

PCI DSS

Compliance Guide



Index

What is PCI DSS?	1
Who must comply with PCI DSS?	2
Consequences of PCI DSS non-compliance	2
PCI DSS requirements for compliance	3
PCI DSS roadmap	4
1. Identify the PCI level that is applicable to the organization	4
2. Map the flow of sensitive data in networks and systems within the organization	5
3. Complete the Self Assessment Questionnaire (SAQ)	5
4. Submit the Attestation of Compliance (AOC)	5
5. Conduct a vulnerability scan	5
6. Submit all necessary documentation	5
PCI DSS best practices: A checklist	6
PCI DSS: Key controls to consider	6
Comply with PCI DSS using EventLog Analyzer	8

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to protect payment card account data and enhance the security of payment transactions globally. In the 1950s when the first modern charge cards were introduced, security policies were managed by the individual organizations and there was no cohesive security practices.

It wasn't until 2006, when the Payment Card Industry Security Standards Council (PCI SSC) was founded by the major payment brands, including American Express, Discover Financial Services, JCB International, MasterCard, and Visa, that unified security standards were developed. Today, more than 700 member organizations support financial transactions in more than 60 countries. The council's main objective is to ensure adherence and boost understanding of these security principles.

By following PCI compliance, organizations are also protecting their businesses from fraudulent activities such as:

- Unauthorized access to their systems through weak passwords.
- Old, unpatched software that could be exploited.
- Embedded malicious software in the network.
- Unauthorized acquisition of data through remote network access for the execution of fraudulent deals.

To keep pace with evolving cyberthreats, PCI SSC periodically updates its PCI DSS guidelines.

[PCI DSS v4](#) is the latest version of the framework. It replaces the PCI DSS v3.2.1 which was published in 2018.

Who must comply with PCI DSS?

Organizations that handle credit card information are required to follow the PCI DSS compliance guidelines. This includes credit acquirers, payment service providers, merchants, banks, and third-party service providers.

Whether the business is small or large, if it takes credit card payments via a website, in person, or over the phone, it needs to abide by the rules. Any business that accepts credit cards such as Visa, Mastercard, American Express, or any other, must be compliant with PCI DSS.

This helps organizations protect against malicious acts that could result in a leak of customer data. By adhering to these regulations, businesses can ensure the security of sensitive payment information.

Consequences of PCI DSS non-compliance

The PCI DSS provides guidelines for securing sensitive information, but compliance with these guidelines is not a legal requirement. The regulations are managed and upheld internally by the industry through vendor agreements. Adherence to the 12 requirements set forth by PCI DSS will save organizations from a range of consequences, including fines from \$5,000 to \$100,000 and the possibility of legal action, insurance claims, canceled accounts, and the withdrawal of credit processing services if a security incident occurs.

The damage from compromised data can be widespread and long-lasting, impacting consumers, merchants, and financial institutions alike and potentially causing irreparable harm to a company's reputation and future success.

The aftermath of a breach might also involve the following costs:

- In-person evaluation by a qualified security assessor
- Detailed forensic investigation
- Reissuing credit and debit cards
- Free credit monitoring for impacted customers
- Technology repairs and upgrades
- Notifying the public about the breach

PCI DSS requirements for compliance

Entities that handle cardholder data or sensitive authentication data must adhere to the guidelines set forth by PCI DSS. In March 2022, PCI SSC updated its standard with the release of version 4. Nevertheless, to ensure a gradual shift, version 3.2.1 remains in effect until 2024. During this period, organizations can choose to comply with either of the two versions.

PCI DSS is a set of 12 security requirements that are divided into six categories. These requirements may be relevant to your business, depending on the type of business you run. To be compliant with PCI data security standards, you must follow three key steps:

- Securely collecting and transmitting consumer data and credit card information.
- Storing data securely using methods like encryption, in accordance with the 12 security domains of the PCI standard.
- Validating security processes annually using an approved auditing method.

