PSR

2021 Payment Security Report insights

PCI DSS v4.0 white paper

Verizon Cyber Security Consulting

The latest update to the flagship Payment Card Industry Data Security Standard (PCI DSS) will help organizations ensure that data security controls remain relevant and more 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 Verizon Payment Security Report (PSR) is essential reading.

Grounded in decades of rigorous research, the PSR provides the definitive guide to innovating a winning approach to security and compliance within the payment card industry. The series of reports, dating back to 2010, is perfect for teams across all lines of assurance—from boardrooms and security steering committees down into the trenches of security and compliance operation teams.

The PSR provides answers to big payment security questions. Keen insights and commentary clear the fog, answering questions such as:

- How do you choose what to prioritize and what to spend time on?
- How do you choose your goals and objectives?
- How do you unravel requirements and remove constraints?

When an organization is doing well, it's usually because employees are productively engaged in their work and have a clear sense of direction as to where the organization is headed. The same is also true for data security and compliance efforts. This only happens when the organization makes a concerted effort to manage performance, both for the business as a whole and individual employees.

How many in your organization honestly understand and know where to find its security and compliance goals and objectives? What criteria are you using to ensure optimization of scarce security team resources? Are you making the right decisions on your goals, objectives and strategy, and how to deal with constraints?

For many organizations that struggle to maintain PCI security compliance, achieving strategic success is closer than they think. This especially becomes true when they follow the PSR's known wisdom and meticulously crafted steps.

The PSR has helped countless organizations find a way forward with sound security program innovation, practical frameworks and novel advice. The report's actionable, hands-on frameworks help security practitioners build and implement innovative, robust security business models, operating models and strategies.

Now comes our invaluable advice on PCI DSS v4.0 and how to negotiate the 10th release of the PCI Standard, one of the most challenging changes in the PCI DSS to date. Let us help your organization be prepared for the coming change.

The release of PCI DSS v4.0 can have a substantial impact on organizations. It's necessary to take the time and steps to update the goals, targets, measures, ownership, initiatives and other procedures that will change with PCI DSS v4.0.

Table of contents

Preparing for PCI DSS v4.0

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 expected in March 2022, it will be nearly nine years since the previous major update (version 3.0) and four years since the previous interim update (version 3.2.1), which made minor changes to the PCI Standard in 2018.

Prior to PCI DSS v4.0, the longest duration between updates to the PCI DSS was version 2.0 in October 2010 and the release of PCI DSS v3.0 in November 2013.

PCI DSS timeline

Release		Version
2004	December	1.0
2006	September	1.1
2008	October	1.2
2009	July	1.2.1
2010	October	2.0
2013	November	3.0
2015	April	3.1
2016	April	3.2
2018	May	3.2.1
	March	v4.0

For more than a decade, Verizon has documented compliance trends within the evolving payment security industry. The PSR has tracked compliance ups and downs while keeping a finger on the pulse of changing payment security technology. During that time, consumers and businesses have substantially increased business activities conducted online. As a result, the number of payment card transactions has also increased. The capabilities of threat actors continue to evolve and escalate—skillfully exploiting both old and emerging threats, as well as weaknesses within payment systems and processes. At the same time, digital transformations that heavily involve cloud technologies are introducing new drivers that impact the payment security industry. This further complicates the role of CISOs and other security managers and practitioners.

The release of PCI DSS v4.0 is a much-needed response to these concerns. It's the most substantial update to the PCI Standard in 17 years—since the release of DSS 1.0 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 PCI Standard, and PCI DSS v4.0 still has the familiar Control Objectives and 12 Key Requirements introduced in 2006, the new version enacts multiple changes to reflect the aims of evolving objectives and requirements. This includes numerous wording changes, updates to existing requirements, several new requirements and future-dated requirements.

Why is the PCI Council instituting a major rewrite of the PCI DSS when version 3.2 of the PCI Standard released in 2016 was considered to be fairly mature?

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

PCI DSS v4.0 specifically supports the use of key technologies, such as 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 PCI Standard requirements and adds intent statements. On pages 6 and 7 of this paper, we explore the two most significant updates in PCI DSS v4.0, which are continuous assessments and customized controls and control environments.

