How to proactively manage PCI compliance with Zscaler

zscaler™

Abstract

The Payment Card Industry Security Standards Council (PCI SSC) created the Payment Card Industry Data Security Standard (PCI DSS) to protect customer payment data and provide clear security standards to companies that process this data. Although PCI DSS has been around for nearly three decades and most companies strive for compliance, achieving and maintaining compliance is complicated, fraught with complexity and compromise, and can be very expensive. Standard compliance must be verified on a yearly basis—either through self-reporting or by an authorized third party. Recent revisions to the standard make understanding customer payment data security and security device management even more complicated.

With more companies adopting digital transformation and blurring the borders of the enterprise network, maintaining PCI DSS compliance has become increasingly complex. Expanded network perimeters make protecting user payment data harder. The systems that process, transport, and store this data and encapsulate customer information dataflows are more greatly distributed across a wider swath of the internet. This white paper discusses how Zscaler Zero-Trust security platforms help companies secure customer payment data and actively maintain PCI DSS compliance.

Disclaimer: This white paper has been created by Zscaler for informational purposes only and is designed to try and help organizations understand PCI compliance in connection with Zscaler's services and products. Therefore, it should not be relied upon as legal advice or to determine how the contents might apply to you or your organization. We encourage you to consult with your own legal advisor with respect to how the contents of this white paper may apply specifically to your organization, including your unique obligations under applicable law and regulations. ZSCALER MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Zscaler product. You may copy and use this white paper for your internal, reference purposes only.

Defining PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS)[1] was created by the Payment Card Industry Security Standards Council (PCI SSC) to formalize methods of cardholder data protection for enterprises using such data as part of their business operations. This standard requires businesses to comply with strict security policies and recommends best practices for maintaining customer data integrity. It also provides a framework for inspecting and reviewing enterprise practices around use of cardholder data that is assessed on a yearly basis.

Any organization that stores, processes, or transmits cardholder data is subject to the PCI DSS. This standard is reviewed and updated as needed by the PCI SSC. The latest version of the standard is v3.2.1, released May 2018. A new version of the standard (v4.0) is anticipated.

The new version of the PCI DSS is largely expected to remain the same, but will include enhanced requirements for authentication and encryption. It is also expected to emphasize security as a process, rather than simply a yearly certification goal. The new standard will give companies more flexibility by focusing on the results of the cybersecurity requirements rather than on the specific implementation details.

A FAQ regarding the latest version of the PCI DSS can be found at the PCI SSC website[2].

Why a standard?

The increase of enterprise and customer engagement via the internet created an obvious need for strict security controls over the credit card data used in those transactions. Cybercriminals began hacking into payment processing systems and stealing customer payment data as more businesses offered customers goods and services online.

The first PCI DSS document went public in 2001. Even with the release of these standards, there has been a steady increase in the amount and severity of customer data breaches. In fact, over 10 billion customer payment records have been breached since January 2005.*

The PCI SSC is made up of the five major payment brands (Visa, MasterCard, American Express, Discover, and JCB) and they strictly enforce adherence to the PCI DSS standard in order to guarantee cardholder security and privacy. The PCI DSS is an industry-wide effort to protect sensitive cardholder data and prevent cybercrime.

* PCI Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1", PCI Security Standards Council, (C) 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Systems under review

PCI DSS audits can be stressful for a company, and what is necessary to meet compliance requirements isn't always clear. This is because the scope of what the audit will investigate isn't always obvious. The best strategy for ensuring compliance is to limit, as much as possible, the scope of the audit. Zscaler can help companies achieve this aim.

[1] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1", PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

[2] "5 Questions About PCI DSS v4.0", PCI Security Standards Council, © 2020, https://blog.pcisecuritystandards.org/5-questions-about-pci-dss-v4-0

PCI DSS audits focus on the “cardholder data environment” (CDE). This classification describes any IT system that processes, transmits, and stores credit card information. “Credit card information” includes data stored on the card’s magnetic stripe, plus any data stored or replicated on the card’s data chip.

