

General FAQ

Payment Card Industry Data Security Standard (PCI DSS)

What is the PCI DSS? And what do the acronyms CISP, SDP, DSOP and DISC stand for?

Are all Businesses and Service Providers required to comply with the PCI DSS?

Is this a one-time requirement?

What are the requirements for PCI DSS?

What is the Visa deadline for compliance for newly-boarded businesses?

How is "cardholder data" defined?

Can I store magnetic stripe data? How about the CVV2 and CVC?

Compliance Validation

What is the PCI Self-Assessment Questionnaire?

What is a Network Vulnerability Scan?

What if I fail the scan?

What is a Directed Scan?

What are the penalties and fines associated with a security breach?

Do I have to use a QSA? Where do I find one?

Who is Trustwave?

Is there a deadline to be compliant?

How are the PCI DSS levels defined?

What if my business does not go through this compliance procedure?

Do I get anything to prove I am compliant, if so, will it be automatically sent to Visa or MasterCard?

Can our internal staff validate our compliance?

We don't have time for this. How long will this take?

TrustKeeper Overview

What is TrustKeeper?

Why should I enroll in TrustKeeper?

What is the PCI DSS? And what do the acronyms CISP, SDP, DSOP and DISC stand for?

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International), to help facilitate the global adoption of consistent data security measures. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures intended to proactively protect customer account data.

The card brands each have their own programs that help businesses enforce compliance with the PCI DSS. The PCI Security Standards Council was founded in 2006 to oversee the standard itself, but each of the card brands issues fines, fees and schedule deadlines through their own enforcement programs.

Visa's Cardholder Information Security Program (CISP)

<http://www.visa.com/cisp>

MasterCard's Site Data Protection (SDP) program

<http://www.mastercard.com/us/sdp/index.html>

Discover's Discover Information Security and Compliance (DISC) program

<http://www.discovernetwork.com/fraudsecurity/disc.html>

American Express Data Security Operating Policy (DSOP)

<http://www.americanexpress.com/datasecurity>

PCI Security Standards Council

<http://pcisecuritystandards.org>

Are all Businesses and Service Providers required to comply with the PCI DSS?

Yes. All entities (businesses or service providers) that store, process, or transmit cardholder data must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and-mortar), mail/telephone order (MOTO) and e-commerce. Validation requirements vary depending on Service Provider or Merchant level.

Is this a one time requirement?

No. Validation actions vary depending on Service Provider or Merchant level. However, the credit card associations require all businesses accepting card-based payments to comply with PCI DSS at all times. There are two main components of validation:

1. Completing the PCI Self-Assessment Compliance Questionnaire annually
2. Undergoing Vulnerability Scans performed by an Approved Scanning Vendor quarterly

What are the requirements for PCI DSS?

There are 12 requirements that fall into six categories:

1. Build and Maintain a Secure Network: Install and maintain a firewall, and use unique, high-security passwords, with special care to replace default passwords.
2. Protect Cardholder Data: Whenever possible, do not store cardholder data. You must also encrypt any data passed across public networks, including your shopping cart and web-hosting providers.
3. Maintain a Vulnerability Management Program: Use anti-virus and keep it up date. Develop and maintain secure operating systems and payment applications. Ensure the applications your use are compliant (see www.visa.com/pabp).
4. Implement Strong Access Control Measures: Access – both electronic and physical access – to cardholder data should be on a “need-to-know” basis. Ensure those people with access have a unique ID and password. Do not share logon information.
5. Regularly Monitor and Test Networks: Track and monitor all access to networks and cardholder data. Ensure you have a regular testing schedule for security systems and processes: firewalls, patches and anti-virus.
6. Maintain an Information Security Policy: It’s critical that your organization has a resource for how data security is handled at your business. Ensure you have a policy and that it’s disseminated and updated regularly.

What is the Visa deadline for compliance for newly-boarded businesses?

To promote payment application security awareness and increase adoption of secure payment applications, Visa instituted a number of payment application security mandates in October of 2007. Effective October 1, 2008, newly boarded Level 3 and Level 4 merchants must be PCI DSS compliant or must use PA-DSS compliant applications.

How is “cardholder data” defined?

Cardholder data is the full magnetic stripe or the Primary Account Number plus any of the following:

- Cardholder Name
- Expiration Date
- Service Code

The PCI DSS applies to any businesses that store, process, transmit or have access to cardholder data.

Can I store magnetic stripe data? How about the CVV2 and CVC?

It is never acceptable to store magnetic stripe data after authorization of the transaction. It is also never acceptable to retain CVV2 and CVC, (the last three digits printed on the signature panel) after transaction authorization.

Compliance Validation

What is the PCI Self-Assessment Questionnaire? The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the PCI DSS. In February of 2008, the PCI Security Standards Council released four versions of the questionnaire to account for different business environments.

1. SAQ A: Addresses requirements applicable to businesses who have outsourced all cardholder data storage, processing and transmission.
2. SAQ B: Created to address requirements pertinent to businesses who process cardholder data via imprint machines or standalone dial-up terminals only.
3. SAQ C: Constructed to focus on requirements applicable to businesses whose payment applications systems are connected to the Internet.
4. SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

What is a Network Vulnerability Scan?

A network vulnerability scan is an automated, non-intrusive scan that assesses your network and web applications from the Internet (on the external-facing IPs). The scan will identify any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data. The scans provided by Trustwave will not require you to install any software on their systems, and no denial-of-service attacks will be performed.

