack of focus)
2 Capability	Inability to direct and apply resources (collectively) to perform security and inadequate supporting processes, tools and guidance	• Lack of tools and processes • Inadequate security standards and procedures for leadership and management control • Inadequate task assignments
3 Competence	Shortcomings in the required skills, knowledge and experience (individually) to design, operate and improve a security control environment	• Deficient strategy, skills, focus • Selecting the wrong objectives (technical, not strategic; lack of robustness and resilience)
4 Commitment	Insufficient ongoing assurance from management that employees are required to consistently adhere to security and compliance requirements, and investment of resources to enable them	• Not prioritizing, no dedication • No executive follow-through • Inadequate support and investment for long-term process and capability maturity development
5 Communication	The lack of clarity with which directives are given for teams and individuals to work toward goals, the frequency of the communication, the level of focus, and measurement of performance	• Low frequency and poor quality of communication • Silos, barriers in reporting lines • Individual performance expectations not measured and communicated
6 Culture	Team, business unit or organization-wide culture not aligned with security and compliance objectives, underinvestment in developing culture	• Relaxed security culture ("let it fail, we will just fix it again" mentality) • Tactical instead of strategic • No continuous improvement and communication
7 Cost	Total-cost-of-ownership constraints: lack of funds or funds allocated elsewhere not supporting security and compliance goals	• Acquisition cost vs lifetime cost • No budget for long-term strategic security design and maturity development

A detailed description of most of these constraints can be found on page 10 of the 2019 PSR.[56]

56 2019 Payment Security Report. Verizon, 2019, https://enterprise.verizon.com/en-au/resources/reports/payment-security/

Application of the Logical Thinking Process

Many organizations are making substantial progress in advancing the maturity of their security and compliance capabilities. Many others need to ramp up their engine speed and make significant adjustments to the management of their compliance program.

In some cases, this requires substantial changes and the adoption of methods entirely new to the organization. Which is why we are dedicating this section to the Logical Thinking Process method, a very strong framework that can help you improve every aspect of data security and compliance and support better decision-making to achieve goals.

Organizations suffer poor performance in compliance environments because they don't have clearly defined outcomes for their data security and compliance programs. Security teams often think they know what they want to accomplish, but in reality, they are unclear about what, specifically, constitutes the end states of their strategy and program. They don't know which components to optimize and prioritize. When CISOs and their teams

are unclear about priorities—what truly matters and requires focus—they sometimes fail to progress out of fear of making the wrong choices. But choices must be made.

These challenges are directly related to the goal. The importance of formulating a clear goal statement for PCI security compliance is reviewed on page 86. The achievement of that goal needs to happen by design, no matter how you define your goal or craft your mission statement. For example: "To develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing protection of payment card data, in a consistent, predictable and sustainable manner." The importance of applying a method cannot be overstated. You need a method that enables you to identify, define and pursue the objectives toward your goal. You need clarity about the requirements—the conditions that need to be in place—for each objective. You also need to address and remove constraints.

How you, your team and your organization progress toward the achievement of your security and compliance goal matters—a lot. You need a proven approach that provides assurance and confidence for success: a process that identifies the roots of the undesirable effects and exposes faulty assumptions related to the root causes of poor security and compliance performance.

As mentioned on page 33, the real challenge is not achieving your security and compliance goal. It's whether you and your organization are willing to accept and commit to the investment of resources and the planning, execution and follow-through required to achieve that goal.

Most organizations are financially restricted and need to achieve the goal with the available resources. The Logical Thinking Process does all of this in a practical, visual way that is easy to understand.

The real challenge is not the achievement of your security and compliance goal. It's whether you and your organization are willing to accept and commit to the investment of resources and the planning, execution and follow-through required to achieve that goal.

Origins of the Logical Thinking Process

The LTP is a framework based on the Theory of Constraints processes developed by Dr. Goldratt, who was introduced on page 9. This method was later enhanced by H. William Dettmer, author of The Logical Thinking Process: A Systems Approach to Complex Problem Solving. It's a method designed to take poorly defined problems and slowly but surely move them toward a solution. This meticulous process breaks down components of a systemic problem to clearly define the nature of the problem. The investment of time helps to correct the systemic problem and avoid ongoing poor performance

that previously resulted in a massive waste of time and capital.

The LTP enhances collaboration and improves communication. It helps you structure ideas and analysis. It visually displays the links between cause and effect in an easily comprehendible format. The LTP also makes it much easier to refine elements and spot design flaws. Decisions are far too often based on wrong assumptions that do not reflect reality, which can be harmful. Often those assumptions are tacit—we don't realize we make them, or fail to understand the negative impact they have on decision-making and system design.

The LTP comprises five steps, based on necessity or sufficiency reasoning, to help improve your decision-making.

"Inside every small problem is a larger problem struggling to get out."[57]

—The Schainker Converse to Hoare's Law of Large Problems

What exactly are the thinking processes?

The thinking processes are a set of tools that provide decision support for initiating and implementing a task or project. When used in a logical flow, they help walk you through a buy-in process to:
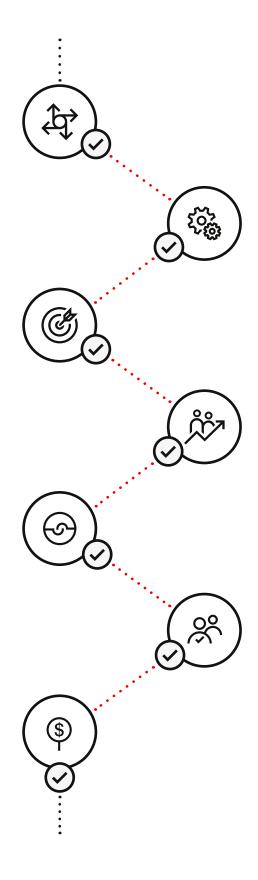
- Gain agreement on the problem
- Gain agreement on the direction for a solution
- Gain agreement that the solution solves the problem
- Agree to overcome any potential negative ramifications
- Agree to overcome any obstacles to implementation

The process of change requires the identification and acceptance of core issues, the goal and the means to the goal. This comprehensive set of logical tools can be used for exploration, solution development and solution implementation for individuals, groups or organizations.[58]

You can anticipate constraints in existing processes, and you can also plan for them while designing a product, process or service.

---

57 Arthur Bloch, "Murphy's Law: The 26th Anniversary Edition," Penguin Group, 2003.
58 "Theory of constraints," Wikipedia, https://en.wikipedia.org/wiki/Theory_of_constraints#The_five_focusing_steps
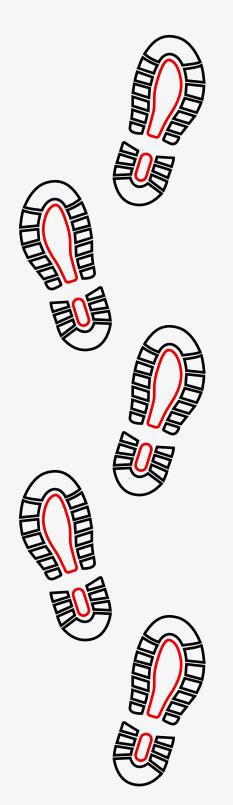
Analysis/structure vs synthesis/function

We mentioned the importance of applying systems thinking to solve PCI security challenges. The key to systems thinking is synthesis—putting components together. The approach to dealing with increasing complexity in data security and compliance environments is not by analysis; it's not to reduce it to manageable "bites" and address each component in isolation from the others. It's an incorrect assumption that all of the parts are essentially independent of one another. This is very true also for PCI DSS requirements, components within the compliance and control environments, where various relations, dependencies and interdependencies exist between system components. That's why you should synthesize—and not stop short at analysis—when conducting design, evaluation and management tasks. True application of systems thinking combines analysis and synthesis, where analysis focuses on structure and synthesis on function. As H. William Dettmer mentions on page 61 of his book Systems Thinking—And Other Dangerous Habits, "The essential difference between analysis and synthesis is this: if each part of a system, considered separately, is made to operate as efficiently as possible, the system as a whole will not operate as effectively as possible."[59] Understanding this is key to unlocking the method for achieving sustainable control effectiveness for your PCI security control environment.

59 H. William Dettmer, "Systems Thinking – And Other Dangerous Habits," Virtualbookworm.com Publishing, 2021.

The Five Focusing Steps in brief

The Theory of Constraints is based on the premise that the rate of goal achievement by a goal-oriented system (the system's throughput) is limited by at least one constraint. So, you need to prioritize improvement activities. The top priority is always the current most significant constraint. The Five Focusing Steps offers a highly defined methodology for creating rapid improvement.

Assuming the goal of a system is articulated and its measurements defined, the steps are:

1. Identify the system's constraint(s)
2. Decide how to exploit the system's constraint(s)
3. Subordinate everything else to the above decision(s)
4. Elevate the system's constraint(s)
5. Prevent inertia from becoming the constraint[60]

The Five Focusing Steps are designed to help you discover constraints early, in order to minimize or eliminate them.

> "To err is human, and so is trying to avoid correcting it."
>
> —Anonymous

---

60 "Theory of constraints," Wikipedia, https://en.wikipedia.org/wiki/Theory_of_constraints#The_five_focusing_steps

The Five Focusing Steps

1   **Identify the system's constraint.**
Identify the specific part of the process (for example, any process within your PCI security compliance environment) that constitutes its weakest link: a policy, procedure, resource or particular system component. Identify anything keeping you from meeting desired goals. Constraints can come from internal factors, such as lack of training or poorly designed processes, or external factors—such as contractual constraints with third parties (vendors, regulators), etc.

2   **Decide how to exploit the system's constraint.**
Determine how you can work with existing resources to reduce the impact of the constraint. For example, if the constraint is an overworked employee or team, redistribute assignments to get the work done. If a constraint is a poorly defined procedure, focus on redefining the procedure and train employees on its correct application. If the constraint is a needed feature in an IT system, optimize the current capabilities (see page 34 of the 2020 PSR, "The unknown resources buried in your 'sandbox'"). Obtain as much capability as possible from a constraining component without undergoing expensive changes or upgrades.

3   **Subordinate and synchronize to the constraint.**
The previous step was about understanding the ins and outs of the constraint itself, and this step is about understanding everything around that constraint. To enable the constraint to operate at maximum effectiveness, the parts of the process that are not constraints (nonconstraint components) need to align with and support it. Once this is done, the overall system is evaluated to determine if the constraint has shifted to another component. For example, if the security analysts can review only X number of logs per day, you would not attempt to remove a constraint on the security information and event management (SIEM) process by increasing the number of logs to be reviewed, or continue to make the analysts aware of the additional components added to the environment that now also add to the log monitoring burden. The solution lies elsewhere. If your solution eliminated the constraint, you can jump to Step 5.

4   **Elevate the constraint.**
If the constraint still exists, you will need to make it a higher priority. Elevating the constraint refers to taking whatever action is necessary to eliminate the constraint. For example, you may need to hire more people to increase the workflow in the area where the constraint exists. This step is only considered if Steps 2 and 3 are not successful. Major changes to the existing system are considered at this point. Since elevation involves expenditure, you need to consider whether the ROI justifies the expense.

5   **Repeat the process as needed.**
You should start the process all over again to identify the next constraint and avoid inertia (meaning you want to avoid becoming complacent). If a constraint is resolved in a step, start again at the first step to identify other constraints. This ongoing process allows for continual improvement. Repeat these steps to ensure that you are getting the work done and meeting goals.

The Five Trees

A problem can reoccur, like weeds in a garden, unless you dig down and eliminate the root. That's much easier to do when you use a tool. These tools can be simple or complex, depending on how deep the root is or the complexity of the root system.
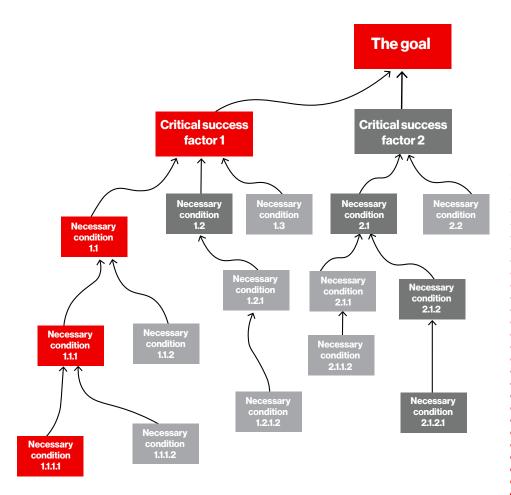
The LTP comprises five separate logic trees. Each one has a specific purpose, designed to help organizational teams make better decisions. The LTP adheres to logical principles that apply to each step of the process.

- **Step 1:** The Goal Tree
- **Step 2:** The Current Reality (Problem) Tree
- **Step 3:** Conflict Resolution (Evaporating Cloud) Diagram
- **Step 4:** The Future Reality (Solution) Tree
- **Step 5:** The Prerequisite (Implementation) Tree

This is a very effective method for resolving complexity in security and compliance problems where many different factors contribute to visible problem indicators, and where the chain of cause and effect between deficiencies in the security control environment and underlying causes often isn't obvious. Even traditional root-cause analysis methods can lead teams to assume that something may be the root cause of a problem when, in fact, it's not. This Five Trees approach presents a step-by-step, workable solution by finding a fully implemented solution for an ill-defined problem.

"I would rather discover a single causal connection than win the throne of Persia."[61]

—Democritus

61 Democritus, Greek philosopher, c. 460-370 BCE

Step 1: The Goal Tree—What is the goal?

The Goal Tree is at the center of all five trees; it's the navigational marker and fixed point of reference for all the other tools. It focuses on a specific goal that you aim to achieve for a particular data security and compliance control system, and what is necessary to get there.

It starts with the goal statement, the vision or what the Lean Six Sigma community refers to as "True North." This step is key to the whole process. This first step is the central and most critical one to help you formulate the desired outcome. The goal can be set only by those who created the system or those responsible for steering the organization toward the goal set by the founders.

Step 1 does not start by analyzing problems. It requires defining where you want to be—the goal that you aim to achieve. Where do you want to be? What is the system's goal, its ultimate destination? This is the clearest definition of the ultimate milestone to complete the mission for any particular PCI DSS objective, or the entire program. It's the finish line, and there can be only one goal.

Next, define what is necessary to get there—the goal is dependent upon critical success factors and a series of conditions necessary to achieve them. The visual representation with the goal at the top and its branching necessary conditions forms the Goal Tree.

The Goal Tree is built upon logic and clearly establishes relationships, such as: "In order to have A, we absolutely need B." A is the next (intermediate) objective and B the necessary condition. A cannot exist/ be true/be achieved unless B exists/ is true/is achieved. The concepts of necessary and sufficient conditions help us understand and explain the different kinds of connections between various PCI DSS security controls, their different states and how they relate to each other. It also helps to explain the relationships between PCI DSS controls and other controls not included in the PCI DSS, in order to bring about the required control effectiveness and sustainability.

When the Goal Tree is used to articulate what needs to be done and why—which is uncomplicated with a robust tree—it tells what is imposed by the circumstances. It's not based merely on someone's opinion. It presents the path with clarity. There's no room for nice-to-haves, biases or whims.

The Goal Tree gives input to the next tool in the Logical Thinking Process: the Current Reality Tree (CRT).

Step 2: The Current Reality (Problem) Tree—What is the problem?

This step helps you analyze why you are not reaching your data security and compliance goals. It assesses where you are in the process, and why there is a gap. Where are we, actually, and why is there a difference?

To accomplish this step, list the problems. They are usually based on the critical success factors. The focus of Step 2 is on identifying all factors that contribute to problems—either individually or collectively. Continue this process until root causes are identified. Identify invalid assumptions that produce conflict. Assumptions can be called what they really are: opinions, theories, hypotheses, guesses and conjectures.

The CRT is a way of analyzing many systems or organizational problems at once. By identifying root causes common to most or all of the problems, a CRT can significantly help focus improvement of the system. It depicts the current reality in a series of dependent, logical, cause-and-effect relationships, starting from undesirable effects (UDEs) down to one or a few critical root causes. A well-defined problem is more than half solved.

With the CRT, you identify and evaluate the gaps between the Goal Tree requirements and the actual condition. Gaps lead to UDEs. These UDEs are the inputs for another tool: the Future Reality Tree (FRT) in which the undesirable effects are neutralized with "injections": causes or conditions not yet existing and designed to turn UDEs into their opposites—desirable effects (DEs)—without bringing negative side effects.

Step 3: The Conflict Resolution (Evaporating Cloud) Diagram —Which assumptions are invalid?

Apply the Conflict Resolution Diagram (CRD) to develop simple breakthrough ideas and solutions. The CRD is also called the Evaporating Cloud (EC), named in honor of Richard Bach's 1977 book Illusions, in which the main characters remove storm clouds from the sky by thinking them away.[62] It's specifically used to structure and solve underlying conflicts. Conflicts usually are based on false assumptions, and the Conflict Resolution Diagram helps bring to the surface and evaporate the conflict. It dissolves dilemmas or

conflicts between opposing objectives or conditions, different alternatives and hidden agendas (the three primary types of conflict). It identifies the exact assumptions behind the logical connections. What prevents us from curing the problem now, and how do we overcome it?

The CRD exposes deeply hidden root causes that must change. It lists the exact assumptions behind the logical connections. Assumptions need to be factually true and also lead to the prerequisites. Injections are ideas that solve conflicts—a solution that fulfills all requirements and invalidates conflicts. Distinguish between needs (necessities) and wants (wishes). Then you are a step closer to the solution.

Step 4: The Future Reality (Solution) Tree —What can we expect if a fix to the problem is applied?

While a well-defined problem may be half solved, a huge leap forward is still needed to transform a solution into reality. This tree is a visualization of a desired future state that allows mapping out future expectations. It

helps to break current-reality problems or core conflicts by introducing new ideas or injections. Introduction of new ideas changes undesirable outcomes of current reality to desirable outcomes of future reality. It answers the questions: "What to change?" and/or "Change to what?" It is a way to confirm that your planned solution will actually work.

The Future Reality Tree is the tool of choice to gain understanding and agreement that your solution will account for all of the undesirable effects that you currently experience and built into your Current Reality Tree. While the Future Reality Tree depicts a could-be future, it does not give all the answers about how to get there. "Injections" are the proposed actions to break the current-reality problems or core conflicts. You need to determine if injections really lead to a workable solution.

Building a future reality is also about setting the right priorities. Map out what steps have to be achieved and precisely how they can reach that goal. Verify that the proposed solution will actually solve the problems. Identify negative effects—the unintended consequences and side effects that might be caused by the solution.

---

62 "Evaporating Cloud," Wikipedia, https://en.wikipedia.org/wiki/Evaporating_Cloud#Origin_of_Name

Step 5: The Prerequisite (Implementation) Tree—How can the solution be executed?

Orchestrating a major system change involves accomplishing a lot of individual tasks. This tree provides a clear definition of what needs to be done, in what sequence, and what must be done in parallel to execute the solution. The Prerequisite Tree allows you to overcome the obstacles that stop you from implementing and executing your plan.

Define the individual steps by constructing a step-by-step implementation plan, and describe how obstacles will be handled. Some injections may require a detailed implementation plan. The Prerequisite Tree can serve as a skeleton for a project plan. It's composed of two elements—an obstacle and an intermediate objective. The intermediate objective is the action that you must undertake to overcome or neutralize obstacles even before implementation; for example, when stakeholders argue about obstacles that hinder implementation of the solutions found with the Future Reality Tree and Evaporating Cloud. Every obstacle is then neutralized or bypassed with intermediate objectives—smaller, sequential steps and conditions necessary to fulfill in order to bypass the obstacles. These objectives help you set intermediate goals to achieve change toward the organization's goal.

For more information, see Systems Thinking—And Other Dangerous Habits by H. William Dettmer, page 221, and From Symptoms to Causes: Applying the Logical Thinking Process to an Everyday Problem by Thorsteinn Siglaugsson.[63]

The application of the Five Trees

With this method, a security team can focus on getting rid of everything that is not crucial and distinguish between needs and wants. It directs the focus toward important problems and away from those that really don't have to be solved. In summary, this method can help you:

- Clarify your goals and their requirements and gain clarity about objectives
- Determine the critical success factors branching out beneath the goals (three to five for each goal)
- Outline the variables and conditions needed for the system to achieve the goals
- Identify the necessary conditions for each critical success factor

This will become increasingly important for organizations opting to follow the PCI DSS v4.0 customized control approach and ongoing assessment validation.

The Logical Thinking Process and GRC²

The benefits of applying the LTP to GRC² are extensive. They include communicating effectively, leading actively, empowering employees and creating an environment of continuous improvement, so organizations can keep PCI security compliance performance from stagnating or regressing. Once this method is integrated into the security management system, it's part of your continuous improvement activities. It vastly improves the chances of successfully sustaining improvements and enables your organization to look regularly for new and better ways to accomplish objectives and reach goals.

Other key strengths of this approach when applied to GRC² are:

Visibility and structure

This includes clear, prioritized and achievable goals. The LTP approach presents a detailed visual presentation, enabling potential flaws in the security and compliance process to be identified immediately when the analysis is presented to a wider audience. The analysis of each stage links directly into the next one, which provides a coherent, seamless framework. This offers the ability to present highly complex problems and solutions in an easy-to-understand manner.

---

63 H. William Dettmer, "Systems Thinking—And Other Dangerous Habits," Virtualbookworm.com Publishing, 2021.
    Thorsteinn Siglaugsson, "From Symptoms to Causes: Applying the Logical Thinking Process to an Everyday Problem," 2021.

