protiviti®
Global Business Consulting

Best Practices for Building a Sustainable PCI DSS Compliance Program

Creating and maintaining a sustainable PCI DSS compliance program is a crucial and complex task for organisations to protect payment card transactions and uphold consumer trust. However, despite the PCI DSS standard being around for almost 20 years, many organisations still struggle to achieve and validate compliance with it.

In April 2016, the PCI Security Standards Council (SSC) introduced the Designated Entities Supplemental Validation (DESV) framework, which provides guidance for maintaining consistent PCI compliance, particularly for higher-risk entities. In our work with clients, we have utilised this framework and expanded on it based on our own experiences and lessons learned over the years. In this summary, we offer key best practices to enhance the maturity of your PCI program.

Program Foundation and Governance

- **Ownership and charter:** A successful program begins with well-defined governance structure, a charter, policies and procedures, roles and responsibilities, clear ownership, and executive support. The team best equipped to own and lead PCI compliance most effectively is the information security department, led by the chief information security officer (CISO). In organisations without a CISO, alternative executive sponsorship should be provided.
- **Payment-acceptance policy:** This policy will define acceptable payment channels and technologies for processing payments and will allow business units to introduce new transaction types while leveraging preapproved solutions and processes that maintain PCI compliance. Standardisation will also facilitate faster implementation of new payment channels and enable the organisation to benefit from common technology components and best practices.
- **Organisational independence:** The PCI compliance program consists of two parts: maintaining compliance and validating compliance. The first part involves managing the scope and ensuring that all requirements are met. The second part focuses on verifying the effectiveness of the activities performed in the first part. It is crucial that the personnel responsible for these parts are organisationally independent.

- **Reporting and performance management:** Transparency is key for support of leadership, proactive identification of potential issues and continuous improvement. Below are examples of metrics that some large organisations have used:
    - Number of confirmed instances of discovered cardholder data per business unit per quarter
    - Consecutive failures of PCI validation reviews per business unit
    - Repeated failures of the same control throughout the year
- Number of initiatives, new vendors or changes that have gone through PCI impact evaluation
    - Time to remediate control failure
    - Percentage of employees who have completed required training

Scope Management

- **Controlling unintentional scope changes:** New business initiatives or changes to an existing process that have not been analysed for PCI compliance may not only expand the cardholder data environment but also increase the number of applicable requirements that needs to be validated. In addition to the previously mentioned payment-acceptance policy, it is important to include checks for PCI compliance impact in change control, project management, legal and contracting, vendor management, application development, mergers and acquisitions, and any other processes that could affect the cardholder data environment and processes involving payment card data.
- **Periodic scope validations:** To provide additional assurance that the scope remains unchanged and that there are no unexpected repositories or transmissions of cardholder data, data loss prevention (DLP) technology can be used as a detective control. Although PCI DSS 4.0 does not specifically require it, this functionality will help meet its requirement 12.5.2. By combining preventative and detective controls in PCI scope maintenance, a reliable and defensible methodology can be established to prevent unintentional changes to the scope and ensure its consistency at the time of validation.

Maintenance of Compliance

- **Checklist of PCI activities:** To ensure consistent execution of controls and a smoother compliance-validation process, a comprehensive checklist of PCI activities should identify tasks to be performed on daily, weekly, monthly, etc., allowing for proper planning and ensuring that time-sensitive controls are not overlooked. It should also identify the parties responsible for executing these tasks and specify the evidence to be produced to support compliance validation.
- **Quarterly compliance reviews:** Quarterly internal reviews of PCI compliance are not only a good practice but also a requirement for service providers in PCI DSS 4.0. Conducting

these reviews allows for early identification of problem areas, giving organisations the opportunity to make necessary adjustments. To meet the requirement, an independent party must perform the reviews. Internal audit can be a valuable resource for conducting these reviews, provided they have the necessary expertise.

- **Service-provider management:** Organisations using many service providers often overlook obtaining updated attestations of compliance (AOC). They should therefore leverage an existing vendor-management system or establish a database of PCI service providers with automated requests to respective service providers for an updated AOC prior to their revalidation due date. The responsible personnel should review the AOCs to ensure that the validation scope has not changed and the contracted services are still covered. Maintaining PCI-compliance records of service providers is not a substitute for proper third-party risk management practices, such as risk ranking and security evaluations of vendors, but it is a necessary component to maintain PCI compliance.
- **Vulnerability management:** In large organisations, the responsibility for remediating vulnerabilities is assigned to system owners, while the centralised vulnerability-management team identifies risks and communicates them to the system owners along with recommendations for remediation. This structure creates coordination challenges that can hinder the timely implementation of patches and rescanning systems to validate remediation.