The following are the 12 core requirements of the PCI DSS categorized into six goals that are key to ensuring its effectiveness.

GOALS

01

Build and maintain a secure network and systems

1. Install and maintain network security controls.
2. Apply secure configurations to all system components.

02

Protect account data

3. Protect stored account data.
4. Protect cardholder data with strong cryptography during transmission over open, public networks.

03

Maintain a vulnerability management program

5. Protect all systems and networks from malicious software.
6. Develop and maintain secure systems and software.

04

Implement strong access control measures

7. Restrict access to cardholder data to those who require it to perform their job responsibilities.
8. Identify users and authenticate access to system components.
9. Restrict physical access to cardholder data.

05

Regularly monitor and test networks

10. Log and monitor all access to system components and cardholder data.
11. Test the security of systems and networks regularly.

06

Maintain an information security policy

12. Support information security with organizational policies and programs.

To ensure compliance with PCI DSS, it is crucial that contracts with third-parties specify their obligation to adhere to the standards. If a third-party is unable to provide proof of compliance, their systems and processes need to be assessed as a part of the annual compliance review of the organization.

Third-parties encompass:

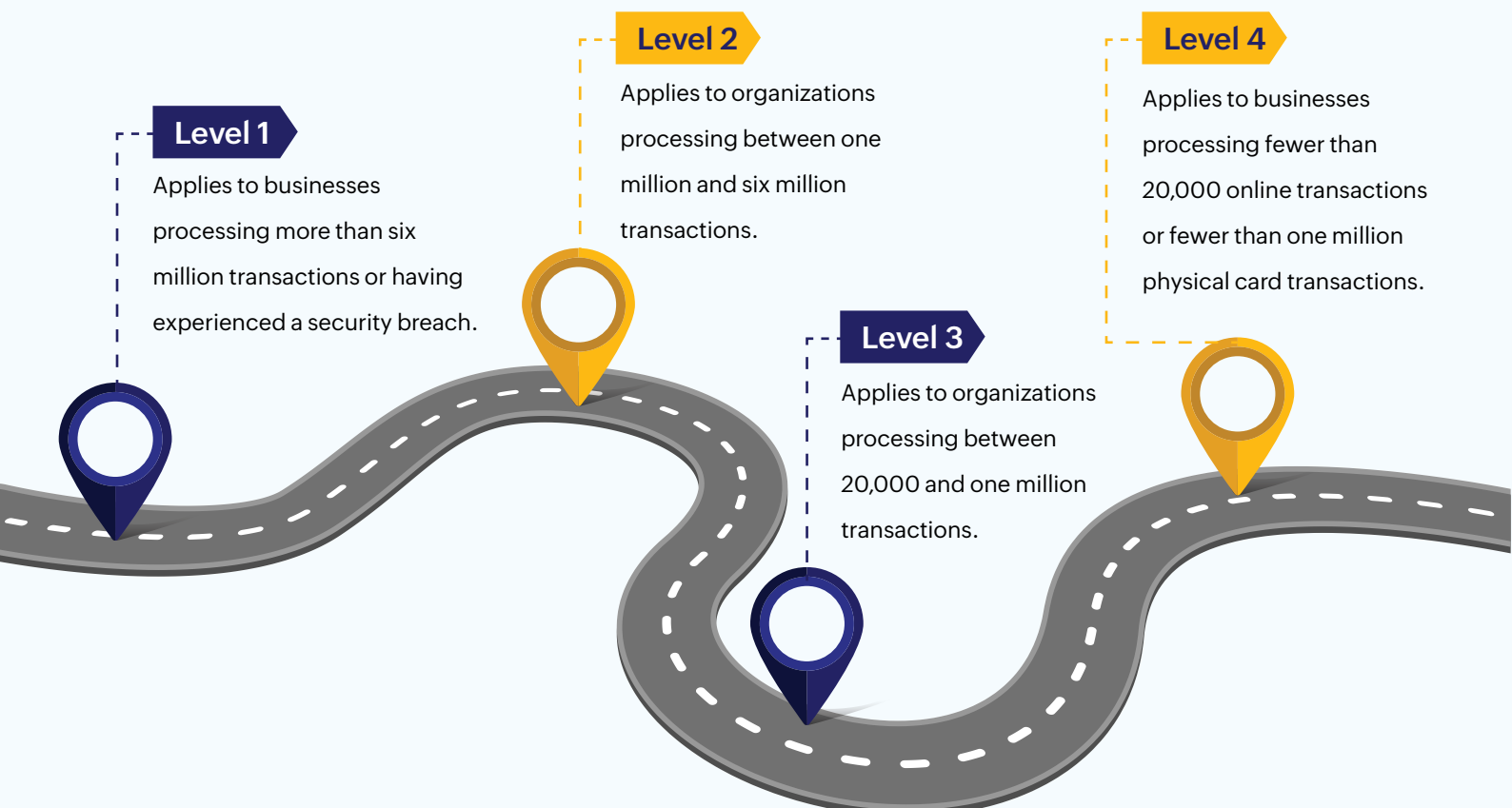
- Software solution providers
- Payment solution providers
- Web hosting services
- Electronic point of sale solutions
- Cash register suppliers