A note on problems vs undesirable effects

Data security and compliance problems come in all shapes and sizes. They can manifest at any time during the control life cycle (see 2016 PSR),64 such as planning and design, implementation, monitoring, and evolution. Some problems are within your control, others aren't. There's seldom a single cause behind an undesirable effect (UDE), but a surprising proportion of UDEs have the same root cause. UDEs can only be eliminated by removing the root causes. As long as a cause remains, the UDE it creates won't be eliminated.

The LTP approaches this by first applying the terminology of "undesirable effects" and avoiding the word "problems" altogether. An UDE is a deviation from any critical success factor, as determined by your Goal Tree. In essence, this means that an UDE is just one way in which current reality differs from your ideal reality. Often, what we call problems are not really the true problems; they are consequences of underlying causes, which are the real problems.

Defining UDEs as deviations from your Goal Tree means that they aren't subjective. They have nothing to do with what you should want or what other people may think is best. You built the Goal Tree, and that's what determines your UDE. So, in a very real way, you choose your undesirable effects in the process of choosing your goals. Ultimately, all of this is within your control.

In this way, the LTP makes difficult problems easier to address, especially when they involve other people, by depersonalizing problems. It avoids appropriating blame and focuses on the chain of events that results in the UDE. Therefore, "undesirable effects" is a useful term because it focuses our attention on the system that produced the effect and its objective analysis.

Clarity and quality of communication

Precision improves communication, lowering the probability for misunderstanding. In addition to sound cause-and-effect relationships, precision requires verification of statements and conditions. "Clarity is the cornerstone of every step of the LTP. The first question to always ask is not only if our statements are true, but also if they are clear. There are no buts and maybes. All conclusions are based on sound logic and all explanations must be sufficiently verified."[65] This process facilitates the enhanced thinking and learning skills of participating individuals, enabling them to handle conflicts with more confidence, correct behaviors that have undesirable consequences and assist in evaluating conditions for achieving desired outcomes.

Improved decision-making

The CISO, steering committee and other participants can make better-informed decisions about the planning and execution of the security and compliance strategy and program.

The LTP also benefits decisions relating to each of the other elements in The Security Management Canvas, including the security business model and security operating model.

---

64 2016 Payment Security Report, Verizon, 2016, https://enterprise.verizon.com/resources/reports/2016/2016-verizon-psr-mainreport.pdf
65 Thorsteinn Siglaugsson, "From Symptoms to Causes: Applying the Logical Thinking Process to an Everyday Problem," 2021.

A foundation for continuous improvements

The LTP provides a structure for continuing advancement. Participants can develop a deeper sense of responsibility for their own actions, through understanding the goals, requirements, constraints and consequences of actions. It also exposes additional capacity without further investment and can enable the security organization to optimize current resources and capacity, rather than spend additional money.

Requirements analysis

The LTP can vastly improve the quality of the requirements analysis by providing clarity and sound reasoning at all stages of the processes, as well as a structured method to formulate projects and strategy.

Refined understanding of constraints

A refined understanding of constraints focuses improvements on areas of greatest impact in the control environment. The determination (analysis, evaluation and documented articulation) of constraints on the security compliance requirements (objectives) makes it easier to find what is slowing down the advancement of the entire control environment. Mapping out goals, requirements and constraints in the Five Trees presents a holistic view of the control environment. The continuous search for constraints gives the security team better control over the overall security and compliance process.

3

State of compliance

The state of
PCI DSS compliance..............

Verizon published the first global analysis of PCI DSS assessments in the 2010 Verizon PCI Compliance Report (renamed the Payment Security Report). Ten years later, in the 2020 publication of this report, we presented several short-, medium- and long-term trends in PCI DSS compliance, revealing the specific compliance strengths and weaknesses within each industry and geographic region. As before, we pinpointed the best- and worst-performing requirements, with a breakdown ranging from high level—PCI DSS Key Requirements and base controls—down to granular details about which test procedures need the most attention within each industry.

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

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

Drawing a distinction between general failures and the failure of control objectives is important. All organizations experience various forms of control failure throughout the year. Failures of individual controls at some point are largely inevitable—but they should be brief. Deviation from control standards should be rapidly detected and corrected. In addition, failure of one or more controls should, in general, not result in a collapse of the entire system, just as the failure of one system should not result in the complete failure of control objectives and of the entire environment.

This is the "defense in depth" principle: To maintain effective data security, control environments need sufficient robustness and resilience built in, even as temporary failures occur.

Dataset
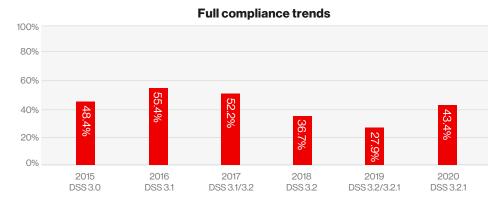
For new readers of the PSR, here is a recap of the dataset (refer to page 142 for additional details and our research methodology). The data reported in this section is taken from draft Interim Reports on Compliance (IROCs). These are formal PCI DSS assessment reports that serve as a snapshot of an organization's PCI DSS state of compliance at a point in time, prior to final assessment. These insightful interim reports capture lapses in controls that can occur as a result of poor compliance management practices or ineffective control design.

Verizon measures compliance performance on three metrics:

- Full compliance
- Control gap
- Use of compensating controls

The state of PCI DSS compliance: Key findings
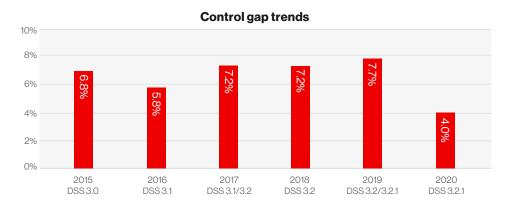
The trend graphs below present an overview of the compliance performance across all DSS requirements for all regions and industries across the globe, for the six-year period between 2015 and 2020. Overall, PCI DSS compliance improved significantly in 2020. The difference in control performance between 2019 and 2020 is indicated in percentage points (pp). Values are not rounded; therefore, the difference in pp values can be off by a decimal, which should have no impact on the interpretation of the data and decision-making.

Full compliance trends

Year	DSS version	Value
2015	DSS 3.0	48.4%
2016	DSS 3.1	55.4%
2017	DSS 3.1/3.2	52.2%
2018	DSS 3.2	36.7%
2019	DSS 3.2/3.2.1	27.9%
2020	DSS 3.2.1	43.4%

Full compliance

The share of organizations achieving 100% PCI DSS compliance at interim validation. This is a reasonable indicator of how well organizations within the dataset managed to sustain compliance by rapidly detecting and correcting controls that fell out of place, and demonstrating 100% compliance when tested prior to their formal annual validation. Nearly all organizations studied passed a previous validation assessment.
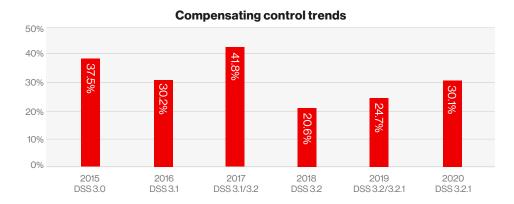
The percentage of organizations maintaining full compliance improved by 15.5 pp, from a low 27.9% in 2019 to 43.4% in 2020.

Control gap trends

Year	Value
2015 DSS 3.0	6.8%
2016 DSS 3.1	5.8%
2017 DSS 3.1/3.2	7.2%
2018 DSS 3.2	7.2%
2019 DSS 3.2/3.2.1	7.7%
2020 DSS 3.2.1	4.0%

Control gap

The "gap" between the measured state of compliance vs having 100% of required controls in place, when measured during interim compliance validation assessments. In other words, the number of failed controls divided by the total number of controls expected. This is an average figure that gives a measure of how far the assessed organizations were from full compliance. For clarity, a low gap is good and a high gap is bad.

The control gap improved substantially in 2020, from a high 7.7% in 2019 (bad) to a low 4.0% in 2020 (better).

Compensating control trends

Year	Value
2015 DSS 3.0	37.5%
2016 DSS 3.1	30.2%
2017 DSS 3.1/3.2	41.8%
2018 DSS 3.2	20.6%
2019 DSS 3.2/3.2.1	24.7%
2020 DSS 3.2.1	30.1%

Compensating controls

This percentage indicates how many organizations used one or more compensating controls when a legitimate technical or business constraint prevented them from meeting a requirement explicitly as stated in the DSS. This percentage is not an indication of how many compensating controls were used.

There is a fair degree of variation on the use of compensating controls, from a high of 41.8% in 2017 to a low of 20.6% measured in 2018. In 2020, the use of compensating controls increased by 5.4 pp, with 30.1% of organizations across the globe applying one or more compensating controls to meet the requirements of PCI DSS v3.2.1.

The overall global average full compliance increased by 15.5 percentage points (pp), from a low 27.9% to 43.4% in 2020. Following three years of full compliance in decline (2017 to 2019), organizations focused their attention on improving security management and governance, resulting in significant gains across six of the 12 Key Requirements.

Full compliance improved for each of the 12 Key Requirements. The most significant improvements are Requirement 12 (20.6 pp gain) and Requirements 10 and 6 (both 10.1 pp gains). Requirement 11 remains the least compliant at 60.7%, followed by Requirements 6 and 2—both at 70.5%. Requirement 11 improved by only 8.8% year-over-year.

Similar to the year before (2019), the two most sustainable key requirements remain Requirements 4 and 7—both achieving a high 90.8% in full compliance.

The reason for this increase in full compliance is likely due to the significant increase in data from the APAC region. APAC data contribution went from 9.3% in 2019 to 23% in 2020. The APAC region as a whole achieved 87.0% full compliance in 2019, and this declined slightly by 2 pp to 85.0% in 2020.

The Americas and EMEA regions both saw a substantial increase in full compliance. The Americas region nearly doubled its region-wide average for full compliance.

In addition, there is also a significant increase in the use of compensating controls, with 30.1% of organizations across the globe applying one or more compensating controls—a 5.4 pp increase from 24.7% in 2019. The use of compensating controls increased across six of the 12 PCI DSS Key Requirements.

Compliance performance in 2020 by PCI DSS Key Requirement

Requirement 1 – Install and maintain network security controls

Requirement 2 – Apply secure configurations to all system components

Requirement 3 – Protect stored account data

Requirement 4 – Protect cardholder data with strong cryptography during transmission

Requirement 5 – Protect all systems and networks from malicious software

Requirement 6 – Develop and maintain secure systems and software

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

Requirement 8 – Identify users and authenticate access to system components

Requirement 9 – Restrict physical access to cardholder data

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

Requirement 11 – Test security of systems and networks regularly

Requirement 12 – Support information security with organizational policies and programs

Full compliance			Control gap			Compensating controls		
Rank		**2020**	**Rank**		**2020**	**Rank**		**2020**
1	**Requirement 4**	90.8%	1	**Requirement 9**	1.6%	1	**Requirement 7**	0.0%
1	**Requirement 7**	90.8%	2	**Requirement 4**	2.1%	2	**Requirement 4**	0.6%
3	**Requirement 5**	88.4%	3	**Requirement 3**	2.6%	3	**Requirement 2**	1.2%
4	**Requirement 9**	85.0%	4	**Requirement 8**	2.9%	3	**Requirement 12**	1.2%
5	**Requirement 3**	84.4%	5	**Requirement 7**	3.1%	5	**Requirement 1**	1.7%
6	**Requirement 8**	83.2%	6	**Requirement 6**	3.2%	5	**Requirement 9**	1.7%
7	**Requirement 1**	78.0%	7	**Requirement 5**	4.3%	7	**Requirement 5**	2.3%
8	**Requirement 10**	76.3%	8	**Requirement 12**	4.9%	8	**Requirement 10**	4.6%
9	**Requirement 12**	75.1%	9	**Requirement 1**	5.1%	9	**Requirement 3**	5.2%
10	**Requirement 2**	70.5%	10	**Requirement 2**	5.2%	10	**Requirement 11**	5.8%
10	**Requirement 6**	70.5%	11	**Requirement 10**	5.5%	11	**Requirement 8**	13.3%
12	**Requirement 11**	60.1%	12	**Requirement 11**	7.4%	12	**Requirement 6**	15.0%

Figure 5. PCI DSS v3.2.1 compliance by key requirement measured in 2020, ranked best (top) to worst (bottom)

The table above presents a high-level snapshot of the state of compliance by measuring PCI DSS Key Requirement compliance performance against the three key metrics: full compliance, control gap and compensating controls.

The release of PCI DSS v4.0 and new requirements it introduced will impact organizations across the globe. The focus of this state-of-compliance analysis is to present the global state of compliance across all industries in support of organizations that need to improve the goal, objectives, requirements and constraints for all key requirements. Detailed analyses of the state of compliance with geographic and industry vertical comparisons are available in separate 2022 PSR data analysis reports.

Full compliance: Here we measure the percentage of organizations that achieved 100% compliance on any particular key requirement, when assessed during their interim compliance validation in 2020. The key requirements are ranked from high to low. The top spot is shared by Requirements 4 and 7 at 90.8%. At the low end, only 60.1% of organizations achieved full compliance on Requirement 11. See pages 130 and 134 for views on Requirement 11.

Control gap: The average control gap across all requirements in the PCI DSS improved substantially, from a high 7.7% in 2019 to a significantly improved 4.0% in 2020. Requirement 11 remains an outlier at 7.4%. Overall, this is a very positive development. Organizations demonstrated that, on average across all key requirements, they could meet the requirements of 96.0% of PCI DSS controls and test procedures, with only 4.0% of controls found not in place during the interim validation assessment.

Compensating controls: The use of compensating controls under Requirements 6 and 8 increased significantly. Requirement 6 remains the key requirement that is most compensated for a second year in a row, followed by Requirement 8. The most significant increase occurred in Control 6.2—Protect components and software from known vulnerabilities (13.9% use), followed by Controls 8.2.4, 8.1.8, and 8.1.6. In general, use of compensating controls is not negative (bad), but it does increase the workload associated with constructing, documenting and validating compensating controls.

Long-term trends

The performance of PCI DSS by key requirement is fairly consistent with marginal long-term variation. This is evident from the long-term (five-year) trends we published on page 68 of the 2020 PSR.

Cream of the crop: The best-performing key requirements continue to be Requirement 7 (Restrict access), Requirement 4 (Protect data in transit), Requirement 5 (Protect against malicious software), and Requirement 9 (Control physical access). Over 80% of organizations keep controls from these key requirements in place.

So-so: These are followed by Requirement 3 (Protect stored cardholder data), Requirement 8 (Authenticate access), Requirement 1 (Install and maintain a firewall configuration) and Requirement 2 (Do not use vendor-supplied defaults). These requirements maintain mediocre performance, where in general, more than 70% of organizations maintain those respective controls.

Bad apples: The worst-performing key requirements still are Requirement 11 (Regularly test security systems and processes), Requirement 6 (Develop and maintain secure systems) and Requirement 12 (Security management) where fewer than 70% of organizations maintain those requirements.

Requirement 11 (Regularly test security systems and processes) remains the worst-performing requirement for more than 10 years running but did improve significantly.

The goals, requirements and constraints of PCI DSS Key Requirements

As mentioned on page 30 (Point 4: Goals specific to PCI security) the overall organizational goal of PCI security compliance can be defined as to develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing protection of payment card data in a consistent, reliable and sustainable manner. To support this overall goal, it's useful to also define the overall individual goal of each of the 12 PCI DSS Key Requirements within its proper operational context. A too-narrow definition and interpretation of the intended function and outcome of any PCI DSS Key Requirement is counterproductive. It can contribute to the failure to structure supporting project tasks and milestones and to secure the investment needed to pursue the achievement of effective, reliable and sustainable security controls.

> The overall organizational goal of PCI security compliance: to develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing protection of payment card data in a consistent, reliable and sustainable manner.

Key requirement goal statements

In the following tables, we included a goal statement that attempts to capture the intended overall outcome of each PCI DSS Key Requirement and its contribution toward meeting the overall goal of PCI DSS compliance. Note that these are initial attempts to produce articulated goal statements, and we look forward to improving and refining these goal statements over time with contributions from the broader payment card industry community, and with closer alignment to the changes introduced by PCI DSS v4.0.

The five fundamental elements that should be present in each PCI DSS Key Requirement goal statement are:

1. **What and why?** This relates to target subject and overall outcomes to be accomplished in context of the overall goal

2. **Who and what?** This relates to the scope; the entities (stakeholders and participants) and material components involved

3. **Will do what?** This describes the action – the essential steps and tasks (objectives) to be initiated and completed

4. **To what level or degree?** This relates to criteria and proficiency needed, and the expected level of performance and achievement

5. **In what length of time?** This is the time frame to complete the objectives and the overall goal

The requirements (necessary conditions): Under what conditions can and should the goal be pursued? Here we are not referring to requirements in the context of PCI DSS security requirements (controls), but the critical success factors and conditions necessary to achieve the goal. These factors and conditions are major milestones or intermediary objectives that describe the situation, setting or given material that will need to be in place for completion of the goal — and in many cases they may overlap with requirements as specified in the DSS. We include examples of some of the primary necessary conditions for achieving the goal. Due to space constraints, only some of the primary necessary conditions are listed, and certainly not all the conditions sufficient to achieve the goal. The examples should help you get started on formulating your own complete list.

Strong dependencies and integration: We list the strongly dependent key requirements in a relative order of the strength of the dependencies and need for integration. It's a short list of strongly dependent key requirements to help support the construction of control systems. There likely is not a single control within the PCI DSS that functions independently of all other controls in the Standard. Every control operates as part of a control system that consists of a collection of controls from various key requirements. It's essential to design security controls in the context of 1) a control system (dependencies and integrations), 2) influences from the control environment (constraints) and 3) the conditions required to meet the intent (compliance). The control environment consists of all the system components (people, priorities, budget, processes, equipment, rules, laws, policies, standards, culture, etc.) that are related to, interact with and influence the control system.

The effectiveness of all key requirements is in some ways dependent on every other key requirement across the DSS. However, some key requirements have stronger dependencies than others. For example, Key Requirements 11 and 6 are conjoined twins. The effectiveness and performance of controls under both key requirements can directly influence each other. Poor performance or failure of a dependent control will affect the performance or can cause failure in other dependent controls. Likewise, improved integration and optimization in one improves performance in the other. This is why we are advocating a systems thinking approach for the goals and requirements of PCI DSS controls.

Objectives: How will progress toward the achievement of the goal be measured? We include considerations for defining relevant short- and long-term objectives as starting points to help decide what should be prioritized and accomplished first in the short term, vs activities that may have a lower priority or require more time to complete. Measuring performance on the completion of objectives is merely one side of the coin. It's also important to measure the improvement of all related processes and capability maturity. Measure what matters to know how effective, reliable and sustainable each key requirement actually is with the amount of resources assigned to it. Also, such measurement provides visibility on the actual performance and areas of development across the control environment.

Level of performance (maturity): It's recommended that the goal statement for each key requirement should include the achievement of a designated target maturity capability level. (See page 25 of the 2019 PSR for details.)

The six designated capability maturity levels 0 through 5 are: 0 – Incomplete, 1 – Performed, 2 – Managed, 3 – Defined, 4 – Quantitatively managed and 5 – Optimized. For the effective operation of the control environment, the core processes and capabilities across all key requirements should be at maturity Level 4 – Quantitatively managed or higher. Any capability lower than 4 negatively impacts the effective and sustainable operation of the control environment, and the security of payment card data. Ideally, organizations should target Optimized maturity (Level 5) if not for all, then for at least the most critical processes. This can initially be expensive to achieve for all processes in terms of time and resource allocation, and may require capacity demands that temporarily exceed some security and compliance teams, but can be a very rewarding investment in the long run.

To meet PCI DSS v4.0 compliance for continuous compliance, measuring control effectiveness, and maintaining compliance as a "business as usual" process, organizations should strive to maintain at least Level 4 maturity.

This is where all core processes are quantitatively managed based on an understanding of the common causes of variation inherent in the process, with established performance measurement baselines, and a focus on continually improving process performance (individual competencies and team capabilities) and incremental improvements of all controls and system components across the control environment.

Constraints

Organizational constraints restrict and limit the performance of the requirements and negatively impact the effectiveness and sustainability with which the control environment is operated and the extent to which it can be improved. Without an effective method, elevating and breaking constraints requires a lot of thinking, analysis and decision-making. Refer to the constraints table on page 68, where we categorized the constraints of organizational proficiency in seven categories: 1 – Capacity, 2 – Capability, 3 – Competence, 4 – Commitment, 5 – Communications, 6 – Culture and 7 – Cost.

It is helpful to understand the distinctions. For example: in general, competence refers to underlying ability of an individual to perform a task, while capability generally refers to the power of an organization to collectively deliver objectives.

Note: The input provided in the following tables is not intended to be exhaustive. It's knowingly incomplete and intended as sample input and a starting point to support the development of articulated goal, objectives, requirements and constraints statements.

Requirement 1:
Install and maintain network security controls

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

Full compliance

■ 2019 ■ 2020

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

68.8%

78.0%

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

% of organizations maintaining full compliance

Control gap

■ 2019 ■ 2020

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

7.4%

5.1%

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

% of controls not in place

Compensating controls

■ 2019 ■ 2020

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

1.9%

1.7%

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

% of organizations using compensating controls
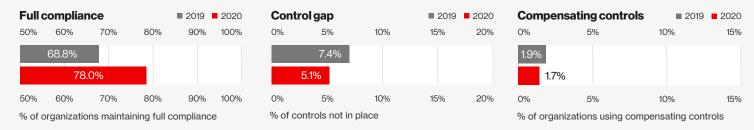
Figure 6. Global state of PCI DSS compliance: Requirement 1

Full compliance:

On average, only 78.0% of organizations across the globe maintained compliance with Requirement 1. The percentage of organizations that kept all controls in place increased by 9.2 pp. Overall, Requirement 1 ranked sixth in terms of full compliance.

