# Lesson 4 | Introduction to PCI-DSS

Updated 2020-09-30

## The PCI DSS

The PCI DSS is made up of 12 requirements. Each requirement has several sub-requirements. The DSS is written to provide guidance for both companies and assessors. Each requirement contains the following.

1. The requirement itself. This is the standard that needs to be met.
2. Testing procedures to assess compliance with the requirement. This is used by the assessor.
3. Specific guidance behind the requirement. The guidance justifies and provides reasoning for the requirement. The guidance is most often used to help create compensating controls that do not meet the specific testing procedures for the requirements.

Overall, the PCI DSS is very detailed and explicit for companies that are assessed against it and for assessors performing PCI assessments.

The 12 requirements are below under the PCI assigned category.

**Build and Maintain a Secure Network and Systems**

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

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

**Maintain a Vulnerability Management Program**

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components

9. Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

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

**Maintain an Information Security Policy**

12. Maintain a policy that addresses information security for all personnel

## Compensating Controls

If organizations are able to meet any of the above requirements because of “legitimate technical or documented business constraints”, the can implement compensation controls that mitigate for the risk of not addressing the DSS requirements. Similar to the DSS requirements themselves, these compensating controls need to be evaluated on an annual basis.

---

*The PCI DSS is the core of PCI. The requirements you need to meet are determined by your entity type and level.*

---

## What next?

If you want to learn more about the PCI DSS, our PCI DSS In-Depth course goes into detail about each of the 12 requirements in the DSS.