  Organisations should establish an automated process of conducting vulnerability scans on a continuous basis — for example, weekly — to provide ongoing confirmation of remediation and vulnerability scanning after significant changes without the need for additional coordination. They should also make vulnerability-scan reports accessible to stakeholders through a self-service portal to eliminate unnecessary communication cycles.

Assessment Technology and Automation

- **Compliance-validation portal:** Organisations should implement a portal for management of compliance-validation activities. This portal would be a central point for collecting evidence, an assessment dashboard and a status-communication tool, and the application where the results of control testing are documented. The documentation for PCI compliance validation (ROC/SAQ/AOC) should be generated from this portal based on the information entered. Using the portal for conducting PCI assessments also allows for the generation of valuable reports on the performance of compliance assessments, which can drive continuous process improvement. Some organisations have utilised existing GRC tools as PCI-assessment portals.
- **Automated evidence collection:** Assessing the configuration settings of systems in scope can be a time-consuming task. Enterprises should develop scripts to capture and report audit logging settings, user accounts, time settings, patching status, password settings and other configuration-hardening settings and load them into prebuilt parsers for more efficient automated evaluation. Alternatively, organisations should load configuration-hardening

standards into vulnerability-scanning tools, like those from Qualys, Rapid7 or Tenable, and leverage their configuration-evaluation capability to test adherence against standards.

Similar automation should be used to meet controls related to identity and access management (IAM), such as ensuring the disabling or removal of accounts for terminated employees and the deactivation of inactive accounts. Companies that use IAM platforms like SailPoint or Okta may be able to leverage existing reports and access review processes used for compliance with other regulations for PCI DSS.

Training and Communications

To ensure a successful PCI compliance program, it is imperative to provide effective training that educates personnel not only on the security of cardholder data and required controls but also on their specific roles and responsibilities within the program. Therefore, training should extend beyond general PCI awareness and be tailored to the different types of stakeholders involved.

- **Executive-leadership education:** Executives should be educated on the risks associated with noncompliance with PCI DSS, and the importance of controlling the scope of the cardholder-data environment. For organisations with a "no storage/no transmission of cardholder data" policy, the training must explain how cardholder data can still be introduced into the environment because of incomplete analysis of new processes, applications or acquisition targets.

  The scope expansion not only can increase the number of components subject to PCI compliance but also expands the set of PCI requirements that must be met. Management should also be educated on the consequences of noncompliance with PCI, which include legal, financial and reputational risks for the organisation, as well as on the responsibilities of executive leadership within the program.

- **PCI education for personnel responsible for maintenance of PCI compliance:** These personnel must be educated on the importance of maintaining adequate evidence of controls and processes for compliance validation, as well as provided detailed explanation of the scope of the cardholder-data environment and ongoing activities required to maintain compliance. The training should also emphasise the benefits of taking a proactive approach to PCI compliance and the implications of noncompliance, and how to analyse the impact of environment changes and service provider relationships and what resources are available to assist in these efforts.

- **PCI education for personnel working with payment terminals:** In addition to training on how to maintain the inventory of payment terminals, how to inspect them, how to handle suspicious behavior around payment terminals and what to do in case of replacements or malfunctions, personnel responsible for payment terminals need to understand their overall responsibility for the security of cardholder data and the procedures for reporting suspected compromises.

Final thoughts

In summary, a sustainable PCI DSS compliance program requires a strong governance structure, specialized training, effective scope management, robust compliance maintenance and verification practices, and tools and processes for efficient handling of PCI compliance tasks and continuous improvement. All these components form an ecosystem designed to protect cardholder data consistently while adjusting to evolving threats, technology advancements, and changes in business priorities and objectives.

Protiviti professionals can assist organisations at various stages of their PCI compliance journey, offering expertise in building programs from scratch or enhancing existing ones.

For additional information, examples and insights, visit Protiviti's Data Protection web page. Protiviti is not a law firm, and nothing within this paper should be relied on for legal purposes. Clients should always seek legal advice from inside or outside counsel.

Contacts

Chip Wolford
Managing Director
chip.wolford@protiviti.com

Daniel Baron
Senior Director
daniel.baron@protiviti.com