Control gap:

The control gap narrowed from 7.4% to 5.1%. This is a much-needed moderate compliance performance improvement. This is the lowest control gap measured by Verizon in over five years (see page 68 of the 2020 PSR for comparative long-term trends).

Compensating controls:

The use of compensating controls remains almost unchanged, at 1.7%. It continues the long-term trend, with few organizations needing to apply a compensating control to meet this requirement, since 2018.

The table below presents the state of PCI DSS v3.2.1 compliance per base control for all organizations across the global dataset.

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

Control gap measures the percentage of controls that were found not in place and needed to be remediated, when checked during an interim compliance validation assessment in 2020. It's determined by calculating the total number of controls assessed for all the related test procedures under a particular control, divided by the controls and test procedures that failed.

Control 1.5 remains the best-performing control in terms of full compliance, scoring 96.5%. Most organizations continue to struggle to keep Control 1.1 – Implement firewall and router configurations – in place. Despite a good improvement (-3.2 pp), Control 1.1 still has the highest control gap, at 6.5%.

Note: It is purely coincidental that the ranking of full compliance from 5 to 1 for this requirement is in sequential order.

PCI DSS v3.2.1 Requirement 1		Full compliance				Control gap			
Performance year-over-year, ranked best (1) to worst		2019	Change	2020	Rank	2019	Change	2020	Rank
1.1	Implement firewall and router configurations	72.3%	+8.7 pp	81.0%	5	9.7%	-3.2 pp	6.5%	5
1.2	Restrict connections between CDE and untrusted networks	85.2%	+3.3 pp	88.5%	4	7.5%	-1.9 pp	5.6%	4
1.3	Prohibit direct public access between internet and CDE	88.4%	+5.8 pp	94.2%	3	4.6%	-1.4 pp	3.2%	1
1.4	Install personal firewall software	92.3%	+3.1 pp	95.4%	2	5.5%	-2.3 pp	3.2%	2
1.5	Document policies and procedures for managing firewalls	94.2%	+2.3 pp	96.5%	1	5.8%	-2.3 pp	3.5%	3

Figure 7. Requirement 1 control performance

A tip on sustainable control effectiveness
Firewalls are a first line of network and application system defense, helping to ensure that strict control over configurations is maintained. To improve firewall effectiveness and sustainability, and prevent controls from falling out of compliance, organizations should automate the maintenance of their system and configuration management and integrate it with change control support systems. The effectiveness of this requirement strongly depends on other requirements, such as Requirement 10. The logs and alerts generated by firewalls and intrusion detection and prevention systems (IDS/IPS) require special attention.

Requirement 1: Install and maintain network security controls

The goal	The goal of PCI DSS Key Requirement 1 is to maintain reliable and sustainable operation and management of network security controls across the in-scope environment, delivering consistent and effective network and application access control to and from the CDE by restricting access to authorized users and systems only, and to support ongoing monitoring and detection of security events and response to incidents.
	This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	This goal applies to all people (internal and external) involved in the evaluation, implementation, operation and management of any in-scope network security component, i.e., all logical (IT) and physical security control components required to restrict network access to and from the CDE.
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capacity:** Maintain the capacity needed for qualified security administrators to proactively and correctly configure, monitor and maintain the security controls in accordance with the intent of the related PCI DSS control objectives • **Competence:** Maintain the competency to evaluate, install and maintain all network security controls across the in-scope environment in an effective, reliable and sustainable manner • **Capability:** Test and measure the consistency and effectiveness of the ongoing restriction of network access to and from the CDE, to limit access to authorized users and systems only, to support monitoring and detection of security events and response to incidents (the team capability) • **Technology:** Maintain modern, up-to-date hardware and software components, and replace outdated technologies across the control environment; automation of change control • **Documentation and processes:** Maintain effective standard operating procedures, with clearly articulated standards, roles and responsibilities. Regularly train and educate staff on how to follow the documented procedures. Frequent internal monitoring and reporting of adherence to standards and procedures

Strong dependencies and integration with other key requirements	• **Requirement 10:** Logging and monitoring of network security control components • **Requirement 2:** Secure configuration of network security controls • **Requirement 6:** Hardening of network security components • **Requirement 11:** Testing of network security components
Short-term objectives	• **Scope:** Install and maintain access control equipment that covers the entire CDE in accordance with documented standards and procedures. Validate the sufficiency (accuracy and completeness) of the scope • **Update:** Replace or update IT components that lack the functionality and capability to provide effective network security control • **Change control:** Enhance automation of configuration deployment and change control management
Long-term objectives	• **Improve:** Improve and refine configurations and support processes, integration, documentation and training • **Maturity:** Achieve and maintain high-capability maturity and performance on all security control operations, with low deviation from configuration standards and high capability for the rapid detection and correction of configuration deviations across the CDE
Common constraints	• **Capacity:** Insufficient capacity of security control administration personnel to manage security component deployment, configuration, monitoring and maintenance tasks with sufficient performance • **Cost:** Lack of budget to update outdated technology and/or increase staff capacity • **Competency:** Lack of staff qualified to configure, operate and manage network security components

Note: The GRC[2] template sample in the table above is explained on page 86 of this report.

Requirement 2:
Apply secure configurations to all system components ··········▶

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

Full compliance ■ 2019 ■ 2020

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

64.9%

70.5%

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

% of organizations maintaining full compliance

Control gap ■ 2019 ■ 2020

0%	5%	10%	15%	20%

7.0%

5.2%

0%	5%	10%	15%	20%

% of controls not in place

Compensating controls ■ 2019 ■ 2020

0%	5%	10%	15%

6.5%

1.2%

0%	5%	10%	15%

% of organizations using compensating controls

Figure 8. Global state of PCI DSS compliance: Requirement 2

Full compliance

Full compliance improved by 5.6 pp, from 64.9% to 70.5%. Despite the improvement, Requirement 2 is (jointly with Requirement 6) the second-lowest-performing key requirement in terms of full compliance.

Control gap

The control gap improved slightly, decreasing from 7.0% to 5.2%. Requirement 2 has the third-highest control gap, after Requirements 11 and 10. Control 2.4 (inventory of system components) features in the Bottom-20 lists of controls. (See page 140).

Compensating controls

The use of compensating controls reduced significantly between 2019 and 2020, from 6.5% to 1.2%—the lowest use of compensating controls for Requirement 2 since at least 2015.

Requirement 2 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
2.1	Change vendor defaults, disable unnecessary accounts	85.8%	+6.1 pp	91.9%	3	4.4%	-2.0 pp	2.4%	2
2.2	Develop configuration standards	78.1%	+4.0 pp	82.1%	5	7.8%	-1.3 pp	6.5%	5
2.3	Encrypt nonconsole administrative access	89.0%	+2.9 pp	91.9%	3	5.5%	-2.1 pp	3.4%	3
2.4	Maintain an inventory of in-scope system components	76.1%	+5.4 pp	81.5%	6	19.4%	-5.2 pp	14.2%	6
2.5	Policy and procedures for managing vendor defaults	94.2%	+2.3 pp	96.5%	2	5.8%	-2.3 pp	3.5%	4
2.6	Document policies and procedures for managing firewalls	98.7%	+1.3 pp	100.0%	1	1.3%	-1.3 pp	0.0%	1

Figure 9. Requirement 2 control performance

A tip on sustainable control effectiveness
Organizations are often unaware that vendor default settings are used on system components within the CDE, due to third-party installation and other reasons. It's critical to increase internal training on secure configuration standards as well as to automate the management and maintenance of devices to maintain cryptographic keys and configuration and authentication settings, and to schedule frequent internal assessments to confirm compliance.

Requirement 2: Apply secure configurations to all system components

The goal	The goal of PCI DSS Key Requirement 2 is to develop, apply and maintain an effective, secure configuration management capability to all in-scope system components, reducing the means available to an attacker to ensure the CDE is not susceptible to attack. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	This goal applies to all in-scope system components, i.e., all applicable hardware and software applications, including wireless network components and components hosted in cloud environments, individuals and teams responsible for implementing and maintaining security configurations, and third parties that support IT system components.
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability—scope control:** Create the capacity and ability for effective and sustainable ongoing identification of all in-scope digital assets and system components included in the security configuration management program • **Capability—change control:** Develop an ability for effective, ongoing monitoring, recording, detection and response to configuration changes made to any in-scope component, and include discernment between authorized vs unauthorized modifications • **Effective communication:** Maintain a complete set of documented configuration and system hardening policies, standards and procedures—with detailed change control standards and procedures for applying hardening standards that cover all types of system components and address all known security vulnerabilities. This should include procedures for removing unnecessary functionality from hardware and software applications, changing vendor defaults and commonly known default credentials or security parameters, and securing administrative access removed to avoid system components to ensure that they are not susceptible to attack upon implementation or after making any updates or changes • **Operating procedures:** Maintain effective, clearly articulated standard operating procedures, regular training and staff education for meeting security change-configuration program performance standards • **Ongoing commitment:** Include the formal assignment of roles and responsibilities to implement and adhere to policies, standards and procedures; measurement, reporting and improvement of security configuration management performance; and ongoing education and training of system administrators
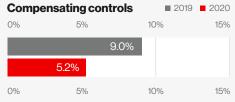
Strong dependencies and integration with other key requirements	• **Requirement 6:** Integration with system hardening requirements • **Requirement 1:** Secure configuration of security network control components • **Requirement 11:** Testing if changes to configurations resulted in or solved vulnerabilities • **Requirement 10:** Logging and monitoring of network security control components
Short-term objectives	• **Scope and automation:** Implement and maintain a configuration management system for the effective, automatic identification and status synchronization and reporting of all in-scope components across the entire CDE • **Communication:** Document and effectively communicate configuration standards and implementation, management and monitoring procedures for all system components across the CDE
Long-term objectives	• **Improvement:** Improve and refine configurations and support processes, integration, documentation and training • **Maturity:** Achieve and maintain high-capability maturity and performance on all secure configuration operations, with low deviation from configuration standards and high capability for the rapid detection and correction of configuration nonconformities across the CDE
Common constraints	• **Capacity:** Not having sufficient capacity of personnel to staff the secure configuration management team. Lack of proper identification of components due to lack of time and automation tools • **Cost:** Lack of budget to procure the tools needed to automate the configuration management functions • **Competency:** Lack of staff qualified to effectively apply secure configuration management tasks

Requirement 3: Protect stored account data ·······················▶

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

Full compliance   ■ 2019 ■ 2020

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

76.6%
84.4%

% of organizations maintaining full compliance

Control gap   ■ 2019 ■ 2020

0%	5%	10%	15%	20%

5.6%
2.6%

% of controls not in place

Compensating controls   ■ 2019 ■ 2020

0%	5%	10%	15%

9.0%
5.2%

% of organizations using compensating controls

Figure 10. Global state of PCI DSS compliance: Requirement 3

Full compliance

At 84.4% global average, this requirement shows good improvement and ranked fourth overall on full compliance. It's the first time in over five years that full compliance with Requirement 3 exceeds 80%.

Control gap

The gap narrowed significantly, resulting in the third-lowest control gap overall—a very positive development. The reduction in control gap is mainly due to significant improvements in Control 3.4 and Control 3.2.2.

Compensating controls

The use of compensating controls under Requirement 3 declined significantly—by nearly half—from 5.6% down to a low 2.6%. While this is the lowest use since at least 2015, it still ranked the fourth highest use of compensating controls across the 12 Key Requirements.

Requirement 3 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
3.1 Keep data storage to a minimum		90.3%	+4.5 pp	94.8%	4	6.7%	-3.0 pp	3.7%	7
3.2 Do not store SAD after authorization		88.4%	+8.1 pp	96.5%	2	6.5%	-4.8 pp	1.7%	1
3.3 Mask primary account numbers (PANs) when displayed		92.3%	+3.1 pp	95.4%	3	6.0%	-2.9 pp	3.1%	6
3.4 Render PANs unreadable anywhere they are stored		86.5%	+8.3 pp	94.8%	4	5.0%	-3.0 pp	2.0%	2
3.5 Protect keys used to secure stored CHD against disclosure		88.4%	+4.1 pp	92.5%	6	5.2%	-2.6 pp	2.6%	4
3.6 Key-management processes		87.7%	+4.2 pp	91.9%	7	5.4%	-2.5 pp	2.9%	5
3.7 Documented policies for protecting stored CHD		92.3%	+5.4 pp	97.7%	1	7.7%	-5.4 pp	2.3%	3

Figure 11. Requirement 2 control performance

A tip on sustainable control effectiveness
It's smart to automate payment transaction data discovery, using appropriate tools to execute. Consistently apply it on the correct scope to avoid accidental exclusions. Report the actual performance of data retention. Enforce continuous improvement on the consistency, so that staff diligently follow these policies and procedures.

Requirement 3: Protect stored account data

The goal	The goal of PCI DSS Key Requirement 3 is to develop, execute and maintain a sustainable capability for the ongoing effective, reliable and sustainable protection of all stored account data across the control environment, keep the storage of account data to a minimum and prevent the storage of SAD post-authorization unless needed for card-issuing functions.
	This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• The goal applies to the storage of all PCI-branded cardholder data (CHD) and/or SAD in electronic and hardcopy formats and related system components
	• It applies to data at rest in all storage locations (servers, databases, storage arrays or areas, removable disks, CDs), and includes storage in nonvolatile memory (disks and storage chips)
	• The scope includes the management of responsibilities of any third parties involved in the transmission, storage and processing of account data
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability – scope control:** The ability to effectively and continuously manage the CDE scope by identifying, tracking, recording and reporting all CHD storage, processing and transmission locations across the CDE, and rapid detection and response to any unintentional storage of account data outside the defined CDE
	• **Capability – maintaining minimal data retention:** Monitor, record and report data storage retention periods of account data, with documented business justifications for each retention period or duration
	• **Capability – data removal:** Effectively and timely secure permanent deletion or destruction of all account data that lacks a valid business justification for the retention of the data
	• **Capability – data protection:** Effectively and continuously protect all stored CHD in a sustainable manner with approved mechanisms (masking, truncation, tokenization, encryption with secure cryptographic keys management)
	• **Third parties:** Manage contractually (by stipulating data protection and incident response responsibilities) any account data received or shared with third parties that is not under the direct control of your organization
	• **Documentation and processes:** Maintain effective standard operating procedures, with clearly articulated standards, roles and responsibilities. Regularly train and educate staff on how to follow the documented procedures. Frequently monitor and report adherence to procedures
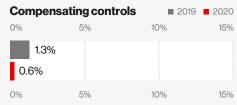
Strong dependencies and integration with other key requirements	• **Requirement 6:** Integration with system-hardening requirements • **Requirements 7 & 8:** Secure authentication and access control to components that store CHD • **Requirement 10:** Logging and monitoring of components that store CHD and related security systems • **Requirement 11:** The testing of components that store CHD and related security systems • **Requirement 12:** Ongoing contractual management of third-party data security responsibilities
Short-term objectives	• **Scope:** Develop and execute a process to accurately map and communicate the entire scope of the CDE • **Automation:** Perform ongoing data discovery with the use of data loss prevention (DLP) tools to effectively detect and report the presence of account data within and outside the defined CDE, and timely correction (inclusion) of in-scope components • **Minimal data retention:** Maintain a process for the secure and permanent deletion or destruction of account data that is not needed • **Data protection:** Frequently measure and report the effectiveness of all stored CHD protection procedures
Long-term objectives	• **Performance management:** Develop the ability for the ongoing measurement, reporting and improvement of CHD protection performance, including the frequency and duration of deviation from established CHD security policies, standards and procedures and the ability to communicate its impact on the effective and sustainable protection of stored CHD • **Maturity:** Achieve and maintain high-capability maturity and performance on the protection of stored CHD. Improve and refine support processes, automation, documentation and training
Common constraints	• **Capability:** Difficulty locating account data across the CDE; lack of capacity and automation • **Competency:** Improper understanding of cryptography and key-management procedures. Not demonstrating the consistent and effective use of cryptographic solutions to protect stored CHD. Limited overview around maintaining cryptographic architecture and infrastructure

Requirement 4:
Protect cardholder data with strong cryptography during transmission

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

Full compliance ■ 2019 ■ 2020

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

86.4%

90.8%

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

% of organizations maintaining full compliance

Control gap ■ 2019 ■ 2020

0%	5%	10%	15%	20%

3.8%

2.1%

0%	5%	10%	15%	20%

% of controls not in place

Compensating controls ■ 2019 ■ 2020

0%	5%	10%	15%

1.3%

0.6%

0%	5%	10%	15%

% of organizations using compensating controls

Figure 12. Global state of PCI DSS compliance: Requirement 4

Full compliance

A slight improvement on full compliance from 86.4% to 90.8%—exceeding 90% for the first time in over five years.

In terms of long-term trends, Requirement 4 consistently maintains a highest level of full compliance, together with Requirements 7 and 5.

Control gap

The control gap narrowed to 2.1%, to the lowest level in more than five years. Requirement 4 has the least amount of controls across the PCI DSS—with only three controls and 12 test procedures.

Compensating controls

In the 2020 dataset, the use of compensating controls reached nearly zero. Historically, the use of compensating controls remains consistently very low for this requirement.

Requirement 4 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
4.1	Use strong cryptography and protocols	89.7%	+2.8 pp	92.5%	3	3.3%	-1.1 pp	2.2%	2
4.2	Never send unprotected PANs by end-user messaging	91.6%	+5.5 pp	97.1%	2	5.2%	-3.8 pp	1.4%	1
4.3	Procedures for encrypting transmissions of CDE	93.5%	+4.1 pp	97.6%	1	6.5%	-4.1 pp	2.4%	3

Figure 13. Requirement 4 control performance

A tip on sustainable control effectiveness
Ensure that wireless networks are configured to support strong encryption for authentication and transmission. Wired Equivalent Privacy (WEP) and Secure Sockets Layer (SSL) are not considered secure and must be removed from all existing wireless network configurations and other components. Automate the detection and reporting of unknown and rogue wireless access points. Maintain a capability to effectively monitor and respond to detection alerts; measure and report control performance over time.

Requirement 4: Protect cardholder data with strong cryptography during transmission

The goal	The goal of PCI DSS Key Requirement 4 is to develop, execute and maintain a sustainable capability for the effective monitoring and protection of CHD across the CDE, through the application of strong cryptography to protect primary account numbers (PANs) during transmission of the PAN over open, public networks. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• The goal applies to all system components across the CDE where any PAN is transmitted over open, public networks, such as the internet, messaging systems or wireless technologies, including Wi-Fi, Bluetooth®, cellular technologies, satellite communications and General Packet Radio Service (GPRS) components • It also applies to all security system components (technology and people) that support the security controls needed to meet this key requirement, such as systems that support security certificates, cryptographic systems, and logging and monitoring systems
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Documentation and processes:** Maintain effective standard operating procedures with clearly articulated standards, roles and responsibilities. Regularly train and educate staff on how to follow the documented procedures. Internally monitor and report adherence to procedures • **Competency:** The correct design, implementation, operation and maintenance of strong cryptography and certificate systems for securing data in transit or in motion; safeguarding CHD before and during transmission of the PAN over open, public networks • **Capability—scope management:** The ability to continuously identify, monitor and improve all system components where the PAN is transmitted over open, public networks, to meet and maintain the compliance requirements. Internally monitor and report scope nonconformity and violations
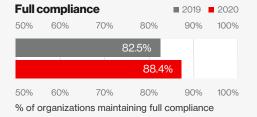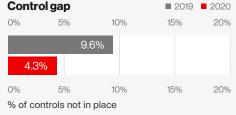
Strong dependencies and integration with other key requirements	• **Requirement 6:** Integration with system-hardening requirements • **Requirements 7 & 8:** Secure authentication and access control to components that store CHD • **Requirement 10:** Logging and monitoring of components that store CHD and related security systems • **Requirement 11:** The testing of components that store CHD and related security systems • **Requirement 12:** Ongoing contractual management of third-party data security responsibilities
Short-term objectives	• **Capability — scope and automation:** Implement and maintain a system for the effective, automatic identification and reporting of the configuration and security status of all components that transmit CHD • **Capability — detect and respond:** Develop and improve the ability to rapidly detect and respond to any clear-text transmission of the PAN from within the organization over open, public networks
Long-term objectives	• **Improvement:** Improve and refine configurations, integration, support processes, documentation and training on all relevant system components • **Maturity:** Achieve and maintain high-capability maturity and performance on all the protection of CHD during transmission, with low deviation from configuration standards, and high capability for the rapid detection and correction of configuration nonconformities across the CDE
Common constraints	• **Competency — scope management:** Failure to include all applicable wireless technologies in the scope of compliance and validation • **Competency — security proficiency:** Insufficient mastery of cryptographic industry standards, cryptography implementation and key management procedures, improper comprehension or inconsistent operation of security certificate management procedures, ineffective maintenance of cryptographic architecture and infrastructure • **Capability — secure operations:** Ineffective design, operation and management of secure end-user messaging technologies • **Cost and capacity:** The cost and effort of upgrading outdated cryptographic protocols across a large environment with many affected components

Requirement 5:
Protect all systems and networks from malicious software ···········▶

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

Full compliance   ■ 2019 ■ 2020

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

82.5%
88.4%

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

% of organizations maintaining full compliance

Control gap   ■ 2019 ■ 2020

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

9.6%
4.3%

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

% of controls not in place

Compensating controls   ■ 2019 ■ 2020

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

1.3%
2.3%

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

% of organizations using compensating controls

Figure 14. Global state of PCI DSS compliance: Requirement 5

Full compliance

Full compliance improved from 82.5% to 88.4%, which is still a bit lower than its 90%-plus performance in 2015 and 2016. In relation to long-term trends, Requirement 5 consistently maintains the highest level of full compliance, together with Requirements 7 and 4.