The CDE definition is both sticky and “greedy.” It includes the network and network devices that CDE systems connect to, and ANY other device resident on these same networks. To limit the scope of the CDE, most enterprises separate CDE machines from other systems with a security barrier—usually a firewall—that isolates the CDE system from other corporate systems. Note that in this model, the firewall is also considered part of the CDE.

Beyond the CDE, there is an “extended CDE.” The extended CDE includes tools that impact the security or management of the core CDE.

This extended CDE can complicate and broaden PCI DSS audit scope. Most audits define customer payment data “dataflows” to map the CDE and extended CDE. Dataflows are the logical and physical connections between the systems transporting or supporting the processing of cardholder data. The extended CDE also includes the people that can access the dataflows both logically and physically.

Reducing PCI compliance scope

PCI DSS compliance efforts can be time-consuming and expensive. Part of maintaining compliance is understanding and mapping the scope of a PCI network. According to the PCI DSS standard:

> The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.[3]

This definition of scope is high-level, even vague, and offers only a broad interpretation as to what exactly constitutes enterprise PCI compliance. The less-than-specific definition raises two key questions:

- **Do merchants and service providers have different responsibilities in a single system?** Yes. Merchants accept the payment from the cardholder and the service provider processes, stores, and/or transmits the cardholder data. Service providers are generally responsible for more oversight in terms of how data is processed, transmitted, and stored than merchants. You can limit the scope of an audit by separating the roles of merchant and service provider.

[3] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1”, PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

- **What systems that comprise the dataflow should be included in PCI compliance?** Ideally, all of the discrete systems that "touch" the dataflows should be included. For some enterprises, not defining the CDE scope widely enough results in gaps in account payment data as it travels through payment processing systems. Conversely, too broad of a definition can result in unnecessary compliance and assessment costs. Security tools, while part of the architecture of the CDE, aren't necessarily included as *part* of the CDE.

Since the expectation is that the PCI DSS scope *could* include the extended CDE, the assumption that all security tools *would* be included is understandable. But it's not that simple. Compliance complexity, CDE scope inconsistency, and management overhead costs are significant headaches. Security service providers like Zscaler help protect and segment the dataflow, but aren't part of the compliance audit. But by ensuring a clear set of dataflows, and understanding the tools, services, and security controls used to specifically support or protect the CDE, enterprises can use Zscaler to *reduce* CDE scope, and thereby reduce compliance overhead.

The important distinction is that a security tool, even if it is used to *enhance your PCI compliance posture*, is not necessarily part of the CDE scope. Although its configuration may be important to prove compliance, *the tool itself does not require compliance*.

Examples of security tools that would likely form part of the CDE and therefore be subject to compliance:

- **Encryption tools** used to protect data in transit from outside view
- **Endpoint protection** resident on devices used to access the CDE
- **Firewalls** connected to/protecting the CDE

Examples of security tools that could be captured as part of the extended CDE are:

- **Endpoint security management consoles** that manage the configuration of endpoint security software connected to and within the CDE
- **Firewall management suites** that manage the configuration of firewalls that protect or segment the CDE
- **DNS and other ancillary IT services** that manage the configuration of domain name service and any other IT services (such as SMTP) that affect the CDE

Other security tools and services that wouldn't be considered part of the CDE scope:

- **Code-scanning** for non-credit card application development
- **Non-CDE firewalls** (unless they provide internet access)
- **DDOS protections**, even if they protect credit card applications as they enhance availability rather than data security

Zscaler and compliance: No network means easier compliance (and no TPSP issues)

Once companies build a complete picture of the PCI DSS scope by documenting the dataflows, and have a clear understanding of the technologies supporting and managing the CDE, they can start reducing their PCI DSS scope.