This revision of the PCI Standard is considered so significant that between 2019 and mid-2021, the Payment Card Industry Security Standards Council (PCI SSC) fielded an unprecedented amount of feedback on the PCI DSS v4.0 draft. For past revisions of the PCI Standard, formal feedback opportunities were limited to a single period for comments from the PCI SSC participating organizations and assessors. For PCI DSS v4.0, the PCI SSC expanded the feedback opportunities to maximize collaboration and stakeholder involvement in updating the PCI Standard.[1]

[1] 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

In summary, the most significant reasons for updating the PCI DSS are to:

- Ensure 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

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?”**

Navigating the transition period

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

Organizations working to upgrade their compliance environments may think they have ample time to resituate their controls. But with significant changes, including the customized approach option, they can't start to

Supporting data security by aligning your goals

The PCI SSC created the 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 will 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. Organizations 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. Once you clarify your goals, you can more easily implement a custom control and validation design.

With this in mind, some organizations successfully transitioned to security as a business-as-usual culture. Unfortunately, our 2020 PSR State of Compliance survey results reveal that nearly three-quarters of organizations (about 72.1%) still focus on passing their PCI DSS compliance assessment instead of maintaining truly effective and sustainable control environments. While control failures can still occur within organizations with effective control environments, they should be very brief, and rapidly detected and corrected. This requires a capability that is not built into the control environment of most organizations.

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.

Developing sustainable control design solutions

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

Some of the major changes introduced by PCI DSS v4.0 are enhanced validation methods and procedures that evolved from a defined-only approach to also include an objective-based, customized-approach option. 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. This traditional method for validating PCI DSS won't be going away with version 4.0. With the defined approach, requirements need to be met in a very specific manner and validated, sometimes regardless of the actual control outcome, such as whether the control system in question is actually effective and sustainable. The new customized approach allows organizations to use security approaches that may differ from traditional PCI DSS requirements as long as they can demonstrate that controls meet the intent of the relevant PCI DSS requirement 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.

Customized approach vs compensating controls

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 (traditional) requirements and testing procedures as written in the PCI DSS. This approach remains valid. All organizations can continue to benefit from the more prescriptive direction on how to meet the objectives. 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 where organizations can custom design security controls or adopt other controls outside of the familiar list of defined controls. This new customized approach of validating PCI DSS controls focuses on an outcome-based approach rather than a must-implement-based approach. As mentioned earlier, all customized controls must still meet the stated security objective of the requirement.

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

Requirements and validation options in PCI DSS v4.0 were redesigned to focus on security objectives and support organizations using different methodologies to meet the intent of PCI DSS requirements. The PCI Standard includes intent 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 achieves 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 methods at meeting intended security outcomes.

This alternate approach allows organizations to custom design and develop security controls by meeting several criteria:

- Determine the controls for a given security objective
- Submit detailed documentation to the Qualified Security Assessor (QSA) outlining the approach to adopt to achieve compliance and demonstrate the effectiveness of the approach
- After review of the evidence by the QSA, the QSA makes a final decision on the effectiveness of the control, based on the analysis of the documentation submitted