What if I fail the scan?

If you fail the network vulnerability scan in TrustKeeper, this means that the scan has discovered areas of vulnerability in your network of high severity. TrustKeeper will help guide you to remediate a failed scan and work toward achieving compliance. First, you'll want to login to TrustKeeper to review the scan results. The report will provide a description of the identified issues and resources to begin fixing the problems. You'll need to address each of the problems and then schedule a directed scan to ensure your remediation of the problem meets the PCI DSS.

What is a Directed Scan?

Many times a vulnerability scan will discover vulnerabilities that need to be resolved in order to maintain compliance. Once you resolve these vulnerabilities, a directed scan can be run upon your request to verify that you have resolved any compliance issues. You may also run a directed scan after you have made changes to your network to ensure that the changes have not affected your compliance status. These are additional scans above and beyond the regular quarterly scans.

What are the penalties and fines associated with a security breach?

Per the card associations, the penalties and fines for failure to comply with requirements or to rectify a security issue can be severe. These fines range from \$10,000 to \$500,000 per incident. If a security breach occurs in your environment, you will be liable for the cost of the required forensic investigations, fraudulent purchases, and the cost of re-issuing cards. Please note that you may also lose your credit card acceptance privileges.

Do I have to use a QSA? Where do I find one?

Yes, you must use a Qualified Security Assessor (QSA) that has been approved by the PCI Security Standards Council (PCI SSC). A list of approved Qualified Data Security Companies can be found on the PCI SSC's website at www.pcisecuritystandards.org. Trustwave is both a certified QSA and an Approved Scan Vendor (ASV).

Who is Trustwave?

Trustwave is the leading provider of on-demand data security and payment card industry compliance management solutions to Fortune 2000 businesses and the public sector. Our flagship product, TrustKeeper®, provides data security and compliance validation services to over 100,000 businesses throughout the world to achieve compliance with the PCI DSS and other regulatory requirements. Trustwave is an Approved Scanning Vendor (ASV) and a Qualified Security Assessor (QSA) for the card associations.

Is there a deadline to be compliant?

Yes. All businesses are supposed to be compliant with the PCI DSS. However, the deadlines vary depending on your PCI DSS level. Your PCI DSS level is determined by the number and type of payment card transactions you process in a year. Acquirers may also set their own deadlines for compliance. Please note that compliance is not a one-time requirement. You should achieve and maintain compliance on an ongoing basis.

How are the PCI DSS Levels Defined?

Visa and MasterCard publish the following levels:

Level / Tier 1	Business Classification Criteria
1	<u>Visa & MasterCard</u> : Any business—regardless of acceptance channel—that: <ul style="list-style-type: none"> ▪ Processes over 6 million Visa or MasterCard transactions per year ▪ Has suffered a hack or an attack that resulted in an account data compromise ▪ Visa or MasterCard determines should meet the Level 1 requirements ▪ Has been identified by any other payment card brand as Level 1
2	<u>Visa & MasterCard</u> : Any business that processes 1 million to 6 million Visa or MasterCard transactions, regardless of acceptance channel
3	<u>Visa & MasterCard</u> : Any business that processes 20,000 to 1 million Visa or MasterCard e-commerce transactions
4	<u>Visa & MasterCard</u> : Any business that processes fewer than 20,000 Visa or MasterCard e-commerce transactions or processes fewer than 1 million Visa or MasterCard transactions, regardless of acceptance channel

What if my business does not go through this compliance procedure?

If you do not comply with the security requirements of the card associations, you put your organization at risk of payment card compromise. Your acquirer may also pass fines levied by the card associations for non-compliance on to you.

Do I get anything to prove I am compliant, if so, will it be automatically sent to Visa or MasterCard?

Once you have successfully completed the compliance program, Trustwave will issue you a Certificate of Compliance. Any reporting to your acquirer will be facilitated by TrustKeeper. It is the acquirer's responsibility to report statuses to the Card Associations.

Can our internal staff validate our compliance?

No. The card associations require that you use an Approved Scanning Vendor to perform the quarterly vulnerability scans. However, your internal staff can complete the Annual PCI Self-Assessment questionnaire.

We don't have time for this. How long will this take?

The length of the process varies. Once non-compliance issues have been identified, the length of time it takes an organization to implement solutions to resolve the issues will affect the length of the PCI DSS compliance process. The length of time also varies depending on the resolution and the complexity of the environment.

TrustKeeper Overview

What is TrustKeeper? TrustKeeper is a state-of-the-art vulnerability assessment and compliance management solution that provides compliance validation tools for the PCI DSS. TrustKeeper offers easy-to-use vulnerability management services to help protect critical business information. In TrustKeeper you have access to:

- Scanning engine that tests for more than 5,000 vulnerabilities
- PCI Self-Assessment Questionnaire
- Detailed compliance status reporting
- Vulnerability prioritization
- Remediation services to address security vulnerabilities and achieve compliance more quickly
- Comprehensive online support resources
- Multi-lingual help desk support

Why should I enroll in TrustKeeper?

In TrustKeeper, you can easily complete the PCI DSS process—have a vulnerability scan and complete the full Self-Assessment Questionnaire. TrustKeeper will help identify the steps you need to take to remediate your vulnerabilities and ensure that you protect your customers' payment card information and your network.