PCI DSS roadmap

Achieving PCI DSS compliance can be approached as a six-step process.

1. Identify the PCI level that is applicable to the organization

The PCI DSS compliance process is based on the number of annual transactions a business processes, with slight variations depending on the credit card company. Once the number of annual transactions of the organization is determined, it can be compared to the requirements set by the credit card companies to find the PCI level applicable. The four levels of compliance are as follows:



2. Map the flow of sensitive data in networks and systems within the organization

To ensure cardholder data is collected and stored securely, it is essential to trace the flow of the data through the organization's network and systems with the help of the IT department. This includes all storage systems, platforms, and networks where the data is either stored or transmitted.

To create a comprehensive map of your systems, follow these steps:

1. Identify customer-facing areas of the business.
2. Record how data is handled at each transaction point.
3. Record which systems the data passes through and where it is stored.

Keeping a record of every network, system, and data center helps secure every step of the payment process and ensures the organization remains PCI DDS compliant.

3. Complete the Self Assessment Questionnaire (SAQ)

The SAQ is a crucial tool for determining if an organization complies with the 12 PCI DSS requirements. Each requirement is divided into smaller parts, and the SAQ helps to confirm your organization's compliance with the PCI requirements that are relevant to your level.

4. Submit the Attestation of Compliance (AOC)

The AOC requirements vary based on the compliance level. The SAQ is an important tool for determining the compliance of any organization with the PCI DSS requirements, while the AOC serves as a demonstration of that compliance.

5. Conduct a vulnerability scan

To keep your organization's system secure, it is important to scan for vulnerabilities. This can be accomplished by using approved scanning vendors or scanning tools. The SAQ can help determine the most appropriate scanning method.

6. Submit all necessary documentation

To ensure ongoing PCI DSS compliance, it's important to regularly conduct vulnerability scans and monitor systems. Organizations are required to submit the SAQ, AOC, and vulnerability scan report to banks, credit card companies, and other stakeholders to prove their compliance. Compliance is an ongoing process, which makes it important to stay vigilant and monitor systems to protect sensitive data.

Renewing PCI DSS compliance is necessary annually, or whenever there is a modification in the mode of card payments. This reflects potential changes in the organization's processes, payment equipment, or the standard itself as it adapts to new security threats or industry needs. Once this is set, the compliance process becomes more manageable in subsequent years and typically requires less time.