The PCI DSS recognizes the network changes that enterprises adopt. The specification includes the concept of a third-party service provider (TPSP). A TPSP is any entity that is contracted to:

> . . . store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. It is imperative for any enterprise to reduce the scope of a PCI audit or assessment to as little IT and data as possible.[4]

The PCI DSS does not offer a comprehensive list of TPSPs, but in general, the category includes vendors who provide management of:

- Security tools (firewalls)
- Physical security (facilities and equipment access)
- Servers (within the CDE)
- Networks (within the CDE)

As a best practice, when a company cedes security control over services to a third party, then the TPSP should either:

- Maintain its own PCI DSS compliance, or
- Provide visibility into how the security platform maintains controls that support PCI compliance

[4] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1", PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

While it appears that Zscaler falls under the TPSP category by providing a cloud platform security service to our customers, in reality it doesn't. Zscaler does not manage a customer enterprise's security controls directly. Therefore, Zscaler plays no role in the way the platform is consumed and should not be considered a TPSP. Although the Zscaler platform is a cloud service, the control of the platform for an individual customer is retained either by a Managed Security Service Provider (MSSP) or by the customer itself. In the former instance, the MSSP acts as a PCI service provider.

Zscaler's comprehensive reporting and dynamic data traffic views foster security transparency. That means **Zscaler can help provide a robust response to an enterprise PCI audit** by clarifying and limiting an organization's use of credit card data to defined dataflows, and excluding card-processing from elements of the Zscaler platform's capabilities. This in turn can simplify card-processing dataflows and the compliance program, and reduce overall risk.

There are three primary means of reducing the scope of a PCI audit and its extensions. These are through:

- **Tokenization:** Substituting important data elements with an equivalent that is meaningless out of context and has no extrinsic or exploitable value

- **Encryption:** Encoding data or information so that only authorized entities can view or capture it, usually by decrypting it with a secure public/private key pair

- **Abstinence:** Completely separating systems from payment card data

While tokenizing cardholder data is a great way to ensure a system is outside the scope of the CDE, it is not pertinent to the discussion of Zscaler and PCI DSS.

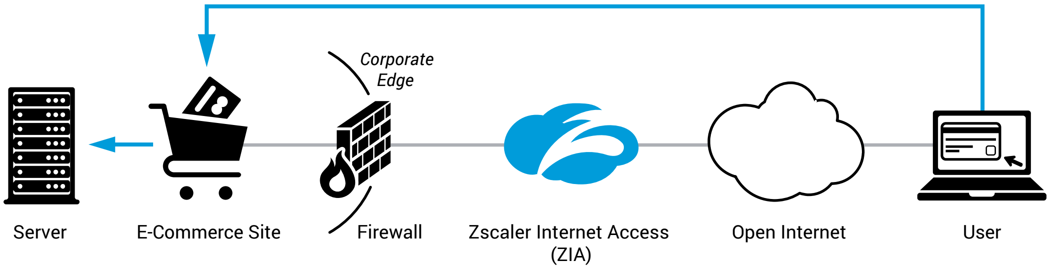
Zscaler uses a combination of encryption and abstinence to exclude systems from the CDE and the extended CDE. Zscaler customers should assess their CDE dataflows to ensure PCI compliance. Dataflows can be specific to an individual enterprise, and Zscaler services can secure elements of the extended CDE. However, with effective scope management on the part of the enterprise, Zscaler can support PCI compliance without qualifying as a TPSP.

There are many possible internet-bound dataflows possible within an organization. A number of these are highlighted below, some with Zscaler as a critical component.

1. CDE dataflows that don't include Zscaler

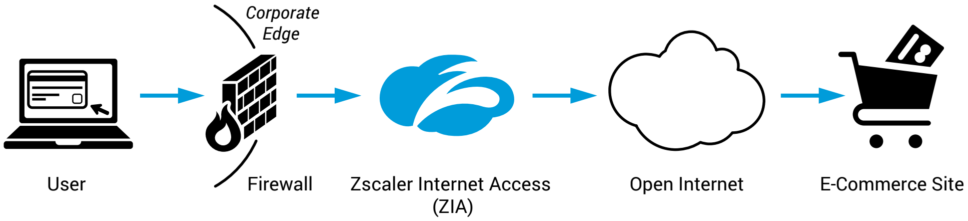
Customer inbound connections to public corporate e-commerce servers

Zscaler does not protect or otherwise provide transit functions for inbound connectivity from unknown internet users to a DMZ or internal device.