Control gap

The improvement of the control gap doubled, with the gap reducing from a high of 9.6% to a more respectable 4.3%.

While the gap with Control 5.2 improved significantly (-4.7 pp), it remains the worst-performing control under Requirement 5.

Compensating controls

The use of compensating controls increased to 2.3%. Control 5.2 is compensated the most, but by a very small number of organizations (1.2%) with a legitimate business or technical reason for not being able to maintain all anti-malware systems.

Requirement 5 controls		Full compliance				Control gap			
Performance year-over-year, ranked best (1) to worst		2019	Change	2020	Rank	2019	Change	2020	Rank
5.1	Deploy antivirus software	87.1%	+8.3 pp	95.4%	2	9.5%	-6.4 pp	3.1%	2
5.2	Maintain all antivirus mechanisms	85.8%	+3.2 pp	89.0%	4	10.3%	-4.7 pp	5.6%	4
5.3	Antivirus actively running and cannot be disabled	89.0%	+4.6 pp	93.6%	3	9.9%	-5.5 pp	4.4%	3
5.4	Document policies for malware protection	94.2%	+3.5 pp	97.7%	1	5.8%	-3.5 pp	2.3%	1

Figure 15. Requirement 5 control performance

A tip on sustainable control effectiveness
Antivirus solutions are only as good as the detection technology and definitions they are running. Permit automatic updating of antivirus mechanisms and, where possible, restrict the operation of systems running outdated definitions. Integrate endpoint solutions and automate monitoring and management.

Requirement 5: Protect all systems and networks from malicious software

The goal	The goal of PCI DSS Key Requirement 5 is to ensure that all relevant systems across the CDE commonly affected by malicious software remain protected at all times against known and evolving malware threats with an effective anti-malware solution, and that organizational capability to respond to malware-related incidents is continuously in place and corrective action is taken in a timely manner to prevent or contain malware contamination of the CDE. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **Technology components:** This goal applies to all in-scope system components known to be affected by malware, which may include servers, employee computers, mobile computers, email systems and storage devices, including related logging, monitoring and incident response systems • **People and teams:** The goal also includes the individuals and teams responsible for the deployment, monitoring and response to malware-related incidents, the training and education of end users that access any CDE system components, and third-party vendors that supply or support anti-malware and related security system components
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability – deployment:** Create a standardized deployment and maintenance process capability for the anti-malware system to be installed and remain active on all in-scope system components, which includes a defined process for identifying in-scope components, i.e., systems commonly affected by malware • **Capability – anti-malware functions:** Install anti-malware systems capable of detecting various types of malicious software to protect systems from current and evolving malware threats, including viruses, worms, Trojans, spyware, adware, ransomware, keyloggers, rootkits, malicious code, scripts and malicious links on in-scope system components, such as servers, employee computer systems, mobile computers, email systems and storage devices. It must include automated regular updates, generating alerts • **Capability – automation and monitoring:** Standardize and automate the deployment and maintenance of anti-malware systems; particularly in large environments, automate the inability to disable anti-malware without management approval, and automate alerts and the ability to detect an alert when an anti-malware system is inactive on an in-scope component • **Capability – detection and response:** Integrate anti-malware systems, network access control (NAC) systems and a centralized security information and event management (SIEM) system for the aggregation of security log data across CDE for normalization, analysis and effective monitoring and response • **Documentation and processes:** Maintain effective standard operating procedures, with clearly articulated standards, roles and responsibilities. Regularly train and educate staff on how to follow the documented procedures. Internally monitor and report adherence to procedures

Strong dependencies and integration with other key requirements	• **Requirement 1:** Integration with network security components, for network-based anti-malware protection • **Requirement 2:** The security configuration of anti-malware system components • **Requirement 6:** Integration with system hardening of components, such as NAC • **Requirement 10:** Integration with logging and monitoring systems • **Requirement 11:** Sufficient security testing of anti-malware systems • **Requirement 12:** The risk-based re-evaluation of systems not known to be affected by malware
Short-term objectives	• **Scope and automation:** Implement and maintain a configuration management system for the effective, automatic identification and status synchronization and reporting of all in-scope components across the entire CDE • **Communication:** Document and communicate configuration standards and implementation procedures, management and monitoring procedures for all system components across the CDE
Long-term objectives	• **Improvement:** Improve the integration of security and refine configurations and support processes, documentation and training, monitoring, and reporting • **Maturity:** Achieve and maintain high performance of process and capability maturity on the deployment, maintenance and monitoring of anti-malware components, alerts and incident response
Common constraints	• **Cost:** Lack of budget to deploy and maintain advanced integrated endpoint security solutions • **Competency:** Lack of qualified staff to properly integrate and maintain various endpoint solutions

Requirement 6: Develop and maintain secure systems and software

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

Full compliance

| | 2019 | 2020 |

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

60.4%

70.5%

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

% of organizations maintaining full compliance

Control gap

| | 2019 | 2020 |

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

6.7%

3.2%

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

% of controls not in place

Compensating controls

| | 2019 | 2020 |

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

11.0%

15.0%

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

% of organizations using compensating controls

Figure 16. Global state of PCI DSS compliance: Requirement 6

Full compliance

There was a very substantial 10.1 pp increase on Requirement 6, from a low 60.4% to 70.5%. Organizations applied more focus on patching and software vulnerability management. The improvement in full compliance may also be influenced by the increase in compensating controls.

Control gap

The control gap narrowed considerably from 6.7% to a relatively low 3.2%. This is due in part to improvements in Control 6.2, where compliance against 6.2.b improved by 11.4 pp, and Control 6.2 improved by 9.0 pp.

Compensating controls

The use of compensating controls increased from 11.0% to 15.0%. Requirement 6 is, for a second year in a row, the requirement that is most compensated, followed by Requirement 8. Control 6.2 was compensated by an average of 14.5% of organizations (+4.1 pp); there was a small increase in the compensating of Control 6.4.

Requirement 6 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
6.1	Use reputable outside sources for vulnerability information	91.6%	+4.9 pp	96.5%	1	6.5%	-3.6 pp	2.9%	2
6.2	Protect components and software from known vulnerabilities	72.9%	+10.9 pp	83.8%	7	17.4%	-9.0 pp	8.4%	7
6.3	Develop secure software applications	90.3%	+5.1 pp	95.4%	3	6.3%	-3.8 pp	2.5%	1
6.4	Follow change-control processes	83.9%	+4.0 pp	87.9%	6	7.5%	-4.6 pp	2.9%	2
6.5	Address common coding vulnerabilities	86.5%	+3.7 pp	90.2%	5	4.4%	-1.5 pp	2.9%	2
6.6	Protect public-facing web applications against known attacks	92.3%	+2.5 pp	94.8%	4	7.7%	-2.5 pp	5.2%	6
6.7	Policies and procedures for secure systems	91.6%	+4.9 pp	96.5%	1	8.4%	-4.9 pp	3.5%	5

Figure 17. Requirement 6 control performance

A tip on sustainable control effectiveness
All system components within and connected to the CDE need to be properly hardened before placed into production—and then maintained. It's important to sign up for vendor security notifications; most support an email alert service or RSS feed, and many offer tailored feeds based on specific solutions or technologies. Monitor these alerts on a daily basis. Organizations save administrators time by automating the deployment of patches.

For example: Deploy a solution such as Microsoft Endpoint Configuration Manager in Microsoft environments.

Requirement 6: Develop and maintain secure systems and software

The goal	The goal of PCI DSS Key Requirement 6 is to achieve and sustain a mature process and capability for developing and maintaining secure software and systems for all relevant system components across the CDE, and to continuously improve processes and capabilities for the effective, reliable and sustainable protection of account data. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **Components:** This goal applies to all applicable system components across the CDE, such as routers, firewalls, operating systems, application software, databases, point-of-sale (POS) terminals, internet browsers, etc., that need to be patched in a timely manner • **Security tools:** The management of web application firewalls (WAFs) and application security assessment tools • **People:** All software developers involved with developing software for CHD-related components, the teams and individuals conducting application assessments and patching, and system-hardening tasks for in-scope systems • **Documentation:** Software development procedures, secure coding life-cycle management methodologies, detailed application security assessment standards and procedures, and security patch management standards and procedures applicable to all relevant components within the CDE
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability—patching:** Maintain a mature capability to manage IT component vulnerabilities through regular, timely and consistent application of security patches, to all relevant components • **Identification of software vulnerabilities:** Develop the capability to effectively identify and process security vulnerabilities—including applicable vulnerabilities for bespoke, custom and vendor software—using industry-recognized sources for security vulnerability information; assign risk ranking to vulnerabilities to include identification of all high-risk and critical vulnerabilities • **Competency:** Effectively use WAFs in front of public-facing web applications, and use web application security assessments to monitor, detect and prevent web-based attacks • **Competency—secure software development:** Properly train software development personnel in secure development practices, software security and attacks to identify and resolve issues related to common coding vulnerabilities. This includes establishing the capacity, competency and organizational capability to manage the full scope of secure system and software activities • **Documentation and processes:** Maintain effective standard operating procedures with clearly articulated standards. Regularly train and educate staff on how to follow the documented procedures

Strong dependencies and integration with other key requirements	• **Requirement 11:** Very strong dependency and integration with security vulnerability testing • **Requirement 12:** Integration and dependency with risk analysis and management practices • **Requirement 2:** Strong dependency and integration with secure configuration practices • **Requirements 7 & 8:** Secure authentication and access control to components that transmit CHD
Short-term objectives	• **Scope:** Develop and maintain the capability to accurately identify, report and monitor a dynamic inventory of in-scope hardware and software assets; create prioritized task lists for securing systems and software across the CDE • **Capacity planning:** Calculate the resources (people, budget, time) needed, and effectively communicate the assigned roles, responsibilities and workload to achieve the goal for Requirement 6 • **Inventory management:** Proactive identification, planning, communication and execution of a treatment plan to effectively address all end-of-life technologies for all related components within the CDE • **Communication:** Complete the set of documentation, which is extensive for this key requirement. Standardize, document and communicate all related processes and procedures in support of this key requirement
Long-term objectives	• **Constraints:** Remove business and technical constraints that prevent timely patching of systems • **Maturity:** Achieve and maintain high-performance maturity for managing time-sensitive patch updates to ensure that all in-scope system components have as few vulnerabilities as possible. Improve and refine configurations, support processes, documentation and training
Common constraints	• **Capacity:** Not having sufficient resources (people, time and budget) to attend to scope of the tasks required to meet the goal and objectives of Requirement 6, such as keeping up with new vulnerability notifications • **Capability:** Technology constraints where equipment does not support required software updates • **Cost:** Lack of budget to upgrade systems and improve tools to support the objectives of this requirement • **Competency:** Lack of staff qualified to design and implement effective secure systems and software programs • **Commitment:** Conflicting priorities; not investing focused time and resources on Requirement 6 activities

Addressing the cause to avoid treating the symptoms

How clarity on goals, requirements and constraints strengthens the control environment

With proper planning, design and execution, PCI security compliance programs succeed quietly, protecting payment card data day after day. Then there are the programs that fail spectacularly, sometimes resulting in a publicly disclosed compromise. The success of the PCI DSS over its nearly 20-year history is punctuated by several high-profile payment card data breaches, and those massive program failures make sensational stories. Not surprisingly, all findings and data made available from various PCI Forensic Investigator (PFI) investigations confirm that none of the organizations that experienced confirmed payment card data breaches were compliant with the PCI DSS requirements at the time of the breach. Furthermore, no known, disclosed and documented cases exist of any payment card data breach where evidence supported that the breached entity had all required PCI DSS controls in place at the time of the breach. In all known cases, numerous key security requirements were not in place—usually with several being material to the breach. This is well documented in several of our previous PSR editions.

That there are negative consequences of a data compromise is a cold, hard reality. In the aftermath, a company's CISO, its security team and others find themselves in the hot seat, responding to tough questions from senior management and third-party forensic investigators—about the what, when, where, how and why of the data compromise.

Publications like the Verizon Data Breach Investigations Report (DBIR) provide the opportunity to learn from others' mistakes. It's critical to document who is targeted by which threat actors, how the threat actors succeeded in breaching the organization, and what the consequences were. In addition to dissecting what went wrong, it's important to review the available data to understand the lessons of exactly how and why data breaches happen, to avert—or at least mitigate—the impact of future breaches.

Moving from symptoms to causes: Understanding the why

It's typical for data breach investigations to uncover several security controls that were not in place at the time of a breach. Breaches often involve a combination of contributing factors that expose human errors, including control design flaws, implementation errors, unpatched systems, etc. But why? Detective work is necessary to determine if the security environment and controls were designed improperly, maintained poorly or simply neglected—or any combination thereof. Did inadequate support processes allow security deficiencies to go unnoticed—or worse, noticed but uncorrected? For what seems to be just a few situations, countless additional "whys" crop up. Was the breached environment designed or implemented improperly because of poor staffing or lack of competence? Ineffective use of security tools is a common contributing factor; the tools may be in place, but the staff is not sufficiently trained to use the

tools to effectively detect and respond to a security incident. Was a culture of indifference to compliance, quality and standards a factor?

In broad terms, the first objective of incident response is not to determine how and why the breach occurred; rather it's to contain the breach and stop the data leak (although, sadly, sometimes our Verizon Threat Research Advisory Center [VTRAC] investigators have the additional task of asset discovery before the collection and analysis effort can be initiated). This is followed by determining the scope and full extent of the breach. Once these activities are completed, the focus can then shift to understanding how and why the breach happened, which controls failed or were not in place to begin with, and to what extent the not-in-place controls led or contributed to the breach. The investigating team then begins the journey of scrutinizing the control environment, working their way back through multiple layers of controls and constraints that impacted the effectiveness of the in-place defenses.

Peeling back the layers: Exposing cause-and-effect relationships

This inevitably leads to uncovering the differences between perception and reality—laying bare poor organizational management practices, operational design, and execution and monitoring deficiencies. Each can contribute to a weakened control environment. Most issues are symptoms that result from poor planning or failing to include them in a strategic plan, starting with inadequate leadership and ending

with commitment, communication and culture issues. Such concerns are a combination of Verizon's Top 7 Strategic Data Security Management Traps (see page 12 of the 2020 PSR). The focus then shifts toward presenting a clear understanding of the remediation steps needed to enhance the security posture to prevent—or at least mitigate—a repeat of the same or similar incidents. The end of a data breach investigation concludes with the presentation of a final management report documenting findings and recommendations. A good report and presentation include an overview of the critical decisions that were made and not made, and the initial key factors that contributed to control failures down the line. The process may also include presenting the findings and recommendations to the board. The presentation should describe, where possible, what the exact or most likely issues were that resulted in the security incident turning into a data breach. Understandably, the board should be most interested in the way forward—the corrective actions required. They are also interested in the critical processes and capabilities needed to achieve a level of security and compliance maturity needed to deliver a proven (assured) level of effectiveness and sustainability. Enabling this understanding is a somewhat daunting and complex endeavor.

With security breaches becoming increasingly common, experienced security professionals are simplifying the complexity of this communication. It requires distilling the presentation content down to root causes and main contributing factors, to clarify the goal of security and compliance that the organization actually pursued (expectations vs reality), and what contributed to conditions that resulted in a security compromise.

PCI DSS controls that lack reliability and sustainable effectiveness are, in most cases, merely a symptom of an organizational lack of commitment to specify a level of assurance that includes those performance qualities (reliability, effectiveness and sustainability in design and operation). These are necessary requirements and objectives of security and compliance goals and should be incorporated as key elements in the security strategy.

Be very explicit about what you are aiming for.

Any actions within a security and compliance strategy should be framed, directed and influenced by the set of goals and objectives you define and communicate.

This underscores the importance of why sustainable control effectiveness should be explicitly and clearly incorporated as a strategic objective and made part of the overall goal. Your goals and objectives and their necessary conditions create the framework for every decision, every action within your security and compliance posture. Spending time on goals, requirements and constraints is essential to create a supporting governance structure that can help ensure that decisions and actions undertaken by people within the organization don't deviate from the strategy, goals and objectives that management determined to pursue. As is evident in the myriad of data breach investigation cases Verizon has conducted, failure to do so can set up a series of consequences that may result in unaddressed core conflicts, lack of focus, poor performance and eventually the nonachievement of goals.

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

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

Full compliance   ■ 2019 ■ 2020

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

89.0% (2019)
90.8% (2020)

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

% of organizations maintaining full compliance

Control gap   ■ 2019 ■ 2020

0%	5%	10%	15%	20%

6.7% (2019)
3.2% (2020)

0%	5%	10%	15%	20%

% of controls not in place

Compensating controls   ■ 2019 ■ 2020

0%	5%	10%	15%

0.6% (2019)
0.0% (2020)

0%	5%	10%	15%

% of organizations using compensating controls

Figure 18. Global state of PCI DSS compliance: Requirement 7

Full compliance

Full compliance improved slightly for Requirement 7. An average of just over 90% of organizations maintained full compliance across all base controls. Control 7.2 improved by 5.7 pp—a good achievement and very positive development.

Control gap

The control gap of Requirement 7 was slashed in half, from 6.7% to 3.2%. The performance improved across all base controls. Control 7.2 reduced by 5.4 pp from a high 8.9% gap to only 3.5% of controls found not in place during interim validation.

Compensating controls

No organizations applied compensating controls to meet Requirement 7.

In over 10 years of compliance trend analyses, 2019 was the only year in which one organization in the PSR dataset applied a compensating control to meet this requirement.

Requirement 7 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
7.1	Limit access to system components	90.3%	+2.7 pp	93.0%	3	6.5%	-3.6 pp	2.9%	1
7.2	Access control system based on "need to know," set to deny all	89.7%	+5.7 pp	95.4%	2	8.9%	-5.4 pp	3.5%	3
7.3	Policies and procedures for restricting access to CHD	92.9%	+4.2 pp	97.1%	1	7.1%	-4.2 pp	2.9%	1

Figure 19. Requirement 7 control performance

A tip on sustainable control effectiveness
System access controls that are not restricted based on an individual's job role and function can result in inconsistent applications of system access permissions and inappropriate levels of access to sensitive data. It's important to establish access matrices that map system access requirements to job roles across the organization and to automate configuration management. These form the basis of effective role-based access control; additional permissions can be added with appropriate approvals.

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

The goal	The goal of PCI DSS Key Requirement 7 is to maintain a reliable and sustainable capability to prevent unauthorized access to account data and systems across the CDE by effectively restricting access to system components and CHD by business "need to know," and the capability to detect and respond to access control violations. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **IT components:** All system components within the CDE, including related security system components that support access control to and from the CDE. The most common role-based access control (RBAC) is Windows® Active Directory® and Lightweight Directory Access Protocol (LDAP) • **People:** All employees (such as IT and security staff, accountants, support staff, call center agents, and executives), contractors, consultants, and internal and external vendors and other third parties that provide support or maintenance services, and any individual that should access CHD or any system component within the CDE (any component that processes, stores and/or transmits account data, and also components that directly connect to or support such components) • **Documentation:** Detailed documented standards and procedures for the configuration of all administrator and user accounts, including procedures to define, identify and assign different roles and responsibilities, access to data resources, required privilege levels, formal approval of access requests, and periodic internal audits for review and reconciliation between expected access privileges and actual system configurations
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Competence:** Document an RBAC standard and procedures to restrict account data access to only those who need it to perform their job, to prevent all unauthorized exposure of account data • **Capability – process:** Maintain the capability for the reliable, sustainable and effective access management process that covers all components within the CDE • **Capability – automation:** Implement and maintain the use of automated tools to support the monitoring and frequent review of access privileges according to the "least privilege" principle. This should include the and periodic auditing and evaluation of access control systems to review consistency and effectiveness • **Documentation and processes:** Maintain effective standard operating procedures, with clearly articulated standards. Regularly train and educate staff on how to follow the documented procedures

Strong dependencies and integration with other key requirements	• **Requirement 8:** Strong dependency and integration with user identity and authentication • **Requirement 10:** Integration with logging and monitoring • **Requirement 2:** Security configuration of system components • **Requirement 9:** Integration with physical security controls • **Requirement 1:** Integration with network security controls
Short-term objectives	• **Standardization:** Identify and document all access control mechanisms to ensure that all components across the CDE conform to authorized and approved access control systems, standards and procedures • **Automation and integration:** Implement or update and integrate an automated RBAC system for centralized management and oversight of access control configurations across the CDE • **Internal audit:** Identify all inactive users on in-scope systems and either permanently disable or delete them; identify and remove all group or shared usernames and passwords • **Hardening:** Properly harden and configure network security components to protect the RBAC system from compromise
Long-term objectives	• **Maturity:** Achieve and maintain high-performance maturity on access control management by further improving IT system capabilities and the level of automation, and refining configurations and support processes, documentation and user training. Improve the detection and response to access control nonconformities and violations
Common constraints	• **Capacity and cost:** The level of effort and cost to implement an RBAC system, and maintain an up-to-date list of users and roles within large environments • **Capability:** Lack of awareness, communication and coordination, often due to siloed internal organizational structures • **Competency:** The ability to manage complex architecture and infrastructure environments and deal with legacy systems or third-party systems that cannot be integrated
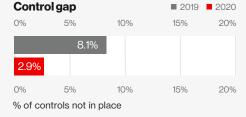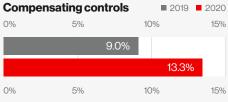
Requirement 8:
Identify users and authenticate access to system components

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

Full compliance ▪ 2019 ▪ 2020

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

74.0%

83.2%

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

% of organizations maintaining full compliance

Control gap ▪ 2019 ▪ 2020

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

8.1%

2.9%

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

% of controls not in place

Compensating controls ▪ 2019 ▪ 2020

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

9.0%

13.3%

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

% of organizations using compensating controls

Figure 20. Global state of PCI DSS compliance: Requirement 8

Full compliance

83.2% of organizations achieved and maintained full compliance with Requirement 8, a very healthy performance increase of 9.2 pp from the year before, and nearly equaling the record of 83.5% set in 2016.