PCI DSS best practices: A checklist

- **Use strong passwords:** User passwords need to be difficult to exploit, which is achieved by using special characters, avoiding character patterns, creating longer passwords, and using all allowed character types. Passwords are also required to be regularly changed to maintain their strength.
- **Encrypt sensitive information:** To protect sensitive data, such as credit card information, it's important to encrypt it both while it is stored and when it is transmitted.
- **Use firewalls:** Firewalls are a crucial component of network security. They prevent unauthorized access to a network by controlling incoming and outgoing network traffic.
- **Get secure payment gateways:** Secure payment gateways ensure the protection of sensitive payment information during transactions by using encryption and other security measures.
- **Use antivirus software:** Antivirus software helps protect the system from malware attacks, which can cause serious harm to the network.
- **Limit remote and physical access:** Limiting remote and physical access to network resources is a key step in protecting sensitive data from unauthorized access.
- **Have a security assessment policy:** A security assessment policy outlines the steps taken to protect sensitive information and ensures that all staff members are aware of the importance of data protection.
- **Restrict traffic to payment systems:** To ensure the security of payment systems, it's important to restrict traffic to only what is necessary and to block any unwanted traffic.

PCI DSS: Key controls to consider

PCI DSS control	Code definition	Compliance recommendations
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	The firewall and router rule sets need to be updated regularly. Organizations should take adequate measures to limit traffic to only inbound and outbound traffic. All the services, ports, and protocols needed for everyday operations are to be documented.
3.2	Storage of account data is kept to a minimum.	Establish data retention and disposal policies with the goal of minimizing cardholder data storage. Implement appropriate access control measures to control cardholder data access.

PCI DSS control	Code definition	Compliance recommendations
6.4	Public-facing web applications are protected against attacks.	Organizations should assess their security vulnerabilities consistently and address them immediately. Within one month of release, critical security patches need to be installed in all applicable devices. Vulnerabilities and known threats to the public-facing web application should be routinely addressed.
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Organizations handling sensitive personal information should implement measures to safeguard data by denying all access requests unless the user is specifically authorized to access the data.
8.6	Use of application and system accounts and associated authentication factors is strictly managed.	Organizations handling sensitive personal information should implement measures, like the Zero Trust policy, to safeguard data by denying all access requests unless the user is specifically authorized to access it.
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	Deploy a logging mechanism to track all access requests and authorization. Logs of audit logs initialization, pausing, and termination should be retained. Security events for all system components should be analyzed to identify suspicious activities.
11.5	Network intrusions and unexpected file changes are detected and responded to.	Organizations are required to deploy a change detection mechanism, like a file-integrity monitoring tool, to facilitate quick response by the security team. Penetration tests are required to be performed annually, or after changes are made to the network infrastructure or applications.

As the threat landscape continues to evolve, it's important to stay current with the latest compliance requirements to safeguard your organization from emerging threats. With its new standards for authentication, password policies, and logging and monitoring, PCI DSS 4.0 further enhances the security of payment card information. Being PCI DSS compliant is not just a requirement, it also offers numerous benefits to organizations. Compliant systems are more secure, and helps in retaining customer trust.

In September of 2017, Equifax, a consumer credit reporting agency, experienced a significant data breach which resulted in the compromise of the personal information of 147 million individuals. To satisfy its obligation, Equifax agreed to a [global settlement](#) with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement provides up to \$425 million to aid those affected by the breach. Strict adherence to PCI DSS can help ensure the systems security and avoid such data breaches. Following PCI DSS standards can also help organizations comply with other federal and state data security regulations. Although compliance may require a significant effort, the potential consequences of non-compliance make it a necessary and worthwhile investment.

Comply with PCI DSS using EventLog Analyzer

Realize the full potential of security and [compliance with ManageEngine EventLog Analyzer](#). You can save time and effort by automating your PCI DSS report generation process, and stay ahead of potential threats with advanced threat analytics. You can also ensure continuous logging and monitoring of activities on all your network devices, and stay alerted to critical security events with EventLog Analyzer's log management and threat detection capabilities. With the comprehensive auditing features of EventLog Analyzer, you don't have to spend tedious hours preparing for audits manually.

ManageEngine **EventLog Analyzer**

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

 **Demo**

 **Download**