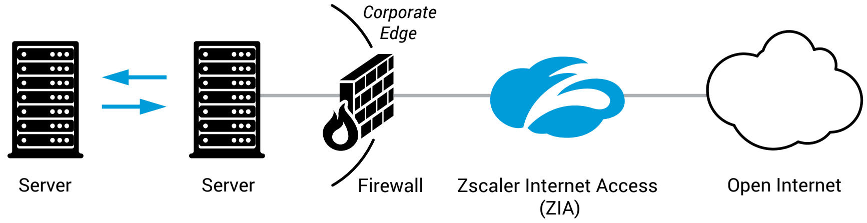
Enterprise employee using personal credit card to make purchases from a third party

Although in this case traffic transits Zscaler, it is not actually a dataflow governed by the employee's company PCI scope. It instead falls under the scope of the e-commerce site from which the employee is purchasing goods or services.



Host-to-host connections within the corporate network processing card data

Zscaler is not a transit stop for this activity, as Zscaler only intercepts and inspects internet-bound traffic.



2. CDE dataflows where Zscaler can be removed from the scope

Dataflow + Description

PCI DSS scope reduction best practice

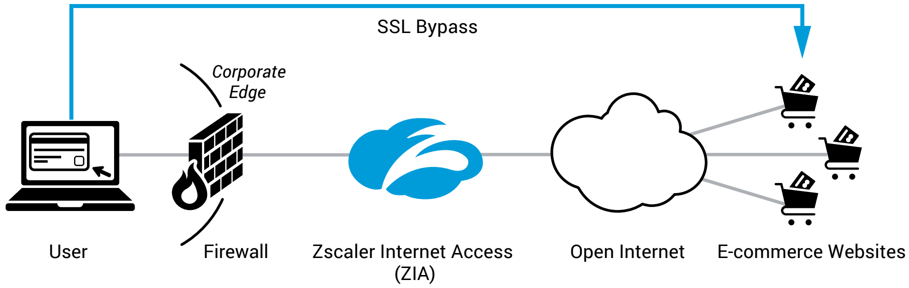
Enterprise employee uses enterprise customer credit card data for purchases from a third party

The dataflow travels via Zscaler Internet Access (ZIA), and is partly within the PCI scope of the payment service or e-commerce site where services are bought. But if the card details are held, and used, by the employee company as well, then it also falls under that company's PCI DSS scope.

Abstinence

Employ Zscaler's SSL Bypass feature for sites used to conduct payment operations.

In this example, Zscaler never has visibility to decrypted cardholder data, and can be treated like any other "public network," which requires sufficient encryption to transmit card data.

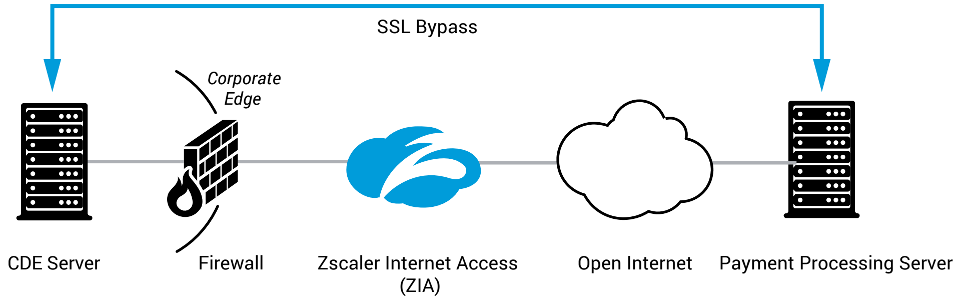


Direct internet communication from CDE servers

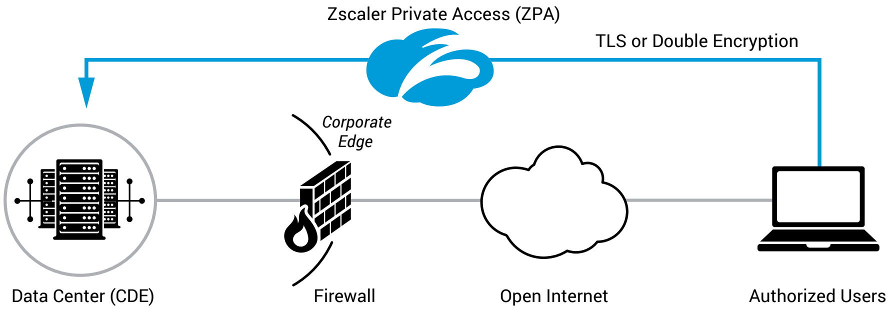
ZIA is not the company's external firewall, but ZIA by default may still have access to this communication. Although the standard suggests avoiding direct internet connections from CDE servers, it is possible that this is a valid dataflow.