The impact of a customized approach

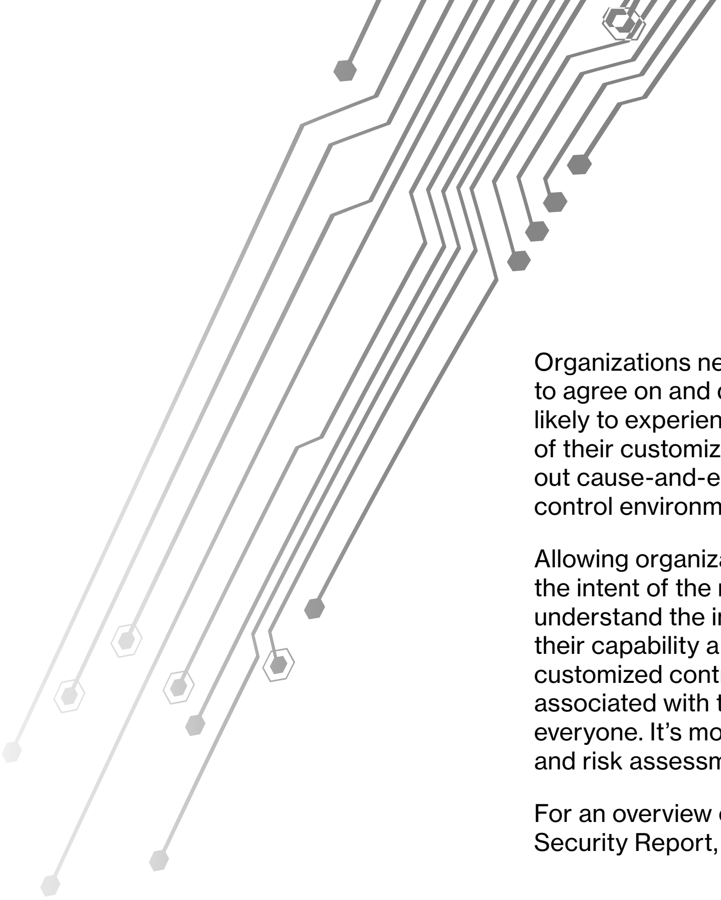
Customizing security controls should be done in a very structured way that delivers measurable and predictable outcomes. Organizations with mature control environments are more likely to embrace the new customized validation approach with confidence. They should also find it easier to rewrite how their 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 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 organizations more flexibility in how the PCI DSS 12 Key Requirements can be met, there is 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 for the design and management of security controls and the maintenance of the control environment. It requires higher levels of process and capability maturity on control design, control risk evaluation, control implementation and monitoring.

When choosing to follow the customized approach, organizations that do not 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 their control environment, which can lead to unintended consequences.



Organizations need to collaborate with the QSA or Internal Security Assessor (ISA) to agree on and develop tailored testing procedures. Several organizations are likely to experience unintended consequences from the design and implementation of their customized controls. They need to be aware of blind spots and seek out cause-and-effect relationships between controls, control systems and the control environment.

Allowing organizations to design their own controls and implement them based on the intent of the requirements can introduce new risks. Organizations need to understand the implications and increased responsibility. They need to determine their capability and competency to design, implement, maintain and monitor customized controls, as well as their capacity to maintain all the requirements associated with their approach. The new alternative approach may not be for everyone. It's most suited for organizations with fairly mature security, compliance and risk assessment processes in place.

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

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" defines three different types of unintended consequences:

- **Unintended benefit:** A positive, unexpected benefit (sometimes called a windfall or serendipity)
- **Unintended drawback:** A negative consequence with a positive benefit
- **Perverse result:** A negative consequence with no positive benefit[2]

[2] "Unintended consequences," Wikipedia. https://en.wikipedia.org/wiki/Unintended_consequences

Increased control risk: The Ever Given's misfortune

The perils of overlooking unintended consequences in security design can easily be underestimated. 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. Payment security requires a comprehensive, well-researched design approach to avert potentially damaging unintended consequences. This is especially true when combining the new customized approach of PCI DSS v4.0 with the multiple drivers of digital transformation, such as 5G, contactless payment, blockchain, artificial intelligence and machine learning.

The March 2021 catastrophe of the container ship Ever Given in the Suez Canal is an apt metaphor for what can happen when design, strategy and planning lack foresight and coordination. Several converging factors apparently resulted in a perfect storm that grounded the Ever Given for over six days:

1. **Container ships have at least doubled in size since 2000, especially in width, with limited regulation and/or coordination between the shipping industry and Suez Canal officials during that time.[3]**
2. **The narrow section of the canal where the Ever Given—one of the longest ships in service—became lodged sideways was not widened during the 2015 Egyptian canal redevelopment project, as were other canal sections.**
3. **The hydrodynamics of wide container ships in shallow, narrow canals creates less of a gap, which increases squatting and bank effects that make ships less maneuverable.[4] High winds and a dust storm on the day of the disaster apparently added to loss of control.**

> **"The best laid plans of mice and men often go awry."**
>
> —Robert Burns[5]

When implementing design changes, CISOs and security managers should consider the "precautionary principle,"[6] which emphasizes the burden of proof as being able to show lack of harm rather than 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," according to the Farnam Street blog.[7] When designing for change, such considerations may help organizations avert a costly data breach.