Control gap

The control gap narrowed substantially, from 8.1% to a low 2.9%. Control 8.3.1 (Verify that multifactor authentication is required) improved by 11.2 pp.

Compensating controls

Requirement 8 was the most compensated requirement since 2015, falling to second place after Requirement 6 took the top spot for the first time this year.

Requirement 8 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
8.1	Policies and procedures for user identification	80.0%	+10.8 pp	90.8%	7	9.1%	-4.9 pp	4.2%	8
8.2	Proper user authentication management	85.2%	+3.9 pp	89.1%	8	8.2%	-4.7 pp	3.5%	6
8.3	Multifactor authentication for all remote access to CDE	85.2%	+10.2 pp	95.4%	6	8.3%	-6.2 pp	2.1%	5
8.4	Communicate authentication policies to all users	93.5%	+4.7 pp	98.2%	2	5.8%	-4.1 pp	1.7%	3
8.5	Do not use group/shared IDs	87.7%	+8.2 pp	95.9%	5	8.2%	-6.9 pp	1.3%	1
8.6	Uniquely identify and secure authentication mechanisms	91.0%	+6.1 pp	97.1%	3	7.7%	-6.0 pp	1.7%	3
8.7	Restrict all access to any database containing CHD	92.3%	+6.0 pp	98.3%	1	6.9%	-5.5 pp	1.4%	2
8.8	Policies and procedures for identification	93.5%	+3.0 pp	96.5%	4	6.5%	-3.0 pp	3.5%	6

Figure 21. Requirement 8 control performance

A tip on sustainable control effectiveness

Organizations often fail to remove terminated user accounts in a timely manner, leaving themselves potentially exposed to account misuse by disgruntled personnel. Terminated user accounts must be disabled immediately, and these processes should be included with Human Resources exit procedures. Strict service level agreements (SLAs) for removal of access should be established so that access is disabled just prior to employee termination, when possible.

Requirement 8: Identify users and authenticate access to system components

The goal	The goal of PCI DSS Key Requirement 8 is to protect payment card account data by maintaining a sustainable capability for the reliable application of strong authentication controls for all in-scope users and systems, and to ensure that only authorized users can access any system component in the CDE; are uniquely identifiable, accountable and traceable; and are given entitlements based on "least privilege" and "need to know." This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **People:** All in-scope users with access to sensitive data, systems and locations, which applies to all personnel, including general users, administrators, vendors and other third parties that access the entity's network from an external or remote network • **IT components:** The application of automated authentication technology across the CDE, including technologies such as remote authentication and dial-in service (RADIUS) with tokens, terminal access controller access control system (TACACS) with tokens, and other technologies that facilitate multifactor authentication
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability—procedures:** Maintain an organizational capability for strong governance on the entire life cycle of users that includes management approval, provisioning, and periodic certification and decommissioning, and maintain documented authentication procedures with supporting awareness and training. All users have their own authorized credentials that are not shared, with passwords meeting industry standards, and inactive and terminated accounts suspended and removed, if possible • **Capability—automation:** Create the capability to establish and reliably maintain strong authentication for users and administrators. The capability to correctly design, implement and maintain multifactor technologies for strong MFA and secure remote network access for all connections originating from outside the entity's network that could access or impact the CDE, preventing in-scope system components from being accessed by the use of a single authentication factor • **Capability—monitoring:** The active, effective and sustainable monitoring of the use and configuration of authentication systems, with timely detection and response to misconfigurations and system event alerts

Strong dependencies and integration with other key requirements	• **Requirement 7:** Strong dependency and integration with access control requirements • **Requirement 10:** Integration with logging and monitoring to detect and respond to authentication incidents • **Requirement 2:** Secure configuration of all authentication system components • **Requirement 9:** Integration with physical security control • **Requirement 1:** Integration with network security controls to protect access to authentication systems
Short-term objectives	• **Scope:** Maintain a capability to effectively identify and document all in-scope components through user-to-component mapping, and formally assign roles and responsibilities to all users and systems • **Automate:** Implement and maintain effective systems to automate user ID and authentication systems, management reporting, and monitoring across the entire CDE • **Secure remote access:** Implement and maintain MFA to secure access to the CDE, and configure MFA systems to prevent misuse
Long-term objectives	• **Maturity — technical:** Improve configurations, documentation and integration with dependent key requirements • **Maturity — process:** Improve the effectiveness with which the authentication process is integrated, maintained and managed to achieve high performance, continuous improvement and maturity
Common constraints	• **Competency:** The design, implementation and maintenance of authentication systems can be complicated in large, complex environments, requiring specialized competencies • **Cost:** The cost of authentication solutions can be prohibitive • **Capability:** The ability to effectively support and sustain authentication system projects with processes and capabilities, which may require many months (or several years) of improvements to achieve maturity
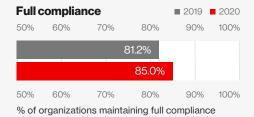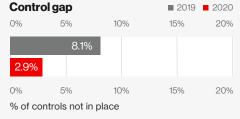
Requirement 9: Restrict physical access to cardholder data

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

Full compliance

| 2019 | 2020 |

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

81.2% (2019)
85.0% (2020)

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

% of organizations maintaining full compliance

Control gap

| 2019 | 2020 |

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

8.1% (2019)
2.9% (2020)

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

% of controls not in place

Compensating controls

| 2019 | 2020 |

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

0.6% (2019)
1.7% (2020)

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

% of organizations using compensating controls
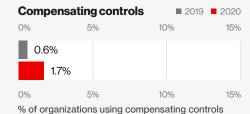
Figure 22. Global state of PCI DSS compliance: Requirement 9

Full compliance

Requirement 9 improved modestly from 81.2% to 85.0%, and reached the highest performance of this control in more than five years in terms of full compliance.

Control gap

The control gap narrowed substantially from 8.1% to a low 2.9% of controls that are found not in place during interim compliance validation.

Compensating controls

1.7% of organizations applied one or more compensating controls. While the use of compensating controls under Requirement 9 remains very low, it increased to the highest level in more than five years.

Requirement 9 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
9.1	Appropriate facility entry controls and monitoring access of CDE	89.0%	+3.5 pp	92.5%	10	5.6%	-3.8 pp	1.8%	7
9.2	Distinguish between onsite personnel and visitors	92.9%	+5.9 pp	98.8%	1	5.6%	-4.6 pp	1.0%	4
9.3	Control physical access for onsite personnel to sensitive areas	92.3%	+5.4 pp	97.7%	4	6.2%	-4.7 pp	1.5%	5
9.4	Procedures to identify and authorize visitors	91.6%	+3.2 pp	94.8%	8	6.5%	-4.2 pp	2.3%	10
9.5	Physically secure all media	92.9%	+5.4 pp	98.3%	3	2.9%	-2.5 pp	0.4%	1
9.6	Control internal and external distribution of media	92.3%	+6.5 pp	98.8%	1	5.9%	-5.1 pp	0.8%	2
9.7	Control storage and accessibility of media	92.3%	+5.4 pp	97.7%	4	7.4%	-5.7 pp	1.7%	6
9.8	Destroy media when no longer needed	90.3%	+6.2 pp	96.5%	6	6.5%	-5.6 pp	0.9%	3
9.9	Protect data capture devices; tampering/substitution	92.3%	+3.1 pp	95.4%	7	4.6%	-2.8 pp	1.8%	7
9.10	Documented policy restricting physical access to CHD	89.0%	+3.5 pp	92.5%	10	5.6%	-3.8 pp	1.8%	7

Figure 23. Requirement 9 control performance

The overall sustainability of controls under Requirement 9 remains good. Control 9.4 (Procedures to identify and authorize visitors) and Control 9.10 (Documented policy restricting physical access to CHD) rank the lowest in performance. Control 9.4 also has the highest control gap across all controls under this requirement.

A tip on sustainable control effectiveness
Organizations that experience issues with establishing point of interaction (POI) device tamper-check procedures and the provisioning of adequate personnel training should use the PCI SSC Skimming Prevention guidance document to support the development of effective training and make tamper-checking part of existing start- or end-of-day processes.

Requirement 9: Restrict physical access to cardholder data

The goal	The goal of PCI DSS Key Requirement 9 is to protect payment card account data by maintaining a sustainable capability for the effective and reliable restriction of physical access to sensitive facilities, systems and any component (such as hard copies) that contain CHD across the CDE to authorized individuals only, and the capability to prevent, detect and respond to access attempts by any unauthorized individuals. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **Scope—CHD components:** All IT components, desktop and mobile computers, storage devices (external hard drives, backups, etc.), paper records, POS devices, and electronic audio recordings that contain payment card account data, as well as components that can access such systems and the facilities in which they reside • **Scope—security components:** Network security components (routers, firewalls, logging and monitoring, access control, and authentication systems), wireless access points, network jacks, telecommunication lines, badge readers, key entry locks, CCTV cameras and recording systems
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability—inventory management:** Create and actively maintain a complete and accurate inventory of all systems that store, process and transmit account data or can affect the security of account data. Identify the physical locations of these systems and all individuals authorized to access them, and also list applications running on these systems, including version number, to stay on top of known vulnerabilities • **Capability—automate:** Implement an application to support and automate the maintenance of an up-to-date list of all devices—including physical location, serial numbers and make/model—and integrate HR and IT processes to remain synchronized with staff, network and system component changes. This includes the classification, logging and management of all CHD-related media in accordance with the sensitivity of the data • **Competence—procedures:** The ability of all relevant frontline staff to detect suspicious activity around payment devices; verification procedures for any third parties requesting physical access to any CHD component, such as POS devices, servers or wireless devices. The capability to effectively and consistently inspect POS devices to ensure that they haven't been tampered with, with sufficient training for staff to be proficient at POS device inspections, effectively verifying serial number matches and detecting security seal compromises • **Documentation and processes:** Maintain standard operating procedures with clearly articulated standards. Regularly train and educate staff on how to follow the documented procedures. Maintain strict, consistent enforcement of the effective identification, authorization and escorting of visitors to sensitive areas

Strong dependencies and integration with other key requirements	• **Requirement 8:** Integration with authorization requirements for effective physical access control • **Requirement 7:** Integration with access control requirements for effective physical access control • **Requirement 10:** Integration with logging and monitoring requirements of physical security components • **Requirement 12:** Integration with risk assessment, governance, training and awareness requirements
Short-term objectives	• **Scope—inventory:** Maintain an up-to-date inventory, including a complete description of all relevant in-scope physical system components across the CDE • **Capability:** Implement and maintain an effective process where all media with CHD (electronic and hard copy) is destroyed when no longer needed for business or legal reasons, across the CDE
Long-term objectives	• **Improve:** Improve the capability to collect, review and correlate all physical access control records and monitoring logs to enhance the effectiveness of physical access controls to all sensitive areas across the CDE • **Maturity:** Improve and refine configurations and support processes, documentation and training to achieve and maintain high-capability maturity on physical access security control processes and capabilities
Common constraints	• **Commitment:** Insufficient ongoing assurance from management that employees are required to consistently adhere to security and compliance requirements, and investment in resources (automation tools, ongoing training and awareness) to enable staff to be proficient at fulfilling the scope of tasks under Requirement 9

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

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

Full compliance ■ 2019 ■ 2020

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

66.2%

76.3%

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

% of organizations maintaining full compliance

Control gap ■ 2019 ■ 2020

0%	5%	10%	15%	20%

9.2%

5.5%

0%	5%	10%	15%	20%

% of controls not in place

Compensating controls ■ 2019 ■ 2020

0%	5%	10%	15%

1.9%

4.6%

0%	5%	10%	15%

% of organizations using compensating controls
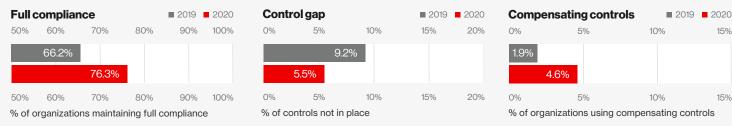
Figure 24. Global state of PCI DSS compliance: Requirement 10

Full compliance

Maintaining full compliance on Requirement 10 increased a whopping 10.1 pp. This is a remarkable improvement possibly due in part to the significant increase in the use of compensating controls.

Control gap

The control gap improved significantly. Controls 10.7 (Retain audit trail history) and 10.2 (Examine audit log settings) appear in the Bottom-20 lists of controls with the lowest performance, and need more attention.

Compensating controls

The use of compensating controls more than doubled for this requirement, from a low 1.9% to 4.6%, returning to about the same percentage it was at in 2015.

Requirement 10 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
10.1	Audit trails linking access to individual users	87.7%	+3.6 pp	91.3%	5	12.3%	-3.6 pp	8.7%	9
10.2	Automated audit trails to reconstruct events	87.1%	+0.4 pp	86.7%	9	8.5%	-0.9 pp	7.6%	8
10.3	Record user ID, date and time events	89.7%	+5.7 pp	95.4%	3	8.7%	-4.5 pp	4.2%	3
10.4	Time-synchronization technology	83.9%	+6.9 pp	90.8%	6	9.8%	-4.8 pp	5.0%	4
10.5	Secure audit trails so they cannot be altered	79.4%	+10.8 pp	90.2%	7	9.8%	-3.7 pp	6.1%	7
10.6	Review logs to identify anomalies or suspicious activity	86.5%	+4.9 pp	91.4%	4	9.3%	-3.7 pp	5.6%	5
10.7	Retain audit trail history for at least one year	88.4%	+1.8 pp	90.2%	7	9.7%	-3.9 pp	5.8%	6
10.8	Reporting of failures of critical security control systems	89.0%	+7.5 pp	96.5%	1	9.0%	-6.6 pp	2.4%	1
10.9	Policies and procedures for monitoring all access	92.3%	+3.7 pp	96.0%	2	7.7%	-3.7 pp	4.0%	2

Figure 25. Requirement 10 control performance

A tip on sustainable control effectiveness
Even in small environments, it's not likely to be practical to monitor logs individually. It's essential to implement and maintain a centralized, automated system with robust log management and monitoring capabilities, linking user access to all system components across the CDE. An integrated, unified security monitoring and compliance management solution that collects, normalizes, analyzes and presents log data—and monitors and correlates the log data against the latest threat intelligence—can significantly increase the effectiveness and reduce the workload associated with Requirement 10.

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

The goal	The goal of PCI DSS Key Requirement 10 is to develop and maintain a sustainable capability to effectively record and track user activities for preventing, detecting or minimizing the impact of a data compromise through reliable logging and monitoring of all access to system components and CHD. This ensures that all required logs are collected for all system components across the CDE, and that they are correlated and reviewed daily, with the ability to effectively detect and respond to incidents in a timely manner. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **IT components:** A centralized, automated logging and monitoring system that collects and correlates logs from all related CDE system components, which includes all system components that store, process or transmit CHD and/or SAD; all critical system components, including those that perform security functions such as file-integrity monitoring or change-detection software, IDS/IPS, routers, firewalls, anti-malware, database logging systems, wireless access point logging systems, email/web server/ e-commerce application logging, physical access logs, etc. • **People:** All internal staff and third parties involved in the implementation, management, monitoring and support of system components (such as those listed above) required to meet the goal of this key requirement • **Standard of performance:** A complete, integrated security monitoring strategy, policy and procedure document with defined scope, roles and responsibilities for the production, protection and retention of audit trails, and expected standard of performance of people and systems supporting the achievement of this goal

Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Technology:** Use the selection and implementation of a centralized, automated logging and monitoring solution that meets all the logging and monitoring requirements under PCI DSS Key Requirement 10. For example, for all audit trails to reliably and accurately link all access to system components across the CDE to individual users that access any components that store, process or transmit CHD, and all actions taken by any individual with root or administrative privileges to any CDE system component • **Competency:** Correctly configure the features of the logging and monitoring system, ensuring that all system components are logging and reporting relevant information • **Capacity and capability:** Ensure the ability of security teams to effectively review logs every day to detect, respond and minimize the amount of time and exposure of a potential breach of any component in the CDE • **Capability — processes:** Maintain effective detection and alerting processes to detect failure of any critical security controls, responding to generated alerts, determining the root cause of the failure and documenting remediation required for the failure of critical security controls within the CDE • **Documentation and processes:** Maintain effective standard operating procedures, with clearly articulated performance standards. Regularly train and educate staff on how to follow the documented procedures
Strong dependencies and integration with other key requirements	• **Requirement 11:** Strongly integrated with incident response procedures • **Requirement 1:** Integration with network security controls to monitor perimeter access • **Requirement 7:** Integration with access controls • **Requirement 8:** Integration with authentication systems
Short-term objectives	• **Scope:** Produce and verify the accuracy and completeness of the component scope, that there are no oversights with any system component accidentally excluded from the logging and monitoring program • **Capability:** Implement technology that effectively synchronizes all system clocks in all systems across the CDE
Long-term objectives	• **Improve:** Enhance configuration to increase the detection of, and improve time spent on, false-positive alerts. Refine configurations and improve support processes, documentation and training • **Maturity:** Achieve and maintain high-capability maturity on logging and monitoring across the CDE by improving the efficiency of manual log reviews, enhancing automation
Common constraints	• **Capacity:** Not having sufficient capacity of personnel to manage the workload associated with Requirement 10 • **Cost:** Lack of budget for procurement of tools and staffing • **Competency:** Lack of proficient staff qualified with log analysis and required level of performance

Requirement 11: ....▶
Test security of systems and networks regularly

This requirement covers the use of vulnerability scanning, penetration testing, file integrity monitoring and intrusion detection to ensure that weaknesses are identified and addressed.
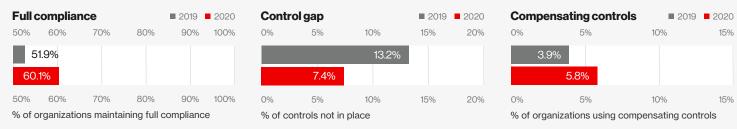
Full compliance ■ 2019 ■ 2020

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

51.9%
60.1%

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

% of organizations maintaining full compliance

Control gap ■ 2019 ■ 2020

0%	5%	10%	15%	20%

13.2%
7.4%

0%	5%	10%	15%	20%

% of controls not in place

Compensating controls ■ 2019 ■ 2020

0%	5%	10%	15%

3.9%
5.8%

0%	5%	10%	15%

% of organizations using compensating controls

Figure 26. Global state of PCI DSS compliance: Requirement 11

Full compliance

On average, only 60% of organizations across the globe maintained compliance with Requirement 11. The percentage of organizations that kept all controls in place increased by 8.2 pp. While full compliance improved significantly, it remains the requirement with the lowest performance and sustainability across the PCI DSS.

Control gap

The control gap declined by nearly half (43%) from a high 13.2% to 7.4%. This is a much-needed improvement, in part due to substantial performance improvement on Test Procedure 11.3.2.a (internal penetration test) by 10.0 pp, and Control 11.2 (internal and external vulnerability scans).

Compensating controls

The use of compensating controls increased modestly from a relatively low 3.9% to 5.8% of organizations that required compensating controls to meet this key requirement.

Control 11.3 was compensated the most (by 3.5% of organizations), followed by Controls 11.1 and 11.5 (both by 1.7%).

Requirement 11 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
11.1	Test for the presence of wireless access points	85.2%	+8.5 pp	93.7%	3	8.8%	-5.4 pp	3.4%	1
11.2	Run network vulnerability scans	65.8%	+10.5 pp	76.3%	5	17.2%	-6.9 pp	10.3%	6
11.3	Implement penetration testing	68.4%	+0.4 pp	68.8%	6	13.7%	-5.1 pp	8.6%	5
11.4	Use intrusion detection systems	87.7%	+6.5 pp	94.2%	2	11.2%	-6.9 pp	4.3%	3
11.5	Deploy change detection mechanism	83.9%	+6.3 pp	90.2%	4	12.7%	-5.2 pp	7.5%	4
11.6	Documented procedures for monitoring and testing	92.3%	+4.3 pp	96.6%	1	7.7%	-4.3 pp	3.4%	1

Figure 27. Requirement 11 control performance

The ongoing trouble with Requirement 11

Many issues contribute to the poor performance of Requirement 11. Some are basic, while others are systemic and impact the sustainable control effectiveness of controls under Requirement 11 and require comprehensive diagnosis and remediation solutions. The following basic issues can be avoided or corrected with relatively little effort.

- Cases where Control 11.3.3 had a larger gap than the external or internal penetration testing itself often point to an organization performing a penetration test but then failing to mitigate the findings, or being unable to do so. Some organizations receive vulnerability scan and penetration test reports that they don't understand or are unsure where to start mitigating. This can be solved by improving the team's skillset through education and training

- Some organizations apply an incorrect interpretation of the requirements, such as Control 11.3.3 — Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections — where the word "exploitable" is incorrectly interpreted as "high-risk vulnerabilities"

- Numerous organizations have yet to achieve a medium level of maturity of their internal security testing processes and capabilities. In larger organizations, removing the silos between teams and completing the integration between various critical activities, such as vulnerability scanning, penetration testing, security incident and log management, vendor management, etc., require attention

See page 134, where we review issues related to Requirement 11 in more detail.