Encryption, Abstinence

The PCI standard already demands that any internet connectivity be strictly documented and limited to the absolute minimum required for the service, so general web browsing is already forbidden. Exclude Zscaler from the dataflow: ensure that CDE dataflows sent over the internet are excluded from SSL inspection using the bypass function.



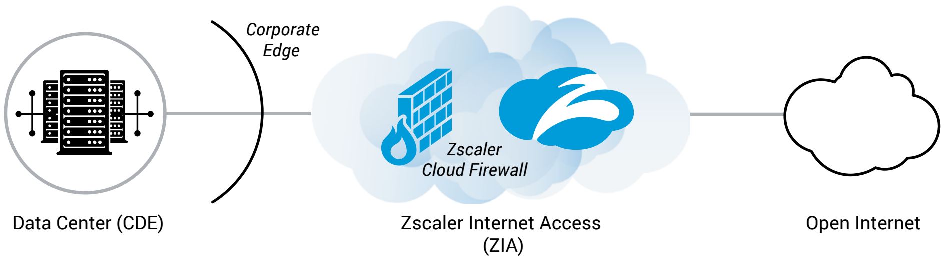
Dataflow + Description	PCI DSS scope reduction best practice
Authorized user access to the CDE Zscaler Private Access (ZPA) provides secure access to CDE hosts.	**Encryption, Abstinence** Ensure that a second layer of encryption is in place in the technology used. If an application is encrypted from client to server, ZPA can connect with no access to the data inside this additional encryption layer. ZPA would therefore be considered a "public network." Additionally, if no encryption is available, use ZPA "double encryption" and the business can use their own keys to render the session invisible to Zscaler. Again, ZPA can be treated as a public network. As a bonus, ZPA's powerful application connectivity and coordination with identity management could be considered an additional compensating control if the application authentication is not adequate (as defined in PCI DSS v3.2.1 sections 12.3.2)[5].



[5] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1", PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

3. CDE dataflow where Zscaler configurations are part of the scope

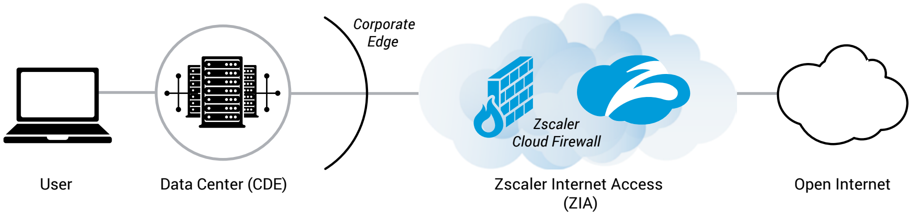
Dataflow + Description	PCI DSS scope reduction best practice
Direct internet communication from CDE servers ZIA Cloud Firewall is the company's external firewall, limiting or controlling connectivity from the CDE hosts to destinations on the internet.	**Part of PCI Scope** Like ZPA above, when the portal is managed by the Zscaler end user it can be validated as the control mandated by the standard itself, and would form part of a PCI audit (as defined in [PCI DSS v3.2.1 sections 1.2.1, 1.3.4, and 1.3.7](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf)).[6]



[6] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1", PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

4. Extended CDE dataflows that include Zscaler as part of the PCI scope, but not part of the dataflow

Dataflow + Description	PCI DSS scope reduction best practice
Authorized user access to the CDE ZIA protects mobile devices used to access the CDE.	**Part of PCI Scope** This again, like endpoint security, forms part of a PCI audit. It enhances the company's ability to protect endpoints from malware (as covered in PCI DSS v3.2.1 section 5)[7].