[3] "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

[4] 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 Apr 20, 2017, https://doi.org/10.1002/9781118476406.emoe006

[5] "To a Mouse," Wikipedia. https://sco.wikipedia.org/wiki/To_a_Mouse

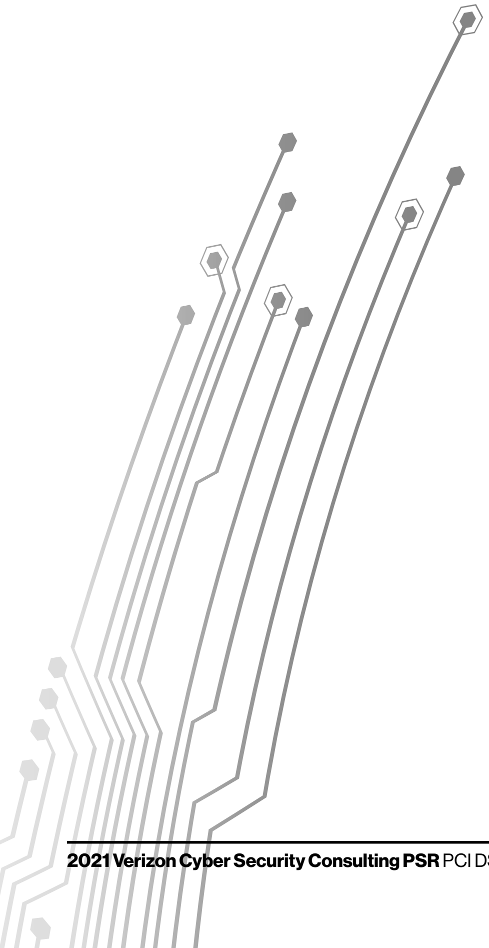
[6] "Precautionary Principle," Wikipedia. https://en.wikipedia.org/wiki/Precautionary_principle

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

Goals, Requirements and Constraints Model:

An approach for complex problem solving

Sustainable design requires sound strategy and a reliable business model. With the introduction of PCI DSS v4.0 and custom control design, CISOs and managers need to clearly understand the scope of the project—both the goals and constraints—in relation to each requirement. Referred to as the Goals, Requirements and Constraints Model, Verizon believes this approach to complex problem solving is an essential process for creating efficient, sustainable custom security design. We discuss this model at length in the 2022 PSR.



Applying logical thinking

The majority of organizations do not design and implement control environments that are truly effective and sustainable. 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 failproof 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. The application of logical thinking improves the ability to achieve progress in incremental but clear and predictable steps.

The misfortune of the Ever Given can be traced back to a lack of foresight and alignment with strategic goals, regulatory requirements and constraints. Security managers can benefit immensely from considering this triangular, interlinking model to avoid oversights in the design process.

During compliance validation assessments, conversations between the QSA and their clients frequently revolve around substantiating the true status of a PCI DSS requirement. A QSA typically works their way back from the current condition of the control at the time of the assessment to the decisions and actions the organization took, or failed to take, that contributed to or directly resulted in the negative outcome. Conversations inevitably journey back to the organization's security and compliance goals. In most cases, the evidence of the management of the control environment confirms insufficient attention was given to Goals, Requirements and Constraints. That ultimately resulted in control failure.

In most cases, this happens due to a combination of weak control design and weak implementation and maintenance that degrades the functional strength of the control system. Remember that each PCI DSS control always operates as part of a control system—without exception. Often when failures occur, it is because controls are not properly evaluated for robustness and resilience in the context of their dependent and interdependent controls. In addition, they often lack operational support from a sustainable environment and therefore are substantially less effective.

What are goals?

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

Clear communication of goals helps you conduct your day-to-day operations with a sense of purpose and direction. It promotes accountability, with team members being held accountable for their responsibilities to the collective team. Good communication lays a foundation for collaboration to work toward the achievement of the proclaimed goals.