Requirement 11: Test security of systems and networks regularly

The goal	The goal of PCI DSS Key Requirement 11 is to develop and maintain a sustainable capability to effectively verify the security posture of all system components across the CDE using automated network scan and penetration testing tools as well as manual methods, all designed to detect network and application vulnerabilities operating inside the network, and to rectify vulnerabilities based on a formal risk-assessment framework. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **Testing scope:** Security testing of all in-scope networks and IT system components across the CDE, including wireless access points, internal and external vulnerability scanning, internal and external penetration testing, segmentation testing, and cloud environments (service providers) • **Security tools:** Configuration, use and maintenance of network scan applications, penetration testing tools, change-detection tools (file-integrity monitoring), automated monitoring tools (IDS/IPS, NAC, wireless) • **Process:** Documented vulnerability management program, including network and application vulnerability management procedures, penetration testing methodology, wireless access point assessments, security alert configuration standard, incident response process
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Capability – program management:** Develop and document a comprehensive vulnerability management program that covers the entire scope of the requirement to effectively support the achievement of the requirement goal • **Capability – testing scope:** Create the ability to effectively sustain periodic security testing of all in-scope components, including after significant changes to the network or systems. Test for the presence of wireless (Wi-Fi) access points, and detect and identify all authorized and unauthorized wireless access points. Maintain mechanisms to detect real-time suspicious or anomalous network traffic, with intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network • **Documentation and processes:** Maintain effective standard operating procedures with clearly articulated performance standards. Regularly train and educate staff on how to follow the documented procedures

Strong dependencies and integration with other key requirements	• **Requirement 6:** Strong dependency and integration with secure systems and software • **Requirement 2:** Integration with application of secure configurations • **Requirement 10:** Integration with logging and monitoring requirements • **Requirement 1:** Testing of network security components • **Requirements 3 & 4:** Testing of components that store, process and transmit account data
Short-term objectives	• **Capability:** Effective communication of a complete vulnerability management program document to all stakeholders involved in the planning and delivery of this requirement (training, education and awareness) to support capacity and capability planning and ongoing project management efforts • **Project planning:** The commitment of resources, confirmation of roles and responsibilities, and scheduling of all tasks that support the effective and timely execution and achievement of all objectives and the goal
Long-term objectives	• **Integrate:** Improve the integration between all in-scope security testing and monitoring components • **Maturity:** Achieve and maintain high-capability maturity on security vulnerability management and incident response
Common constraints	• **Capacity:** Lack of capacity to scan large internal networks and to scan real-time environment and system availability; lack of resource capacity planning to manage the workload of this requirement • **Competence:** Misinterpretation of compliance requirements, lack of education and awareness. Operating without a well-defined, documented vulnerability management program • **Capability:** Failure to project manage the scheduling and completion of tasks; planning and timely execution • **Legal constraints:** Business and technical constraints due to legislation around cryptography and software • **Business critical:** Highly sensitive, business-critical systems where risk of unplanned downtime trumps software vulnerabilities, preventing scans and penetration tests from being conducted

On measuring and reporting sustainable control effectiveness: Requirement 11

Various reasons exist for the prolonged poor compliance performance of PCI DSS Key Requirement 11, including failure to maintain firm process and capability control to perform the required actions. We reviewed this on pages 64 through 67 and 102 through 106 of the 2020 PSR. Another reason for the low performance of the network scan and penetration testing controls is the presentation of evidence of compliance. Organizations continue to complete and "successfully" pass their PCI DSS compliance assessments, despite creating and presenting evidence of compliance "just in time." This behavior doesn't demonstrate the ability and commitment to rapidly detect and correct controls that fall out of place. It often demonstrates lack of intent to address the root causes of weak control performance. This continues to happen, primarily because the metrics for the evaluation and reporting of sustainable control effectiveness and continuous improvement are not explicitly included in the PCI DSS assessment procedures within and across PCI DSS requirements (for PCI DSS v3.2.1 and prior versions).

For most of the PCI DSS controls, evidence of compliance can be produced and submitted to an assessor just in time for review as part of an annual compliance validation assessment. For example, policies and standards can be updated relatively quickly (and superficially), and a signature from management easily obtained to indicate that documents were internally reviewed and approved. Employees who need to receive security and awareness training can be subjected to a quick and superficial security training and awareness session a week before the arrival of the assessor. Similarly, insecure system configurations, weak passwords and poor vendor default settings in critical components can be corrected just prior to the assessor's arrival and the finalization of the Report on Compliance (ROC). While this behavior from assessed organizations is certainly not ideal, it is widespread.

QSAs rightfully frown upon receiving evidentiary documents clearly created for the purpose of "passing" a compliance assessment, since they don't demonstrate commitment to meeting the intent of PCI DSS. These conditions involve maintaining a control environment that is sustainable and effective — essential conditions needed for the protection of payment card data. QSAs are trained to follow the specifications for assessment validation included in the PCI DSS Assessment Procedures. Despite an observed lack of control effectiveness and sustainability, it can be difficult for a QSA to disqualify evidence presented by organizations. There are various reasons for this, which we discuss in further detail.

Why has Requirement 11 consistently been the lowest-performing key requirement for more than a decade — both in terms of maintaining full compliance and control gap? Controls 11.2 and 11.3 are some of the few requirements that involve external entities to produce evidence of compliance. Meeting the security testing procedures of Controls 11.2 and 11.3 requires documented proof that network and application vulnerability scans and penetration test procedures were initiated and concluded within the required time frame and by qualified people. For various reasons, organizations continue to miss completing these time-sensitive requirements, such as producing reports that substantiate that all requirements were met for quarterly network vulnerability scans and annual penetration tests, conducted in time and after substantial changes were made to the CDE. High-risk vulnerabilities must also be corrected in time. Failing this, organizations are unable to produce a fully populated network scan or penetration testing report after the fact — as evidence that the controls were in place within the required time frame. Penetration tests and vulnerability scan reports are technical and detailed; they include numerous timestamps and dates that record the exact period in which the control actions (scans and pentests) were executed. Fabrication of evidence is never an option; it's a clear violation of compliance assessment requirements and, when discovered, will result in the immediate termination of the assessment, as well as other repercussions.

> Despite the existence of payment card brand compliance programs for 20 years, some organizations still assume that achieving annual compliance is all, or most, of what it takes to protect payment card data.

But achieving data security and compliance success is more than just avoiding failure of compliance validation assessments.

This situation highlights a larger issue—a weakness that has existed within the PCI DSS assessment procedures since the introduction of the PCI security regulation. The intent of PCI DSS is to ensure that security controls are effective and remain in place. However, organizations are not compelled to provide evidence of "sustainable control effectiveness" as part of their compliance validation assessments for individual requirements. Procedures for evaluating and reporting the effectiveness of any particular control, and its sustainability based on influences from its control environment, are not included in the Standard (PCI DSS v3.2.1 and prior versions). Organizations are only compelled to control environment sustainability when ticking the checkbox in part 3a of the Attestation of Compliance (AOC) acknowledgment: "I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times." The compliance status recorded in the ROC is the implicit evidence of this "sustainable effectiveness." A ROC primarily records that controls were present within the control environment; it does not include a record of the actual control performance over time. As mentioned, many security controls can be out of place for several months and corrected just in time to pass the annual validation assessment. Therefore, a typical ROC does not report the actual level of assurance of controls present within

and across the CDE. A ROC is unlikely to mention any increase in the risk exposure to account data and the reduced effectiveness of the CDE as a consequence of security controls not being in place for prolonged periods prior to the validation assessment.

Organizations tend to document the minimum amount of evidence required in accordance with what is specified in the PCI DSS assessment procedures. The required evidence documentation does not specifically compel the assessed entity, nor the QSA, to report that a security control was operating as required and in place throughout the duration of its relevant control period and the typical 12-month period preceding the annual compliance validation. As explained before, with the exception of a handful of requirements, evidence that a control was temporarily not in place is often not recorded in the final ROC, and subsequently not a critical factor included in the criteria for organizations to "pass" their validation assessment.

PCI DSS v3.2.1 assessment procedures don't include explicit stipulations for the proactive evaluation and reporting of security control sustainability and effectiveness individually per requirement. No defined procedure is included for how control effectiveness should be measured and documented and what minimum documentation should be submitted as evidence as part of a compliance validation assessment. For example, very few specifications are included in the PCI DSS to report the date when a control was discovered to be not in place, the number of days the control was not in place and the date when remediation activities were completed for the control to be back

in place, operational and functioning as intended—not merely present (such as, Control 10.8.1 that applies to service providers only, and Designated Entities Supplemental Validation [DESV] control A3.3.1.1). Including this data is invaluable for recording and reporting the actual performance of the control environment. It vastly improves individual and team responsibility and accountability to ensure that controls are operating in a manner that meets the objective and intent of the requirement. At an individual control level, it also brings much-needed visibility to how controls that are not in place negatively impact the effectiveness of the control and control environment, not to mention its value during post-breach forensic investigations.

This is an important issue that PCI DSS v4.0 will help strengthen by introducing a customized approach to controls and emphasizing ongoing assessments and other changes to the compliance procedures. It largely depends on the specifications and procedures for evaluating control effectiveness included within the PCI DSS validation assessment procedures. To be truly useful as an indicator of data security, a PCI DSS ROC should include adequate expression of a level of assurance of security controls. This requires setting minimum criteria for the quality of evidence accepted, and specification of metrics to evaluate the strength, validity and reporting of the actual control performance of individual controls or control systems. The extent to which updated requirements in PCI DSS will support this should be more evident in 2024, when the new PCI DSS v4.0 requirements become effective.

Requirement 12:
Support information security with organizational policies and programs ....▶

Actively manage security team data-protection responsibilities by establishing, updating and communicating security policies and procedures aligned with the results of regular risk assessments.
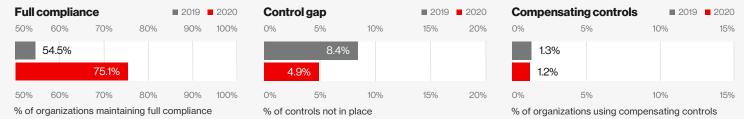
Full compliance   ■ 2019 ■ 2020

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

54.5%

75.1%

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

% of organizations maintaining full compliance

Control gap   ■ 2019 ■ 2020

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

8.4%

4.9%

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

% of controls not in place

Compensating controls   ■ 2019 ■ 2020

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

1.3%

1.2%

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

% of organizations using compensating controls

Figure 28. Global state of PCI DSS compliance: Requirement 12

Full compliance

Requirement 12 saw the biggest gain across all 12 Key Requirements. In 2019, only 54.5% maintained compliance with this requirement, and it improved by 20.6 pp to 75.1% in 2020. This improvement is not due to an increased use of compensating controls, which actually reduced very slightly.

Control gap

The overall control gap for this requirement narrowed from 8.4% to 4.9%. This is due to Control 12.8.2 (written agreements with service providers), which improved by a substantial 11.4 pp. Control 12.6 (security awareness program) also improved substantially.

Compensating controls

The use of compensating controls remained almost unchanged (-0.1 pp) with very few organizations requiring any. Only Controls 12.1 (security policies) and 12.10 (incident response plan) were compensated.

Requirement 12 controls		Full compliance				Control gap			
Performance year-over-year		2019	Change	2020	Rank	2019	Change	2020	Rank
12.1	Publish, maintain and disseminate security policy	83.9%	+5.1 pp	89.0%	8	7.7%	-2.8 pp	4.9%	6
12.2	Implement a risk-assessment process	83.2%	+5.2 pp	88.4%	10	14.8%	-5.0 pp	9.8%	11
12.3	Develop usage policies for critical technologies	92.3%	-1.5 pp	90.8%	6	6.1%	-1.7 pp	4.4%	5
12.4	Define InfoSec responsibilities for all personnel	85.8%	+9.6 pp	95.4%	4	8.9%	-6.0 pp	2.9%	2
12.5	Assign InfoSec management responsibilities	90.3%	+5.6 pp	95.9%	3	6.2%	-3.2 pp	3.0%	4
12.6	Implement a formal security awareness program	81.9%	+8.8 pp	90.7%	7	11.4%	-5.3 pp	6.1%	9
12.7	Screen potential personnel prior to hire	95.5%	+2.2 pp	97.7%	1	4.5%	-2.2 pp	2.3%	1
12.8	Manage service providers with policies and procedures	74.2%	+12.5 pp	86.7%	11	11.5%	-5.1 pp	6.4%	10
12.9	Service providers acknowledging responsibility	89.7%	+7.4 pp	97.1%	2	10.3%	-7.4 pp	2.9%	2
12.10	Implement an incident response plan	83.9%	+5.1 pp	89.0%	8	7.7%	-2.8 pp	4.9%	6
12.11	Additional requirements for service providers	86.5%	+6.0 pp	92.5%	5	11.4%	-5.6 pp	5.8%	8

Figure 29. Requirement 12 control performance

A tip on sustainable control effectiveness
Numerous applications are available to support the automation (scheduling, delivery and monitoring) of objectives under Requirement 12—such as policy communication, risk management, vendor management, user awareness and training applications. Attempting to manage communication via ordinary email is not advised. Automate and schedule the communication of compliance directives in advance, with automated email sent and response tracking integrated into issue-tracking software.

Requirement 12: Support information security with organizational policies and programs

The goal	The goal of PCI DSS Key Requirement 12 is to develop and maintain a sustainable and secure control environment for the effective protection of payment card data by maintaining a comprehensive program, supported by an integrated set of documented organizational information security, risk management and compliance standards, policies and procedures, with oversight from a governance structure and supporting processes for effective execution and continuous improvement. This goal includes complete integration with all related PCI DSS Key Requirements for the establishment of an effective, integrated series of control systems, and the development and ongoing improvement of all related capabilities, processes, documentation, tools and training needed to achieve <Quantitatively managed/Optimized> maturity of this key requirement by <insert date>.
Goal applicability and scope considerations	• **Documentation:** Security policies, standards, procedures and guidance documents that cover all PCI DSS requirements, third-party vendor agreements, incident response plan, and security awareness program plan • **People:** This goal applies to all employees (such as IT and security staff, accountants, support staff, call center agents, and executives), contractors, consultants, and internal and external vendors and other third parties that provide support or maintenance services, and any individuals who can access account data or any system component within the CDE
Goal requirements: Some of the primary conditions necessary to achieve the goal	• **Control environment:** Establish and maintain an effective and sustainable control environment: the actions, policies, values and management styles that influence and set the tone of the day-to-day activities of the organization; a reflection of its values; the atmosphere in which people conduct their activities and carry out control responsibilities. An environment in which competent people understand their responsibilities, the limits of their authority, and are knowledgeable, mindful and committed to doing what is right and doing it the right way • **Security policy—design and documentation:** Establish the capability to design, document and maintain a complete and integrated set of PCI security and compliance, and risk management policies, standards and procedures • **Security policy—training:** Create the capability to design, implement and maintain supporting processes to effectively communicate and update, and to monitor user awareness and comprehension of the policy documentation set • **Capability—incident response:** Establish the ability to develop a comprehensive incident response plan that covers all components within the CDE, and to test its effectiveness, and continuously improve it • **Capability—risk management:** Maintain the ability to develop, implement and maintain a comprehensive risk management strategy, method and implementation plan with performance management • **Capability—resource management:** Create the ability to develop, implement and maintain secure human resources and third-party management practices, policies and procedures

Strong dependencies and integration with other key requirements	• **All Requirements:** Security policies and standards required for all key requirements • **Requirements 10 & 11:** Integration with logging, monitoring and testing for incident response • **Requirement 6:** Risk management integration with secure systems and software requirements • **Requirements 5, 7, 8 & 9:** Targeted risk analysis integration
Short-term objectives	• **Communication:** Make policy, standards procedures and guidance available online to all stakeholders and track access and use • **Training:** Conduct online policy training, track which individuals read relevant security policies and completed the training (implementation coverage), and test their comprehension of the material presented
Long-term objectives	• **Integrate:** Improve the integration and alignment between policy, standards, procedure and guidance documentation. Frequent internal identification, reporting and correction of any misalignments • **Maturity:** Achieve and maintain high-capability maturity on maintaining an effective control environment
Common constraints	• **Competence:** Incomplete, unclear, poorly articulated and ill-constructed security policies and standards • **Capability:** Lack of information security proficiency; governance, program design, risk management, compliance management; inadequate training and education

Bottom-20 lists

The 20 biggest control gaps

The control gap indicates the number of failed controls divided by the total number of controls expected. This is an averaged figure that provides a measure of how far the assessed organizations were from full compliance. The table below lists the 20 DSS test procedures with the highest control gap in 2020 and changes from 2019 expressed in percentage points (pp).

A reoccurring pattern year after year, Requirement 11 test procedures on penetration testing and security vulnerability scans continue to have the highest control gap.

PCI DSS	control	Control description	2019	Change	2020
1	11.3.3	Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed remediation.	27.1%	0.6 pp	27.7%
2	11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change.	33.5%	-9.8 pp	23.7%
3	11.2.1.b	Review internal vulnerability scan reports, and verify that all high-risk vulnerabilities are addressed and that the scan process includes rescans to verify remediation.	23.2%	-2.4 pp	20.8%
4	1.1	Inspect the firewall and router configuration standards and other documentation to verify that standards are complete and implemented.	27.7%	-8.7 pp	19.0%
5	2.4	Maintain an inventory of system components that are in scope for PCI DSS.	24.5%	-6.0 pp	18.5%
6	2.4.a	Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	23.2%	-5.9 pp	17.3%
7	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor patches, and install critical patches within one month.	25.8%	-9.6 pp	16.2%
8	6.2.b	Select a sample of system components and related software, and compare the list of security patches.	26.5%	-11.4 pp	15.1%
9	11.2.1.a	Review internal vulnerability scan reports, and verify that four passing quarterly scans were obtained in the most recent 12 months.	20.6%	-7.9 pp	12.7%
10	3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of CHD.	12.3%	-0.1 pp	12.2%
11	12.2.b	Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	14.2%	-2.6 pp	11.6%
12	1.2	Examine firewall and router configurations, and verify that connections are restricted.	14.8%	-3.3 pp	11.5%
13	12.2	Implement a risk-assessment process that is performed at least annually and upon significant changes and which identifies assets, threats and vulnerabilities and results in a formal, documented analysis of risk.	16.8%	-5.2 pp	11.6%
14	5.2	Ensure that all antivirus mechanisms are periodically maintained.	14.2%	-3.2 pp	11.0%
15	2.4.b	Interview personnel to verify the documented inventory is kept current.	15.5%	-4.5 pp	11.0%
16	10.2	Verify logging through interviews of responsible personnel, observation of audit logs and examination of audit log settings.	11.6%	-1.2 pp	10.4%
17	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.	11.6%	-1.8 pp	9.8%
18	11.5.a	Verify the use of a change-detection mechanism within the CDE by observing system settings and monitored files, as well as reviewing results from monitoring activities.	16.1%	-6.3 pp	9.8%
19	1.1.6.b	Identify insecure services, protocols and ports allowed; and verify that security features are documented for each service.	7.1%	2.7 pp	9.8%
20	1.1.2.a	Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to CHD, including wireless networks.	14.2%	-4.4 pp	9.8%

Biggest decreases in control gap

The control gap improved significantly for several controls across Key Requirements 6, 8 and 11. Overall, the average global control gap improved substantially in 2020, from a high 7.7% control gap in 2019 (bad) to a low 4.0% in 2020 (better). The table below lists the top 20 biggest decreases (improvements) in control gap.

PCI DSS	control	Control description	2019	Change	2020
1	6.2.b	Select a sample of system components and related software and compare the list of security patches.	26.5%	-11.4 pp	15.1%
2	12.8.2	Observe written agreements and confirm that they include an acknowledgement by service providers.	14.8%	-11.4 pp	3.4%
3	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.	13.5%	-11.2 pp	2.3%
4	8.3.1.a	Examine network and/or system configurations, as applicable, to verify that multifactor authentication is required for all nonconsole administrative access into the CDE.	13.5%	-11.2 pp	2.3%
5	11.3.2.a	Examine the scope of work and results from the most recent internal penetration test to verify that testing is performed per defined methodology at least annually and after significant change.	18.7%	-10.0 pp	8.7%
6	11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change.	33.5%	-9.8 pp	23.7%
7	1.1.7.b	Examine documentation relating to rule set reviews and interview responsible personnel to verify that rule sets are reviewed at least every six months.	16.1%	-9.8 pp	6.3%
8	3.4	Render PANs unreadable anywhere they are stored (including on portable digital media, backup media and in logs).	14.8%	-9.6 pp	5.2%
9	6.2	Ensure that all system components and software are protected from known vulnerabilities.	25.8%	-9.6 pp	16.2%
10	8.3	Incorporate multifactor authentication for remote network access originating from outside.	14.2%	-9.6 pp	4.6%
11	11.1	Implement processes to test for the presence of wireless access points; detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	14.2%	-9.0 pp	5.2%
12	8.1.8	For a sample of system components, inspect system configuration settings.	13.5%	-8.9 pp	4.6%
13	11.1.c	If wireless scanning is utilized, examine output from recent wireless scans to verify that authorized and unauthorized wireless access points are identified; scan at least quarterly for all system components and facilities.	12.9%	-8.9 pp	4.0%
14	11.4.c	Examine IDS/IPS configurations and vendor documentation to verify that IDS/IPS devices are configured, maintained and updated per vendor instructions to ensure optimal protection.	12.3%	-8.8 pp	3.5%
15	11.2.2.a	Review output from the four most recent quarters of external vulnerability scans and verify that four occurred in the most recent 12 months.	17.4%	-8.7 pp	8.7%
16	1.1	Inspect the firewall and router configuration standards and other documentation to verify that standards are complete and implemented.	27.7%	-8.7 pp	19.0%
17	5.1.1	Review vendor documentation, and examine antivirus configurations to verify that antivirus programs detect, remove and protect against all known types of malicious software.	11.0%	-8.7 pp	2.3%
18	3.2.2	Examine data sources and verify that the card verification code value printed on the front or signature panel is not stored after authorization.	11.0%	-8.7 pp	2.3%
19	12.6	Implement a formal security awareness program to make all personnel aware of the importance of CHD security.	13.5%	-8.3 pp	5.2%
20	11.2.2.c	Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor.	13.5%	-8.3 pp	5.2%

Methodology ....