[7] "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures version 3.2.1", PCI Security Standards Council, © 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

5. Zscaler detects inappropriate use of credit-card data

Dataflow + Description

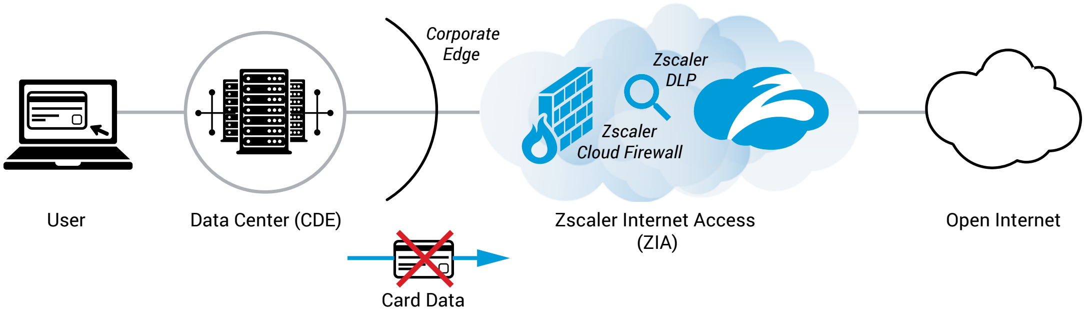
Zscaler prevents data from leaving the CDE

ZIA ensures that employees are not storing credit card data on SaaS or other inappropriate platforms using ZIA DLP functionality.

PCI DSS scope reduction best practice

Exception

Even though Zscaler DLP and other security features may identify and “process” credit card data, this should be an exception and evidence of a failure on the part of employees or the company, and would not form part of a PCI dataflow.



Moving from reactive to proactive compliance

Enterprises that process customer payment data must secure it from theft and exploitation by bad actors. The PCI DSS was created to provide guidance on how to achieve this goal. The PCI DSS is an established security standard that evolves to meet new technologies, architectures, and threats. As such, the yearly assessment is meant to help companies achieve a secure level of protection for their customers' information as it transits within the enterprise's span of control.

Compliance does not necessarily mean secure, however, and many companies gain a false sense of security by equating a PCI audit with a proper security stance. The goal for enterprises should be proactively establishing and maintaining a secure, PCI-compliant culture throughout the year—not just reactively making their environment eligible to pass the audit.

Focusing solely on passing compliance audits can engender complacency, increase the risk of poor security between assessments, and risk a security breach with severe consequences. For the sake of continuous improvement, enterprises that deal with credit-card data should work to establish an ongoing review process for all security controls in order to promote a continual, dynamic compliance state.

The PCI SSC document Best Practices for Maintaining PCI DSS Compliance[8] recommends ten principles of maintaining compliance:

1. **Develop and maintain a sustainable compliance program:** Make compliance "business-as-usual," and the ongoing protection of cardholder data as the goal.
2. **Develop program, policy, and procedures:** Drive proper behavior and to maintain repeatable business and operational processes.
3. **Define performance metrics to measure success:** Carefully define information-security measurement based on specific needs, objectives, operating environments, risk priorities, and compliance program maturity.
4. **Assign ownership for coordinating security activities:** Assign a specific management-level individual responsibility for continuous compliance.

[8] "Best Practices for Maintaining PCI DSS Compliance", PCI Security Standards Council, © 2019, https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

5. **Emphasize security and risk management to attain and maintain compliance:** Build a culture of security and protecting an organization's information assets and IT infrastructure, allowing compliance to be achieved as a consequence.

6. **Continuously monitor controls:** Continuously monitor, test, and document the implementation, effectiveness, efficiency, impact, and status of controls and activities.

7. **Detect and respond to control failures:** Recognize and respond to security-control failures promptly.

8. **Maintain security awareness:** Implement a formal security awareness process with content that is up to date with the latest trends in breaches.