Setting clear goals for PCI security compliance can affect individual performance through four mechanisms:

- Clear security-compliance goals direct action and effort toward goal-related activities and away from unrelated activities
- Clearly communicated goals energize employees and lead to higher employee effort
- Goals motivate employees to apply their existing knowledge to attain a goal or to acquire the knowledge needed to do so
- Frequent reminders of goals affect persistence, and employees may exert more effort to achieve high goals

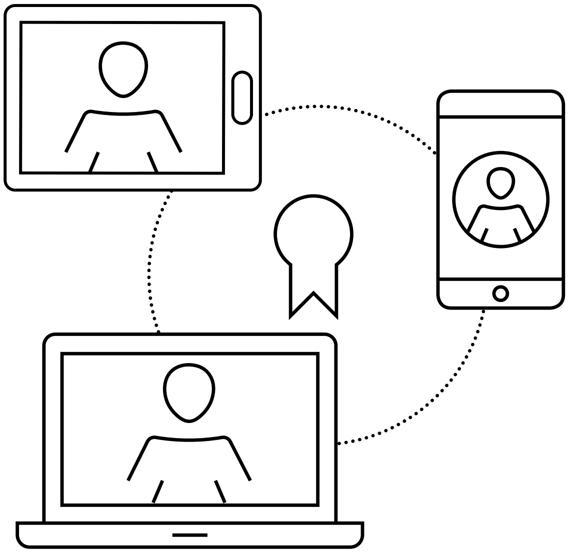
The following questions are worth asking:

- What goals were decided upon and communicated to the organization in regard to data security and compliance?
- Are they the same goals that members within each of the 4 Lines of Assurance (see page 12, 2019 PSR) will articulate, and should they be asked what are the priority goals for security and compliance?
- Which percentage of PCI DSS controls across the control environment are truly and demonstrably effective and sustainable?
- How much success is truly achieved by design versus by luck?

Making the connection between stated goals and lack of compliance sustainability and effectiveness should be obvious. But for many organizations, it's not. It should not require a high degree of diagnostic skills to uncover the relationship. Organizations are unlikely to hit a target that they are not aiming for. It's very rare to encounter organizations that truly embed security control effectiveness and sustainability as an explicit goal to accomplish across their control environment. As we repeatedly mention in our publications, achieve success (high-quality outcomes that are predictable, consistent and repeatable) by design, not by luck.

Without specific goals, security and compliance departments are more likely to stagnate, struggle to obtain the investment they need and fail to achieve meaningful accomplishments.

CISOs and their security teams are understandably busy. The day-to-day operations always appear to be more pressing and are given higher priority than taking the time for proper introspection and foresight (Verizon covered this subject extensively in the 2020 PSR). The proper setting of data security and compliance goals provides a clear vision for teams and individuals involved in the control environment or that can influence its security—particularly for the teams within each of the 4 Lines of Assurance.



The Theory of Constraints and its relevance to payment security

The Theory of Constraints (TOC) is a proven process-management methodology that can help uncover and address the underlying root causes that prevent control environments from being effective and sustainable. It provides systematic steps to help identify the most important limiting factor or constraint that stands in the way of reaching a desired goal. It then focuses on ways to remove or improve that factor until it no longer acts as a constraint or obstacle to reaching the goal.

The TOC asserts that any manageable system is limited in its ability to achieve its goals due to the existence of a small number of constraints. It then seeks to improve those systems through a scientific approach. Eliyahu M. Goldratt, the creator and author of the TOC, describes it as "a process of ongoing improvement" and a thinking process that enables people to invent simple solutions to complex problems.[8]

Every complex system, including PCI security compliance and data security in general, consists of multiple linked activities. At least one of these linked activities can act as a constraint upon the entire system and at least one constraint always exists. In fact, the whole process itself can be the constraint. Other departments, and even senior management, can be considered the constraint. By identifying the constraint activity that can be considered the weakest link in the chain, the constraint can then be elevated or broken to the point where it's no longer the system's limiting factor. Some other part of the system or something external to the system will then become the limiting factor. This methodology can also be applied to PCI DSS compliance environments to break the constraints that prevent control environments from achieving the required level of effectiveness and sustainability.

Opening your window to the big picture

The TOC is a prioritization method, a way of looking at a complex system and identifying, challenging and correcting unexamined assumptions. The TOC helps you to closely evaluate each step and process within the context of the entire line, process or organization. This holistic perspective is a key part of the TOC because it views organizations as a chain of departments and functions.

Organizations have a lot of moving parts. The TOC identifies how you can make the biggest impact and the most difference to what you are trying to achieve – without spending a lot of money. There are several tools unique to the TOC that provide structure and consistency in problem recognition and problem solving, and help maintain focus on the organization's goals.

