**Twelve core PCI DSS requirements**

1. Install and maintain network security controls
2. Apply secure configurations to all system components
3. Protect stored account data
4. Protect cardholder data with strong cryptography during transmission over open, public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict access to system components, and cardholder data by business need to know
8. Identify users and authenticate access to system components
9. Restrict physical access to cardholder data
10. Log and monitor access to system components and cardholder data
11. Test security of systems and networks regularly
12. Support information security with organizational policies and programs

**Twelve PCI DSS requirements for compliance**

There are 12 main requirements in six overarching goals for PCI DSS compliance. According to the PCI SSC, a vendor must complete the following tasks as part of its PCI compliance checklist:  
  
**Goal 1. Build and maintain a secure network.**  
1. Install and maintain a firewall configuration to protect card holder data ([CHD](https://www.techtarget.com/searchsecurity/definition/cardholder-data-CD)).  
2. Not use vendor-supplied defaults for system passwords and other security parameters.

**Goal 2: Protect cardholder data.**

3. Protect stored cardholder data.  
4. Encrypt transmission of cardholder data across open, public networks.

**Goal 3: Maintain a vulnerability management program.**

5. Use and regularly update [antivirus software](https://www.techtarget.com/searchsecurity/definition/antivirus-software).  
6. Develop and maintain secure systems and applications.

**Goal 4: Implement strong access control measures.**

7. Restrict access to cardholder data by business need-to-know.  
8. Assign a unique ID to each person with computer access.  
9. Restrict physical access to cardholder data.

**Goal 5: Regularly monitor and test networks.**

10. Track and monitor all access to network resources and cardholder data.  
11. Regularly test security systems and processes.

**Goal 6: Maintain an information security policy.**

12. Maintain a policy that addresses [information security](https://www.techtarget.com/searchsecurity/definition/information-security-infosec).

To protect stored account data, companies can turn to [Data Loss Prevention (DLP)](https://www.endpointprotector.com/solutions/finance)solutions. These tools prevent data leakage through DLP policies that identify, monitor, and control the transfer and storage of files containing sensitive information such as [personally identifiable information](https://www.endpointprotector.com/blog/how-to-protect-pii-with-data-loss-prevention/) (PII) and account data. DLP tools support regulatory compliance with standards like PCI DSS but also data protection laws such as General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA).

**PCI DSS Compliance Levels**

**Level 1** organizations need to provide a yearly Report on Compliance (RoC) which involves an audit performed by a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA) certified by the PCI Security Standards Council. The auditor submits the RoC to the organization’s acquiring institutions to demonstrate its compliance. They must also undergo an annual network scan by an approved scanning vendor (ASV).

**For levels 2 to 4**, merchants can complete a Self-Assessment Questionnaire (SAQ) with multiple versions to accommodate different types of businesses and processing methods. Requirements for these levels, however, may differ depending on the card scheme: MasterCard, for example, requires Level 2 organizations to complete their SAQ with the assistance of a trained QSA or ISA.

**5 Best Practices for PCI DSS Compliance**

### 1. Data transparency

In the age of compliance, not only of PCI DSS but also [data protection](https://www.endpointprotector.com/blog/data-protection-in-canada-pipeda/) regulations such as the EU [General Data Protection Regulation](https://www.endpointprotector.com/epp/gdpr-the-most-in-depth-guide-to-stay-compliant) (GDPR), knowing exactly where your data is and where it’s going are two fundamental requirements.

Requirement 3 of PCI-DSS states that data should only be stored in specific, known locations with limited access to protect credit card information. Organizations must therefore map their data flow and regularly conduct network scans to ensure credit card information has not been saved or forgotten in unpermitted locations by careless employees.

This can be done through Data Loss Prevention solutions such as [Endpoint Protector](https://www.endpointprotector.com/products/endpoint-protector) which offer data discovery tools that can automatically or manually scan networks for credit card information and encrypt or delete it when it is found on unauthorized users’ computers.

### 2. Securing your data on the move

The two main ways data can be protected on the move are tokenization and encryption. Tokenization generates an alternate ID for a card number which can then be used for transactions, reducing the risk of the actual card information being exposed during transmission.

When it comes to encryption, SSL/early TLS are no longer considered secure forms of encryption and are therefore not enough for PCI DSS compliance. Organizations that want to use encryption to protect card data must use TLS v1.2 or higher.

Data’s mobility can also be checked through DLP tools that allow admins to not only monitor credit card information transfers through predefined policies but also block its transfer altogether through exit points deemed insecure such as file-sharing services or instant messaging applications.

### 3. Restrict access rights

Under requirement 7 of PCI DSS, access to data must be restricted to authorized personnel only. Companies must evaluate which of their employees need access to card data to fulfill their job responsibilities and then use the proper tools and processes to limit access based on business needs.

To achieve this, organizations must first and foremost implement unique ID credentials for every employee to track which users take actions on credit card information and to prevent concurrent logins. Access rights can then be set according to an employee’s job scope using appropriate Access Rights Management (ARM) software.

### 4. Employee training

The weakest link in any security strategy is often the human one: employees are behind over 27% of data breaches, according to a survey conducted by the [Ponemon Institute](https://www.ibm.com/downloads/cas/861MNWN2" \t "_blank). Therefore, it is essential that companies do not neglect the human element in PCI DSS compliance. Software, whether DLP, ARM, or antivirus, while it can increase security greatly, is much more effective when employees understand its need.

An informed workforce is less likely to look for ways to bypass security measures when they know their purpose. Companies must therefore invest in industry-specific employee training, ensuring that they comprehend the importance of PCI DSS and the risks and consequences of noncompliance.

### 5. Document and log everything

Part of requirement 12 of PCI DSS compliance, document everything underlines the need for organizations to keep records of all its security policies and procedures, risk assessments, and security incidents. Strong documentation helps CIOs and security professionals make informed decisions concerning future security measures and allows companies prove compliance.

Logs and log monitoring are found under requirement 10 of PCI DSS and include logs of all security events, servers, and critical system components. Companies should ensure that their antivirus solution provides logs of security incidents. They can also generate logs of attempted unauthorized transfers and the users responsible for them through DLP solutions.

**Internal Security Assessor (ISA)™ Qualification**

The Internal Security Assessor program teaches you how to perform internal assessments for your company and recommend solutions to remediate issues related to PCI DSS compliance. Assessors are sponsored by their companies, so when you receive this qualification, you will be able to act as a liaison with external PCI auditors and manage interactions with a Qualified Security Assessor (QSA).

PCI Fundamentals

PCI Fundamentals is a prerequisite for many of our courses. This class assures that all candidates have the same baseline understanding. The PCI Fundamentals course must be completed within thirty days of initial access and a minimum of one week prior to the start of a training class.

The online prerequisite course concludes with a 60-question multiple-choice exam. Once the candidate has completed the PCI Fundamentals training and exam, the Primary Contact will be notified of either a passing or failing grade. If the candidate failed the exam, he or she will be allowed two additional attempts to take and pass without being charged an additional fee.

To help you prepare for the course, we encourage you to review two publications from the Document Library on the PCI Council website:

* PCI Glossary
* PCI Data Security Standard