9. **Monitoring compliance of third-party service providers:** Develop and implement processes to monitor the compliance status of its service providers to determine whether a change in status requires a change in the relationship.

10. **Evolve the compliance program to address changes:** Evolve controls to meet developments in the threat landscape, changes in organizational structure, new business initiatives, and changes in business processes and technologies so that changes do not negatively impact the organization's security posture.

These are ambitious goals, especially in large companies where corporate and business networks have grown beyond traditional networking architectures. Maintaining continual compliance is especially difficult in castle-and-moat security environments, where the complexity of managing separate policies and security requirements for both inbound and outbound hardware security stacks complicates PCI DSS compliance efforts. Add to that PCI complexity branch internet breakouts, expanding cloud services, and growing numbers of remote users.

Zscaler's services were born in and designed for the cloud: highly-distributed, inline, and (with more than 150 data centers around the world) geographically close to every user. This service model improves visibility and management for PCI compliance. It puts all monitoring and logging data in one place with instant, global correlation. Zscaler provides full session-by-session logging and storage and SLA-backed storage of blocked traffic for six-months.

IT security teams are used to struggling with patchworked, cobbled-together "reports" containing thousands of lines of numbers and codes. Such reports deliver questionable practical value. By contrast, Zscaler consolidates security data in its dynamic dashboards, with deeper analytics and details on demand.

Zscaler's cloud-first approach provides security visibility and speeds incident response with user authentication and easy audit-trail tracking. Rule changes are made once and immediately enforced everywhere.

Comprehensively transparent: Zscaler’s data security visibility

Zscaler provides real-time visibility into applications, users, and threats across all locations. Customized transaction logs can be streamed from Zscaler to a SIEM with the Nanolog™ Streaming Service (NSS). These provide insights that help visualize dataflows, detect and respond to threats, and gain additional visibility into payment-processing networks. IT teams can activate new services, define and immediately enforce policies, and manage all branch locations from a single, centralized, cloud-based console. This makes it easier to enforce compliance for all the systems involved in the processing of a dataflow.

As Zscaler detects threats and attacks, it updates and protects an affected machine, as well as immediately replicates countermeasures to the Zscaler cloud. This guarantees immediate security for the entire organization, and every Zscaler enterprise, not just one machine or branch office.

For auditors and compliance officers, Zscaler makes it easy to show what types of threats and attacks are attempting to hit a company on a daily basis. This enables informed security policy management at the highest levels.

Comprehensively reported: Zscaler’s system audits

Zscaler’s System Audit Report highlights the status of all areas of a company’s security: GRE tunnels, PAC files, authentication frequency, PAC file sizes, Office 365 One-Click, and IP visibility. If there are any present issues, the report makes recommendations on how to fix them.

This audit tracks how crucial payment information dataflows are traveling the network, and if there are gaps in the security protecting the dataflow.

Comprehensively dynamic: Zscaler dashboards

The Zscaler platform provides both standard and customizable dashboards with real-time visibility into an organization’s internet traffic. Multiple dashboards provide different views, so enterprises can track internet usage and quickly take action in response to anomalous trends or security threats. Each dashboard contains widgets that present data in interactive charts.

Comprehensively compliant: Zscaler helps maintain PCI DSS compliance

PCI DSS compliance is imperative to any company that processes customer payment data. In order to comply, companies must establish processes that secure payment dataflows and clearly document the systems and machines that this data traverses.

The drive for PCI compliance can be a daunting process. Zscaler helps reduce overall security risk and fosters enterprise compliance success. Zscaler plays an important role in protecting data and reducing the risk of loss of cardholder data.

Zscaler can narrow PCI DSS audit scope by clarifying an organization's use of credit card data, controlling dataflow exposure, and excluding card-processing from elements of the Zscaler platform's capabilities. This, in turn, can simplify card-processing dataflows and the compliance program, and reduce overall risk.

Zscaler's visibility and monitoring capabilities can provide companies and PCI auditors with concrete information about dataflow security across an entire CDE, and make sure that security updates or changes are propagated to all devices in a system. This centralizes control of the security platform and allows cloud-based enterprises a simple way to manage dataflow security across the entire CDE.

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.