The TOC provides a structure for continuing improvements where they can have the most impact. The holistic view and continuous search for constraints gives you better control over your process, and it exposes additional capacity – often without the need for further investment. In other words, the TOC forces you to use what you already have instead of immediately spending money on new equipment or more resources. This is exactly the solution that many organizations need to improve their PCI security compliance capability. (The 2022 PSR delves into how to effectively apply the TOC to security programs.)

[8] Eliyahu M. Goldratt, "What is this thing called Theory of Constraints and how should it be implemented?" The North River Press, 1999.

The TOC presents a better way to find answers to these basic questions:

- Why change? (What is the goal?)
- What should change? (Where is the problem and what is the root cause?)
- What should it change to? (What is the solution?)
- How can we effect the change? (How can it be implemented?)

It provides a powerful approach to help you:

- Clarify your goals and their requirements, and gain clarity of the objectives
- Determine the critical success factors branching out underneath the goals (three to five for each goal)
- Outline the variable and conditions needed for the system to achieve the goals
- Identify the necessary conditions for each critical success factor[9]

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. This will become increasingly important for organizations opting to follow the custom control design and validation approach.

[9] H. William Dettmer, “The Logical Thinking Process: A Systems Approach to Complex Problem Solving,” American Society for Quality Press, 2007.

PCI DSS v4.0 navigational points

1. Do not delay.

Organizations should not delay preparations to meet the requirements of PCI DSS v4.0 simply because the new PCI Standard hasn't taken effect. 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 are not, following the defined approach for each requirement applicable to your cardholder data environment (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 DSS. The biggest impact is within changes to 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 requires 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.) Custom controls, as with traditional defined controls, need to show consistent operating effectiveness over long periods of time to meet the control objective and intent without interruption.

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 the environment they operate in. And documented evidence should be maintained to substantiate that it meets the intent of the relevant security objective(s). Customization requires a structured and detailed documented approach. 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: validating and approving controls.

6. Use control design and management templates.

The importance of assessing control effectiveness during regular assessments 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 when opting to implement a customized control approach. (See further details at “The necessity and value of control design templates” on page 16.)

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 custom control designs could be delayed.

8. Prepare for ongoing assessments.

Define the requirements and constraints for your security team to support the design, implementation and maintenance of ongoing assessments. This requires capacity planning and commitment for teams to support this process, to frequently evaluate, document and report on the control status of the environment throughout the year. The internal recording of PCI DSS evidence of compliance should be an ongoing business-as-usual activity.

The necessity and value of control design templates

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

In general, a PCI DSS control profile document should be prepared for each control system and typically include the following 12 items:

1. **Control objective:**
   Defines the applicable control objective(s) of the control or control system

2. **Control owner:**
   Assigns ownership and responsibilities

3. **Control function:**
   Describes the control function, such as management, procedural or technical

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

5. **Architecture:**
   Defines the control architecture, such as system-specific, common or hybrid

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 control test procedures and standards

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

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

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

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

12. **Governance:**
    References related policies, standards, frameworks and regulations[1.0]

[10] Payment Security Report, Verizon, 2018, page 12, for more details on documenting control profiles. https://enterprise.verizon.com/resources/reports/2018/2018_payment_security_report_en_xg.pdf

Maintaining control design profiles can have a 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 these 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 specification of the design profiles, the tighter 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 require 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 of the team or person tasked with its implementation, not the actual measurement of control strength and sustainability requirements.

Gaps typically exist in areas of control dependency. 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 refinement. 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.

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

Visit verizon.com/paymentsecurityreport for a collection of Payment Security Report resources.

About Verizon Cyber Security Consulting

This white paper is a product of Verizon Cyber Security Consulting, a global leader in the Payment Card Industry 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 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 cyber threats while ensuring compliance with applicable regulations and standards.