State of compliance

This research is based on the analysis of quantitative data gathered by QSAs from multiple Qualified Security Assessor Company (QSAC) organizations across the world. The dataset for this edition is based on information from five sources, four of them external to Verizon.[66] These findings are presented globally, with additional comparisons between geographic regions (Americas, EMEA and APAC).

Dataset

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

Assessments
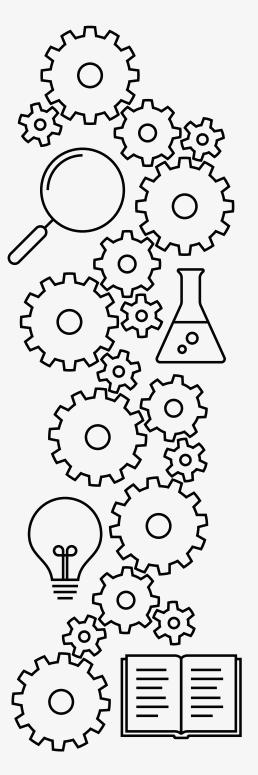
PCI DSS version: PCI DSS v3.2.1 consists of 12 PCI DSS Key Requirements, 79 base requirements, 252 control requirements and 440 test procedures.

In 2020, the compliance status of a total of 77,504 PCI DSS controls validated against PCI DSS v3.2.1 was assessed and compared against 68,992 controls from PCI DSS v3.2.1 assessed in 2019.

Reports: The 2019–2020 comparative analysis is based on an aggregate of 328 PCI DSS compliance validation reports and a combined total of 146,496 controls.

PCI DSS Report on Compliance (ROC) dataset:

2019:	155	(68,992 controls)
2020:	173	(77,504 controls)
Total:	328	(146, 496 controls)

---

66 See page 163 of this report for list of PCI DSS data contributors..

2020 PCI DSS validation dataset	2020 PCI DSS results – Interim validation
PCI DSS v3.2.1	100% compliance (passed): 75 (43.3%)
	<100% compliance (failed): 98 (56.7%)
Number of engagements: 173	
Americas: 97	For the 2020 assessment year, 75 entities passed their interim compliance validation, demonstrating that they kept all applicable PCI DSS controls in place. Over half (56.7%) of the organizations failed their interim validation assessment due to one or more security controls found to be not in place, with an average control gap of 4.0%—the percentage of controls that failed.
EMEA: 36	
APAC: 40	
The share of APAC organizations in the combined global dataset increased significantly in 2020 (from 9.3% to 23.0%).	Trend analysis includes year-over-year comparisons to determine how the state of compliance has evolved over multiple years. Changes in contributors and the potential changes in their areas of focus add a layer of difficulty when identifying trends over time.

The PSR analysis process

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

1. Contributor identification and collection of eligible PCI DSS v3.2.1 assessment reports

2. Full anonymization and conversion of the reports by the contributors into normalized data. All contributors received instruction to omit any information that might identify organizations or individuals involved

3. Secure submission of the anonymized data to the Verizon PSR data science team for aggregated analysis

Data eligibility

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

In addition to having the level of details necessary to pass the quality filter, the assessment reports must be within the time frame of analysis. For the 2020 dataset, this includes PCI DSS assessments conducted between January 1 and December 31, 2020.

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

"Anything can be measured. If a thing can be observed in any way at all, it lends itself to some type of measurement method. No matter how 'fuzzy' the measurement is, it's still a measurement if it tells you more than you knew before."[67]

—Douglas W. Hubbard

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

Noncommittal disclaimer

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

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

"Anything that gives us new knowledge gives us an opportunity to be more rational."[68]

—Herbert A. Simon

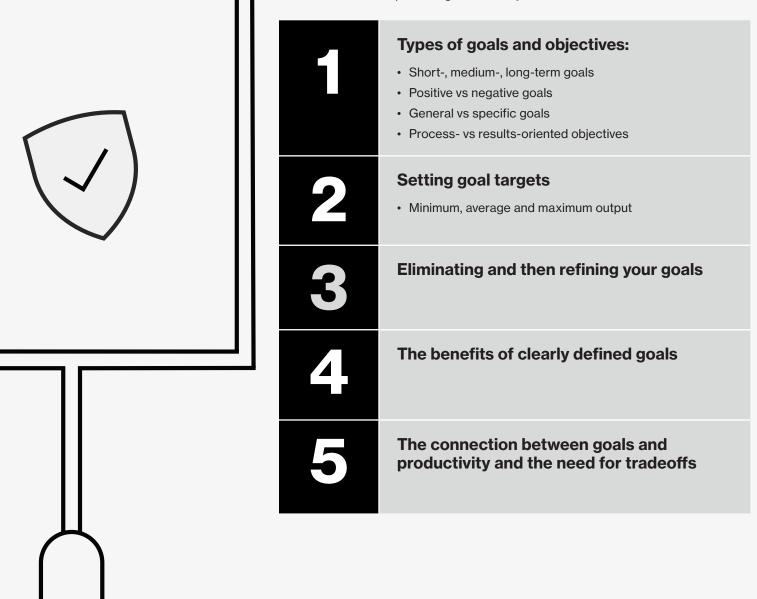"One accurate measurement is worth a thousand expert opinions. Without data, you're just another person with an opinion."[69]

—Rear Admiral Grace M. Hopper and W. Edwards Deming, Chicago Analytics Group

68 Herbert A. Simon, https://www.brainyquote.com/lists/authors/top-10-herbert-a-simon-quotes
69 Rear Admiral Grace M. Hopper and W. Edwards Deming, Chicago Analytics Group, Mar 30, 2016, http://chicagoanalyticsgroup.com/blog/archives/03-2016

4

Appendices

Appendix A: Primer for crafting security and compliance goals ....▶

Goals come in many forms. The extent to which governance, risk management and compliance goals are accomplished is an indication of the capability maturity of an organization. Most security and compliance goals require multiple steps. Deconstructing a goal by breaking down specific actions is helpful in defining individual steps and achieving the finished result. It's important to apply a goal-setting method that helps you be highly specific when articulating goals and their requirements and constraints.

Below are various aspects of goals and objectives:

1	**Types of goals and objectives:** • Short-, medium-, long-term goals • Positive vs negative goals • General vs specific goals • Process- vs results-oriented objectives
2	**Setting goal targets** • Minimum, average and maximum output
3	**Eliminating and then refining your goals**
4	**The benefits of clearly defined goals**
5	**The connection between goals and productivity and the need for tradeoffs**

Types of goals and objectives

Security and compliance goals can incorporate short-, medium- and long-term objectives designed to identify steps toward overall success. Goals typically present the big picture and, if they are not specific enough, may seem intangible because they are too broad or general. For instance, one of the goals for your business might simply be "24/7 protection of sensitive data in accordance with regulatory compliance requirements." With such a general statement, this goal may seem unattainable.

Determine your long-term security and compliance aims.

Start by distinguishing long- from short-term goals. Your long-term goals should have a timeline of three to five years. Long-term goals generally reflect your company mission and should be distinguished from short-term goals.

Break down each long-term goal into medium- and short-term objectives.

Similar to how you break down short-term goals, you will need to break down your long-term goals into actionable medium- and short-term objectives. A goal that remains unclear, not broken down into concrete objectives (partial goals), runs the risk of taking on a life of its own. Without concrete goals, there are no criteria that can be used to judge whether progress is, in fact, being made. For example, if your long-term goal is for every system component across your compliance environment to be demonstrably effective and sustainable, you will need to break this down into short-term objectives that ultimately will help you accomplish the long-term goal. Examples of actionable objectives for the above goal would be to prioritize the system components that can most impact the risk and security of CHD and ensure that the components are designed to operate in an effective and sustainable manner. Then, incrementally move on to improve other components to the desired level of effectiveness and sustainability.

Positive vs negative goals

In general, there are two different kinds of goals: positive and negative. With some security and compliance projects, you act to bring about conditions considered desirable. With others, you act to change, abolish or avoid conditions considered undesirable. To work toward a desirable state of affairs is a positive goal; to correct or prevent a deficient state of affairs is a negative goal. This is an important distinction. With a positive security and compliance goal, you want to achieve a definite condition. The organization pursues changes to bring about certain conditions that are considered desirable. With a negative goal, you want a condition to not exist. The intentions to avoid or change undesirable conditions (negative goals)—such as a payment card data breach—are often not well defined, but instead expressed in broad, rather vague terms.

General vs specific goals

You can also distinguish between general and specific goals. Typically, general (or generic) goals define broad primary outcomes and general security and compliance intentions and ambitions of the organization. They are comparatively easier to define and cover a larger scope—setting a wide, overarching target with a few or single criterion. However, they may be more difficult to measure. In contrast, specific goals are very precisely defined by many criteria. Specific goals lead to specific practices. Goals are more likely to be reached when they are clearly defined, with as much detail and specificity as possible.

Process- vs results-oriented objectives

Process objectives are like resolutions. The security team may resolve to allocate resources to spend a certain number of days per month assessing and documenting the status of controls, or they may decide to update a certain percentage of outdated systems each week.

Results-oriented objectives are usually dependent on processes or a series of actions, but are considered achieved based solely upon the outcome.

A security team may be successful in achieving an objective when all outdated systems are successfully upgraded. Another example would be when all required PCI DSS controls are fully documented across the control environment.

Unless standards are set very low, process objectives are more readily achieved than the results-oriented objectives, because processes are more controllable than outcomes. Organizations that have the skills and experience to achieve a certain result find it easier to design their activities to assure that they reach their objectives and goals.

PCI security management: Setting goal targets

When you establish goals for your security and compliance program, there are several different ways you can go about it.

Minimum output

The first way is to target the minimum output for your PCI security program. Typically, this means doing only what is necessary to avoid failing a compliance validation assessment. However, the intent is to focus on making steady progress so that overall you'll end up doing enough to make it count. It's all about steadily improving process and capability maturity while effectively protecting payment card data across your control environment.

Example: Create an objective to improve the processes and documentation for a specific percentage of PCI DSS controls each week.

Average output

The second way is to commit sufficient resources to your PCI security program to target the average output. Set a goal and objectives that require higher performance. You may not achieve them all the time, but if you reach them enough, you'll end up making a big difference.

Examples: Improve the daily log-monitoring capability and process. Increase the daily target of the manual log-review processing throughput, and reduce the number of false-positive log alerts so the team can fully meet the intent of PCI DSS Key Requirement 10.

Maximum output

There are several situations that mandate high performance and increased workload for security and compliance initiatives to succeed. That means investing resources and energy to drive maximum output, surmounting a specific, intense threshold that will push your compliance program output to a new level. Examples include driving progress on compliance initiatives with tight deadlines; reorganizing your resources and their assignments and priorities to focus on the PCI security compliance program deliverables, with minimum distraction from work that's not PCI-security related, increasing the input and support received from other departments to maximum capabilities.

When should you target the minimum?

Focusing on the minimum without consistently sustaining the effort is not a recommended strategy for anyone protecting payment card data. Minimum targeting is the art of patience and endurance. When improvements are applied consistently each week, even small efforts can accumulate into large gains over time.

When should you target the average?

Average targeting is the strategy of continuing what you have been doing, but expecting more from yourself, your security teams and your organization—and continuing the effort for longer. In contrast to minimums, many data security and compliance goals are set to try to provoke an average investment. The difference between this approach and a minimum isn't, however, strictly about how much effort you invest. Rather it's about how you frame the goal. Targeting the average is about keeping the long term in mind. You're hoping to sustain something, even if it's not always an easy and consistent output.

When should you focus on the maximum?

Focusing on the maximum has the advantage of expanding the potential of your security and compliance capability. Many areas where growth is needed to improve data security and compliance within your control environment exhibit elements of friction that, barring some kind of intense effort, planning and potential frustration, won't be realized.

> "If you set your bar at 'amazing,' it's awfully difficult to start."[70]
>
> —Seth Godin

The downside of focusing on a maximum is that it often isn't sustainable unless you have proportional investment and commitment from the organization. Bursts of high intensity rarely make for stable, long-term habits.[71]

Maximum targeting should not be applied as a sprint; data security is a marathon. A sprint cannot be sustained perpetually. However, maximum targeting works well when there is an efficiency gain for reaching higher levels of intensity, or when other barriers impede progress without such intensity. For example, if there are critical PCI DSS controls that are not in place, and they are putting your control environment and payment card data at risk, you may need to apply maximum targeting (as a sprint) to break through and overcome constraints that prevent you from putting those controls in place.

Manage goal competition.

Organizations have security and compliance goals that they need to accomplish in the long term. However, many find it difficult to focus on all of them simultaneously.

"Goal competition," where goals are competing with one another for time and attention, is one of the greatest barriers to securing needed commitments and resources. In many organizations, it's common for departments and individuals to pursue multiple goals. In that scenario, the importance of a goal can shift during the year, becoming, for whatever reason, a lower priority compared to a competing one. This can result in key stakeholders or departments investing few resources (attention, time, people, focus, money) in what was originally a prioritized goal, and more in one that's perhaps less critical.

For this reason, it's important to eliminate competing goals and then prioritize those that are remaining. Align your teams and focus your resources into accomplishing your reduced set of prioritized goals before moving on to others.

At the same time, in complex environments like payment card data environments, it's essential to pursue several goals at once.

Contradictory goals are the rule, not the exception. For example, an important goal is to achieve sustainable control effectiveness. PCI DSS requirements have three major goals:

- **Meet all relevant requirements:** the intent of the control objective, the requirements and test procedures
- **Control environment effectiveness:** the intent and objective over extended, uninterrupted periods

- **Control environment sustainability:** sufficient robustness (resistance to unwanted change) and resilience (ability to rapidly recover from unwanted change)

It's essential that all mandatory requirements are met. Compliance with PCI DSS is binary—you either met all of the requirements or you didn't. It's not only the effectiveness of individual security controls, but also the effectiveness of all the interdependent control systems within the environment, that determine the overall effectiveness. To make the control environment more effective, organizations need to do more work, such as improving processes and documentation. This typically requires manual labor, which increases workloads. Increased workloads can divert attention away from other important activities. So, attending to security governance and maturity improvement can, in the short term, be perceived as making the environment less sustainable unless more resources are added. Therefore, it can be perceived that these goals are at odds with each other.

When dealing with problems in complex systems, few activities are as important as setting useful goals. When you don't formulate your goals well or understand their interactions, the performance of the compliance and control environments suffer. If you overlook implicit contradictions among the security and compliance goals, you may initially achieve good results, but in the long run, you'll experience bad results.[72]

---

70 "Seth Godin Quotes," https://citatis.com/a20730/26d453
71 Scott H. Young, "Should You Target the Minimum?" Scott H. Young blog, Feb 2019, https://www.scottyoung.com/blog/2019/02/13/min-avg-max
72 "The Importance of Setting Business Goals," happierco, https://www.happierco.com/blog/importance-business-goals/

Security and compliance benefits of clearly defined goals

Clearly articulating and documenting security and compliance goals may be seen as additional work. But there are compelling reasons why it's beneficial to invest the time.

1   **Setting goals helps you establish perspective and frame your approach.**
When you have clearly stated goals (which should be written and communicated to all stakeholders), attention is brought back to what you are trying to accomplish. The 2020 PSR (page 21)[73] included the challenges of security teams being much too focused on technology. "Shiny Object Syndrome" is common. To address this problem, your goals should focus on the achievement of sustainable control effectiveness of the entire control environment, which requires a strategic approach.

2   **Articulating goals helps to focus attention.**
Goals provide decision support. They give you a clear sense of when to say "yes" or "no" to requests that compete for your attention. Strategy is about directing resources to focus on prioritized objectives and goals. It's more about saying "no" to avoid distractions than about saying "yes" and diverting attention elsewhere.

When CISOs and their teams are approached to give away their time and attention, each request can be measured against the stated goals. You can ask yourself, "Does this move me closer or further away from my goals?" We are all busy. The question is: "What are you busy doing?"

3   **Goals allow you to measure overall progress.**
Measuring overall progress is probably one of the most important reasons for having goals and setting milestones and time frames. It presents a yardstick to gauge how you are doing against the overall targeted outcome. Rather than having a vague notion of how the improvement of the control environment is advancing, you have something to measure against.

The security team should work toward goals that result in an organization's capabilities and processes, where the control is sufficiently robust and resilient; where it can confidently and demonstrably be proven that it achieved the required level of sustainable control effectiveness.

Having these measurements also can give you a sense of accomplishment. Having documented where you started from, it's possible to see your progress. It can keep the motivation of the security team high when working toward a goal becomes hard. From here you can assess what's working, what's not, where you may need some help or how you need to tweak the goal.

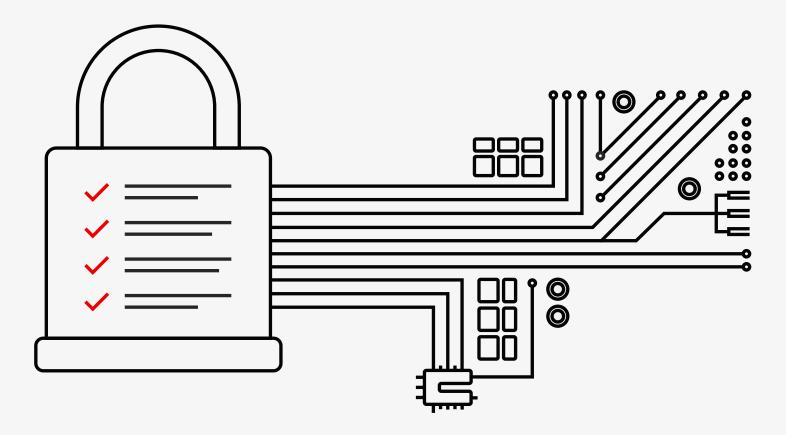**4**   **Goals should be communicated to employees, contractors, partners and vendors.**
If the goal is vague ("to be PCI security compliant"), not much exists for people to get inspired by nor determine how they can help. Crafted goals and objectives motivate other people to see where they can make a difference for you to achieve your goals. People want to help and contribute, but perhaps don't follow through because they're not clear on how to make an impact. Sharing clear goals and objectives, and why you want to achieve them, helps them understand the organization's needs.

---

73   2020 Payment Security Report, Verizon, 2020, https://www.verizon.com/business/resources/reports/payment-security-report/

Appendix B:
Content review and security checklist

The table on the next page is a summary of essential knowledge and insights gleaned from the Commentary section on page 16. It serves as a handy checklist to help identify which critical elements may not be fully in place within your control environment. During a PCI security assessment, it's common for assessors to find underdeveloped or missing key management elements. This lack of capability and process maturity brings the effectiveness of many, if not most, PCI security programs rightfully into question. The elements listed serve as major milestones on the journey to develop a mature approach to managing governance, risk management and compliance activities.

#	Critical security and compliance management components	Relevance	Yes/No
1	**The Security Management Canvas (TSMC):** Are all five elements of TSMC in place? Review the questions below to decide**.**	Any missing element from TSMC can degrade visibility, management decision-making and performance. See page 32 for details.	
1.1	**Security business model:** Is an up-to-date, overarching security business model applied to support communication and decision-making?	Without a documented business model, it's difficult to clearly express the value of security and compliance, making it harder to secure investment for compliance and security programs.	
1.2	**Security strategy:** Is the strategy effective at directing resources to remain focused on achieving prioritized goals and objectives?	Unclear strategy results in a lack of direction, alignment, focus and clarity on goal and objective prioritization, and muddies the determined path and approach to their achievement.	
1.3	**Security operating model (SOM):** Are all key operational elements across the control environment and their relations documented and visually mapped?	A SOM is essential for understanding how organization structures and processes deliver value, and it's an essential tool for identifying and diagnosing performance issues.	
1.4	**Security frameworks:** Are supplemental security frameworks fully integrated into your GRC/PCI security program?	The use of additional frameworks supports your security and compliance management system. Refer to page 55 of the 2020 PSR for details.	
1.5	**Security program:** Is your program management maturity sufficient to maintain sustainable control effectiveness?	Maintaining management at a program (not project) level helps to direct and ensure the integration and achievement of long-term goals and objectives.	
2	**GRC:** Is your PCI security program fully integrated within your larger corporate governance, risk management and compliance initiatives?	The synchronized integration of all GRC activities translates into increased efficiency and bottom-line financial benefits for businesses.	
3	**Goals:** Are the goals for your overall security and compliance initiative, and for each individual critical management component, clearly defined, documented and communicated?	Clearly defined and communicated goals are indispensable to effectively directing and managing a security strategy and program. Neglecting to communicate goals and objectives is highly detrimental to program performance and outcomes.	
4	**Requirements:** Are all requirements (conditions) to achieve the goals known, fully understood, clearly defined and communicated?	Determining the exact requirements to achieve goals and objectives is essential and includes clarity and distinction between necessary vs sufficient conditions.	
5	**Constraints:** Do you have an effective process to identify and remove all critical program limitations and restrictions that hamper the achievement of goals?	The best approach for performance, capability and maturity improvement is knowing what the biggest constraint is and an ongoing process to repeatedly remove that constraint.	

Appendix C:
5G and payment security

By Ravi K. Annadanam,
5G and MEC Innovation,
Verizon Business Group

The appeal of emerging technologies, such as 5G and edge computing, gained significant momentum when the COVID-19 pandemic exposed the weakest links of the financial services industry. Many financial technology (fintech) companies are seeking to use such technologies to help the industry move forward.

COVID-19-related public health concerns also forced many merchants to open their businesses through digital doors, which accelerated the growth of online commerce. This shift of consumer behavior from in-store to online, as well as a significant increase in contactless payments, is expected to become the new norm and continue in the post-pandemic environment. Some smaller retailers forced to close in the crisis may not ever reopen physically but are seeking a digital future instead. The rapid build-out of omnichannel retail capabilities—which will bridge payments in any environment, physical or digital—is expected to become an essential requirement for all commerce.

More digital and mobile device payments

The finance sector is experiencing a significant increase in the use of mobile devices for customer transactions, especially personal banking. The speed and stability of 5G could enhance this experience as well as provide greater security by enabling consumers to opt into advanced biometric-based identification and verification methods. The financial sector could also allow consumers to opt into geolocation technologies in an effort to more effectively pinpoint fraud.

For customers, 5G can provide highly secure connections for video conferencing with financial professionals and loan counselors. Additionally, connecting a 5G device to a 5G network could unleash revolutionary experiences for consumers. For example, 5G may finally deliver on the promise of "shoppable videos." Have you been in a situation where you see a pair of shoes and want to take a picture, click on it and buy them instantly?

The high bandwidth and low latency that 5G can offer could make these shopping experiences possible through what is called augmented reality and virtual reality (AR/VR). The retail industry could also offer "experiential" purchases, such as buying a vacation package or purchasing a bed and other home furniture through AR/VR. The added depth of understanding could boost buyer confidence and potentially improve conversion rates. Enabling new features for consumers opting into them—such as digital IDs, transaction monitoring and reporting to mobile wallets —could fuel even more growth. 5G and edge computing also could make geotargeted offers for consumers opting into such notifications timelier and more accurate, thanks to faster throughput and higher data volumes. These technologies, as well as secure contactless payments, are expected to increase in demand with companies of all sizes.

As mobile transactions increase in volume, security in a digital identity environment becomes paramount, and fraud prevention for mobile transactions becomes critical.

Fraud prevention, combined with consumer awareness, could change consumer attitudes toward data usage and provide opportunities to use mobile and transaction data with customer consent in other areas, such as contact tracing during pandemics.

To embrace emerging e-commerce trends, financial institutions need to increase the speed and reduce the cost of payment processing and leverage cloud-based infrastructure, automation and AI-driven analytics to enhance user experiences.

In summary, providers of managed 5G networks and security services need to understand the uncertainty and increased pressure the financial services and other industries face while providing the technology fabric to address challenges to:

- Adapt to new social conditions
- Apply 5G and mobile edge computing (MEC) to new capabilities
- Stay cyber resilient

What exactly is 5G?

The 5th generation mobile technology (5G) provides a more-advanced global wireless standard, building on the solutions provided by 1G, 2G, 3G and 4G technologies. 5G is designed to interconnect machines, devices and the Internet of Things (IoT). Its technology can deliver higher multigigabits per second (Gbps) speed, and a more uniform experience for a wider quantity of users through a massive network. 5G's reliability, peak data speeds, ultralow latency and overall improved performance and efficiency will enable new industries, artificial intelligence (AI) and device-centric industries, and more small and medium businesses to connect in new ways.

5G's unified, more-capable interface and extended capacity for next-generation user experiences will impact every industry—from payment security to remote healthcare, transportation safety and agriculture.

5G building blocks

First generation—1G
1980s: 1G delivered analog voice.

Second generation—2G
Early 1990s: 2G introduced digital voice (such as Code Division Multiple Access [CDMA]).

Third generation—3G
Early 2000s: 3G brought mobile data (such as CDMA2000).

Fourth generation—4G LTE
2010s: 4G LTE introduced mobile broadband.

Potential impact of 5G on payment card compliance

Financial institutions and merchants will continue to find innovative ways to benefit from 5G-enhanced features, open architecture and MEC technologies. At the same time, security practitioners need to explore how these new innovations might impact the payment card industry (PCI) compliance posture. What unintended consequences might occur as society transitions to greater connectivity through 5G networks? Since we are talking about innovation and the future, we don't have answers to all questions, and in many cases, we don't even know what questions to ask. However, the following are some areas to consider:

Education and learning: Traditionally, the work of PCI compliance and security assessors with wireline and Wi-Fi networks is well understood. It is expected that many services and applications in a PCI security scope will be hosted in public or private MEC environments in the future, which will require everyone to understand how cellular networks work, since 5G and MEC are usually combined to provide maximum benefit.

New data flow paths: Many merchants are already exploring how 5G technologies could prove more beneficial than Wi-Fi in some areas, including retail stores. This creates new data flow paths that would traverse not only the 5G radio network, but also back-end wired networks of 5G service providers. Understanding these new data flow paths will be crucial both for merchants and PCI security assessors.

Compliance status of new cloud service provider (CSP) offerings: Major 5G vendors have started offering 5G MEC services that connect 5G networks with CSPs, including Amazon Web Services (AWS), Azure, Google Cloud and others. It's expected that PCI security applications will be hosted in these new offerings from CSPs, which will require PCI compliance.

Threat monitoring for applications hosted in MEC: Traditional security controls (network segmentation, threat monitoring, integrating into SIEM/SOC, encryption, etc.) will still apply for MEC-enabled applications. This will require working closely with 5G service providers, and in some cases, integrating their services into overall solutions for PCI compliance.

New use cases: It's expected that new innovations will create new use cases that would come under a PCI compliance scope—for example, purchases inside AR/VR applications, and interactive videos, apps and games running in a MEC environment.

IoT devices: The 5G standards create new opportunities for using IoT in all industries, including financial and retail segments. It's expected that more and more organizations will use IoT technologies for financial transactions, which will bring new areas under a PCI compliance scope.

Search for a killer app: Many people are searching for a killer app built on 5G technologies. We don't know yet what that killer app will be, but retail and finance sectors are likely to see significant innovation in the coming years, with new ways of doing business that involve payment card processing.

What security features exist in the 5G standards?

Securing the 5G network is about leveraging new security features that are part of the 3rd Generation Partnership Project (3GPP) standards. Enhanced security, as compared with 4G LTE, is possible, thanks to 3GPP's new trust model and security architecture. The main components of the security architecture are:

- **User equipment (UE):** Includes protecting information that could be used to identify and track a subscriber, preventing attackers from modifying user traffic, and ensuring subscribers only connect to trusted cell sites

- **Radio Access Network (RAN):** Provides secure communications on all RAN interfaces and includes extra protections at places that are vulnerable to physical attacks

- **Core network:** Includes specialized network functions (NFs) and enhanced protections for the new service-based architecture (SBA) that NFs will use to communicate

What are public and private MEC anyway?

Mobile edge computing is an evolution of cloud computing services that brings application hosting out from centralized data centers down to the network edge, or in the case of private MEC, actually on-premises, thus closer to wireless devices or 5G endpoints. Developers can use the same familiar cloud platform services and tools (such as compute, networking and storage) on the MEC platform.

Public MEC is located on the edge network closer to the end users; therefore, it can enable network latency in the 20–30 milliseconds (ms) range instead of requiring data to be processed in the core cloud data centers. The network latency range provided does not include application latency and is a target within the coverage area of 5G Ultra Wideband (UWB). This also provides enhanced security and data sovereignty. By enabling cloud servers to run closer to end points, MEC can help developers reduce latency, enhance reliability and speed local processing. MEC also enables processing to happen in the network, rather than in devices, and this can allow for increased battery life and faster deployment of new applications and services.

Private MEC brings these cloud platform services even closer by physically co-locating them on the customer's premises where data is generated and actioned and thereby providing the lower latency range of (10–20 ms), based on the deployment environment, required for the many critical and latency-sensitive applications. Having a private onsite 5G wireless network coupled with these on-premises compute resources can also enable data sovereignty and enhanced security. It's possible for the 5G network operator to provide full end-to-end installation and management, simplifying the customer's day-to-day operations. Think of it as having the cloud in your back pocket!

Our recommendations?

Verizon expects 5G to revolutionize use cases and applications in the financial services industry, including security and fraud control, as highlighted below.
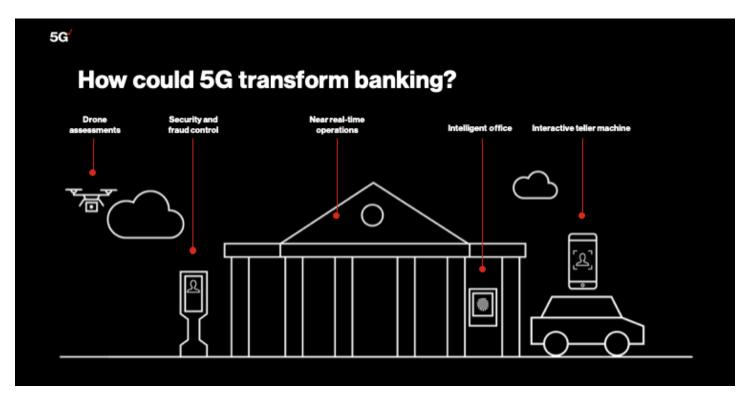

Figure 30. Five ways 5G could impact banking

5G use cases in financial services

Security and fraud control

Security challenges that financial services companies face today include:

- Securely monitoring financial transactions
- Assisting customers with wrongfully declined transactions and security updates to applications
- Reducing fraud: In 2020, the U.S. Federal Trade Commission (FTC) received more than 2.2 million reports about fraud totaling nearly $3.3 billion in losses[74]

5G could help solve those—and other—challenges by supporting:

- Increased use of AI and machine learning (ML): These technologies provide risk management and customer service benefits. Additionally, AI is recognized for its fraud detection potential. Some 80% of specialists who use AI to detect fraud believe it has the capability to reduce payments fraud[75]
- Enhanced proactive fraud prevention, with near real-time security monitoring
- Rapid sorting of data, such as transaction amount and merchant ID, to reduce fraud detection errors
- Enabling near real-time security enhancements and updates

The security benefits to businesses utilizing 5G-related services include:

- Boosting mobile security with rapid incident detection and fraud monitoring
- Updating and delivering security enhancements in near real time, without customer involvement
- Allowing more data to travel across networks in near real time, helping to augment fraud prevention

---

74 Monica Vaca, "The top frauds of 2020," Federal Trade Commission Consumer Information, Feb 4, 2021, https://www.consumer.ftc.gov/blog/2021/02/top-frauds-2020

75 "Deep Dive: How AI and ML Can Reduce Fraud and Increase Customer Satisfaction," PYMNTS.com, Feb 23, 2021, https://www.pymnts.com/fraud-prevention/2021/ai-ml-fraud-customer-satisfaction/

5G use cases in financial services

Interactive teller machine

Some of the challenges that today's banks are facing include:

- **High cost of buildings:** Bank branches typically cost between $600,000 and $800,000 a year to run[76]

- **Low profitability:** Just slightly more than half (52%) of all branches in the banking industry are achieving acceptable levels of profitability; more than one-quarter (28%) are below breakeven[77]

- **Traditional customer preferences:** Brick-and-mortar locations are still one of the leading sales channels; 30% to 60% of customers prefer doing some of their banking at branches[78]

5G/MEC-enabled interactive teller machines (ITMs) could help solve these — and other — challenges, by enabling banks to:

- Deploy full-fledged banking services in locations where a traditional brick-and-mortar branch isn't practical

- Support functionality generally found only in brick-and-mortar branches

- Enable remote video sessions with a human banker, where more sophisticated solutions are required or a personalized touch is needed

- Help drive sales through highly personalized services using AI-driven analytics

5G may also help enable near real-time financial operations, accelerating trading, loan transactions and other processes. And intelligent branch/smart offices could provide high customer satisfaction, productivity and shareholder value.

5G security is constantly evolving. Updates to various features are expected in 2022. The content presented in this appendix was written in 2021.
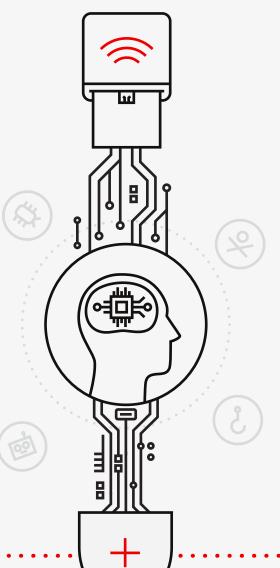
76 Guenther Hartfeil with Peak Performance Consulting Group, "Are Your Bank's Branches Too Small to Survive?" The Financial Brand, Aug 15, 2018, https://www.thefinancialbrand.com/74386/bank-branch-roi-deposits-profitability/

77 Ibid.

78 Klaus Dallerup, et. al., "A bank branch for the digital age," McKinsey & Company, Jul 18, 2018, https://www.mckinsey.com/industries/financial-services/our-insights/a-bank-branch-for-the-digital-age

Appendix D: AI and ML in the payment card industry

By Rafeeq U. Rehman, Verizon Security Solutions

Machine intelligence is a brave new world that has just started to emerge with significant opportunities for the payment card industry. Effectively managing risk in this new world is crucial to realizing these new opportunities. Expansion of artificial intelligence (AI), especially machine learning (ML), is occurring in a range of areas, including:

- Detecting fraudulent credit card transactions
- Effective targeting for cross-selling and upselling
- Managing credit lines
- Overdraft and pay-later options
- Intelligent chatbots with natural language processing (NLP) capabilities
- Smart and personalized management of reward systems

ML models, if properly built and trained, can identify issues as well as create new opportunities for different players in the payment card industry value chain.

Why organizations should care about advancement in AI/ML

AI clearly is revolutionizing many areas and creating new possibilities, but it also needs careful implementation to safeguard against new types of attacks, such as:

- Poisoning the training or test data to impact ML models' decision-making; embedding backdoors
- Evasion methods that cause a trained model to malfunction
- A variety of other attacks, some of which are listed in the Adversarial Robustness Toolbox documentation[79]
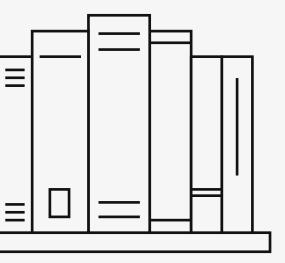
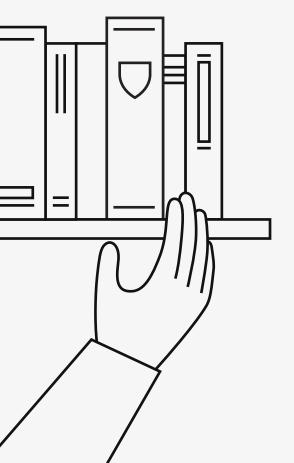79 "Art Attacks," GitHub, https://github.com/Trusted-AI/adversarial-robustness-toolbox/wiki/art-attacks

What organizations should consider doing

A major issue for security teams is the lack of understanding of how ML models are built, trained and utilized. Most of this implementation is done by innovation teams that lack a decent understanding of the security implications. So, what should organizations do to prepare for and better understand AI and ML?

Security teams need to create budget and train personnel to build capabilities to understand these new technologies. Organizations need to protect the development and test environment, which is crucial, as this is where models are built, trained and tested. Compromises of these environments are key to poisoning attacks, by altering training and test data sets. This is counterintuitive to the traditional notion of focusing on protecting the production environment. Testing, verification and certification of trained models for vulnerabilities is key to stopping many attacks, especially evasion.

Appendix E:
Suggested reading

"Reading alone is not enough. We have to contextualize the knowledge. When does it work? When doesn't it work? Where can I apply it? What are the key variables? The list goes on. If you can take something you've read and apply it immediately, it will reinforce the learning and add context and meaning. Another way to reinforce the learning is to apply the Feynman technique, named after the Nobel Prize-winning physicist Richard Feynman. You can think of it as an algorithm for guaranteed learning. There are four simple steps: choose a concept, teach it to someone unfamiliar with the subject, identify gaps in your understanding and go back to the source material, and review and simplify. Teaching others is a powerful way to embed information in your mind. Upon completing a book, grab the nearest (willing) person and tell them about what you have learned. You'll have to remove or explain the jargon, describe why this information has meaning, and walk them through the author's logic. It sounds simple. After you try it the first time, you'll realize it's not easy. If there is no one around who is interested, try writing a review where people are encouraged to comment and debate. In order to think for yourself, you need to reflect on your views and see how they stand up to feedback,"[80] according to Farnam Street.

This suggested reading list is a gold mine of information for those tasked with managing security, data protection and compliance programs. One of the best ways to develop proficiency and master data security is to absorb the wealth of information accumulated from experts in the last two decades. CISOs should brush up regularly on guidance from the best and brightest. This list includes new additions to those published in the Verizon 2019 and 2020 Payment Security Reports.[81] This year's focus is on strategic guidance for CISOs on how to apply a systems approach to complex problem solving and continuous improvement – by using the Logical Thinking Process and the Theory of Constraints to achieve clear goals.

80 "How to Remember What You Read," Farnam Street, https://fs.blog/2021/08/remember-books/
81 2019 and 2020 Payment Security Reports, Verizon, https://www.verizon.com/business/resources/reports/payment-security-report/

Suggested reading list

	Year	Title	Author	Publisher	Pages	ISBN
1	2007	The Logical Thinking Process: A Systems Approach to Complex Problem Solving (A new edition of Goldratt's Theory of Constraints)	H. William Dettmer	American Society for Quality (ASQ) Press	413	978 0 87389 723 5 https://www.amazon.com/dp/0873897234
2	2020	From Symptoms to Causes: Applying the Logical Thinking Process to an Everyday Problem	Thorsteinn Siglaugsson	Thorsteinn Siglaugsson	54	978 1654 544829 https://www.amazon.com/dp/1654544825
3	1996	Goldratt's Theory of Constraints: A Systems Approach to Continuous Improvement	H. William Dettmer	ASQ Press	378	0 87389 370 0 https://www.amazon.com/dp/B001DORDE8
4	1999	Theory of Constraints	Eliyahu M. Goldratt	North River Press	162	88427 166 8 https://www.amazon.com/dp/0884271668
5	2021	Systems Thinking—And Other Dangerous Habits	H. William Dettmer	Virtual Books	409	978 163838 003 1 https://www.amazon.com/dp/1638680035
6	2010	Theory of Constraints Handbook	James Cox, John Schleier	McGraw-Hill Education	1216	978-0071665544 https://www.amazon.com/dp/0071665544
7	2019	Theory of Constraints, Lean, and Six Sigma Improvement Methodology	Bob Sproull	Productivity Press	306	978-0367247096 https://www.amazon.com/dp/0367247097/
8	1999	Management Dilemmas: The Theory of Constraints Approach to Problem Identification and Solutions	Eli Schragenheim	The St. Lucie Press	208	978 1574 442229 https://www.amazon.com/dp/1574442228
9	1998	Project Management in the Fast Lane: Applying the Theory of Constraints	Robert C. Newbold	CRC Press	284	978-1574441956 https://www.amazon.com/dp/1574441957
10	1999	The Measurement Nightmare: How the Theory of Constraints Can Resolve Conflicting Strategies, Policies, and Measures	Debra Smith	Saint Lucie Press	184	978-1574442465 https://www.amazon.com/dp/B0095H1E0Y
11	1998	Essays on the Theory of Constraints	Eliyahu M. Goldratt	North River Press	280	978-0884271598 https://www.amazon.com/dp/0884271595
12	2003	The Systems Bible: The Beginner's Guide to Systems Large and Small	John Gall	General Systemantics Press	316	978-0961825171 https://www.amazon.com/dp/0961825170
13	1997	Rapid Problem Solving with Post-It® Notes	David Straker	Da Capo Press/ Perseus Books	176	1555611427 https://www.amazon.com/dp/1555611427
14	2021	Big Breaches: Cybersecurity Lessons for Everyone, 1st ed.	Neil Daswani and Moudy Elbayadi	Apress	474	978 1484266540 https://www.amazon.com/dp/1484266544

Verizon 2022 Payment Security Report

Editorial team

Lead author

Ciske van Oosten

Co-authors

Cynthia B. Hanson, Rafeeq U. Rehman, Ravi Annadanam

Lead editor

Cynthia B. Hanson

Data analysts

Abdelkrim Aoued Ahmed Bacha, Allison M. Fortier, Eric Jolent, Mikhail Banguerski, Noel Richards, Ron Tosto, Xavier Michaud

Contributors

Abdelkrim Aoued Ahmed Bacha, Claire Lavelle, Dyana Pearson, Ferdinand Delos Santos, John Galt, John Grim, Michelle Wire, Neal Maguire, Rokon Rokonuzzaman, Sean Sweeney, Virgil Hayes, Xavier Michaud

Payment security consulting practice

Verizon Cyber Security Consulting

Managing Director, Security: Kristof Philipsen

PCI and payment security consulting practice

Global lead: Sebastien Mazas

APAC region: Ferdinand Delos Santos

Americas region: Matt Arntsen

EMEA region: Loic Breat

Global intelligence: Ciske van Oosten

Legal review: Sudha T. Kantor

Team email:

paymentsecurity@verizon.com

PCI DSS data contributors

Third-party contributors

Marco Borza (Advantio); Héctor Guillermo Martínez, Alberto España, Rogelio Nova, Russell M. Latimer (GMSectec); Anthony Petruso, Michael Vitolo (MegaPlanIT); Ron Tosto (Servadus)

About Verizon Cyber Security Consulting

This research publication is a product of Verizon Cyber Security Consulting, a global leader in the payment security practice with a security team of over 600 consultants in 30 countries. Verizon has one of the largest teams of PCI Qualified Security Assessors.

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

verizon✓