2021 Verizon Cyber Security Consulting PSR
PCI DSS v4.0 insights

Published November 4, 2021

Editorial team:

Lead author
Ciske van Oosten

Coauthor
Cynthia B. Hanson

Lead editor
Cynthia B. Hanson

Contributors
Abdelkrim Aoued Ahmed Bacha, Claire Lavelle, John Galt, Michelle Wire, Mikhail Banguerski, Sean Sweeney

Payment security consulting practice:

Managing director, security Verizon Cyber Security Consulting
Kristof Philipsen

Global lead
Sam Junkin

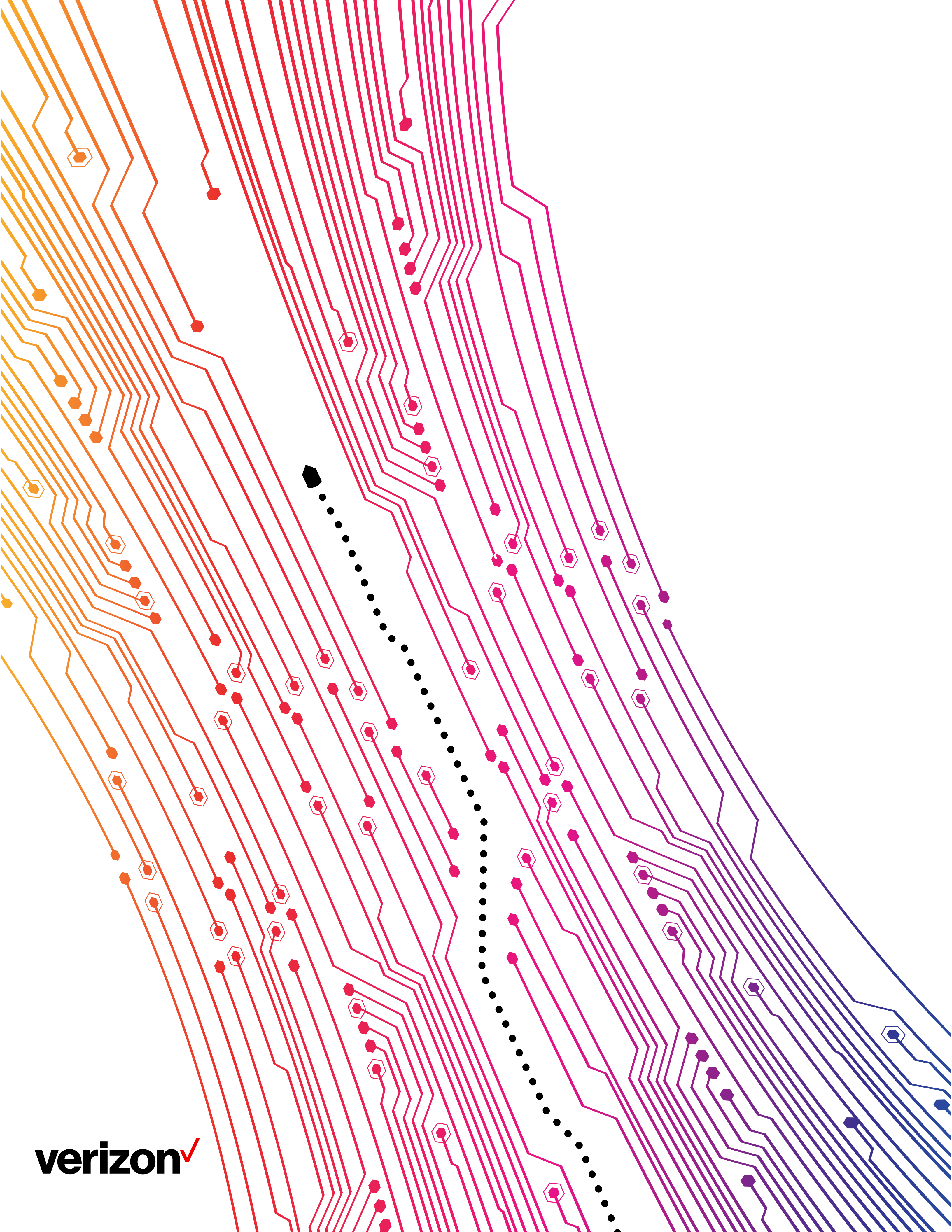
Americas region
Matthew Arntsen

APAC region
Ferdinand Delos Santos

EMEA region
Loic Breat

Global intelligence
Ciske van Oosten

Team email
paymentsecurity@verizon.com



verizon✓