

Account Information Security

Implementing the Payment Card Industry
Data Security Standards (PCI DSS)

A guide for Service Providers



Contents

1.0	Introduction	02
1.1	Protecting customer data	02
1.2	What is the Payment Card Industry Data Security Standard?	03
1.3	Who does it apply to?	03
1.4	The benefits for your business	04
2.0	Understanding the implementation process	06
2.1	Helping your business with the implementation	06
2.2	An overview of the implementation process	06
3.0	Guiding principles	09
4.0	Implementing PCI DSS	11
4.1	Step One: Establish how PCI DSS relates to you	11
4.2	Step Two: Map out the data flows	11
4.3	Step Three: Contact Visa and inform us of your status	12
4.4	Step Four: Conduct a gap analysis and plan your remediation activity	12
4.5	Step Five: Remediation activity	12
4.6	Step Six: Certification and validation	13
4.7	Step Seven: Notifying Visa and your customers	13
5.0	Staying compliant	15
6.0	We are here to help	17



1.0 Introduction

- 1.1 Protecting customer data
- 1.2 What is the Payment Card Industry Data Security Standard?
- 1.3 Who does it apply to?
- 1.4 The benefits for your business



1.0 Introduction

1.1 Protecting customer data

Right around the world, the security of cardholder account data has become a matter of real concern - to the banks that offer payment card services, as well as the merchants that accept them and, of course, the customers that use them.

In many countries worldwide, there have been instances of hackers accessing computer systems, stealing cardholder data, and using this data to commit fraud. In most cases, these computer systems have been operated by merchants that accept payment cards, or service providers that process payments on their behalf.

In response, Visa has created the Payment Card Industry Data Security Standards (PCI DSS). This is a set of industry-wide requirements and processes, developed in partnership with MasterCard International, and supported by every other major international payment card system.

Account Information Security (AIS) is the name for Visa's compliance programme.

Clearly, the implementation of PCI DSS has significant implications for the service provider community - that is, any companies that are involved in the processing of card transactions, or that provide any associated products, services or applications.

Visa is here to help.

We have created a set of tools and resources to make it as straightforward as possible for you to implement PCI DSS. By implementing these standards you become compliant with our own AIS programme, and you automatically meet the requirements and recommendations set out by other international payment card systems such as American Express, Diners Club, JCB and Discover.

This guide tells you more about the process.



1.2 What are the Payment Card Industry Data Security Standards?

PCI DSS consists of a standardised, industry-wide set of requirements and processes.

Its purpose is to ensure that valuable cardholder account data is always secure.

It comprises 12 key requirements.

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for passwords or other security parameters
3. Protect stored data
4. Encrypt the transmission of cardholder data and sensitive information
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

By implementing PCI DSS, any business will automatically comply with the requirements and regulations set out by all of the big international payment card schemes and their acquiring banks.

Full details can be accessed at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

1.3 Implications for Service Providers

PCI DSS applies to every acquiring bank, every merchant that accepts payment cards and, by implication, every service provider that works on their behalf.

Most service providers will be well aware of the background to PCI DSS.

In recent months several high profile cases of data compromise have been covered in the media. In many cases, service providers have been directly implicated, and the consequences for their respective businesses have been severe - including some business failures.

Against this background, it is therefore inevitable that:

- > Both acquirers and merchants will insist that service providers and their products are compliant
- > Service providers will use their degree of compliance as a point of competitive differentiation



Clearly, the service provider community includes many different types of company. For the purposes of this guide, however, we will refer to two broad business categories, namely:

- > Payment Service Providers - those companies that are involved in the actual processing and/or storage of payment card transactions (including processors, payment gateways, payment processing bureaux, and iPSPs)
- > Payment Application Providers - those companies that provide products or applications which are used in the processing of payment card transactions (including software vendors and EPOS vendors)

The steps you need to take will depend on which of these two categories you fall into. In the case of Payment Service Providers, it may also depend on the scale of your business (in terms of the volume of transactions you are involved in processing).

If you are in any doubt at all about which category your business falls into or the requirements expected, please do not hesitate to contact us at datasecuritystandards@visa.com

1.4 The benefits for your business

In today's environment, security has to be a consideration for every type of business.

Right around the world, there is a general expectation - and often a legal requirement - that every business should protect customers and consumers, and safeguard any information relating to them.

Irrespective of the requirements specified by the all of the international card schemes, implementation of PCI DSS therefore makes sound business sense for any service providers.

In particular, it can:

- > Identify any risks in the way you or your products store or transmit cardholder data
- > Provide a clear path of action and remediation to address any risks
- > Demonstrate to your customers that you are serious about security

Also, by minimising the risk of data compromise, it can:

- > Protect against financial liabilities
- > Protect against the risk of investigative and legal costs
- > Protect against the risk of invasive media attention

The fact is that, as card acceptance technologies have evolved, payment card fraud has become more sophisticated. Every business which stores or transmits cardholder account data is a potential target. Details of some high profile cases of data compromise, and their global repercussions, can be accessed at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

PCI DSS minimises the risk to your business.

Visa provides a full listing of PCI DSS compliant service providers at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity. By working in partnership with you, we want your business to appear in this listing.



2.0 Understanding the implementation process

- 2.1 Helping your business with the implementation
- 2.2 An overview of the implementation process



2.0 Understanding the implementation process

2.1 Helping your business with the implementation

The particular way that PCI DSS relates to your business, and the way in which it should be implemented, will depend upon the nature of your business and the scale of your operations.

In most cases, however, PCI DSS compliance will represent a significant undertaking, which may take several months to complete. Visa is eager to help you through every step of your implementation - and we have a dedicated programme of activity to work with service providers.

This document is intended to:

- > Guide you, step-by-step through the process
- > Give you easy, immediate access to all related documentation
- > Put you in direct touch with Qualified Security Assessors

Visa provides a full listing of PCI DSS compliant service providers at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity. By working in partnership with you, we want your business to appear in this listing.

If you have any questions please contact us direct at datasecuritystandards@visa.com.

2.2 An overview of the implementation process

The diagram overleaf provides you with an overview of the implementation process.

The first step is to familiarise yourself with the specific details of PCI DSS, and the way that it relates to your own business.

> **For Payment Service Providers**

It will be necessary to assess whether your systems and operations (plus the systems and operations of any third parties you may work with) comply with PCI DSS and undertake any necessary remediation. Then, to validate your compliance, it will be necessary to conduct a full PCI DSS assessment of your operations.

> **Payment Application Providers**

It will be necessary to assess whether your products and/or applications comply with PCI DSS and to update them accordingly. Then, to validate their compliance, it will be necessary to have your products assessed and certified

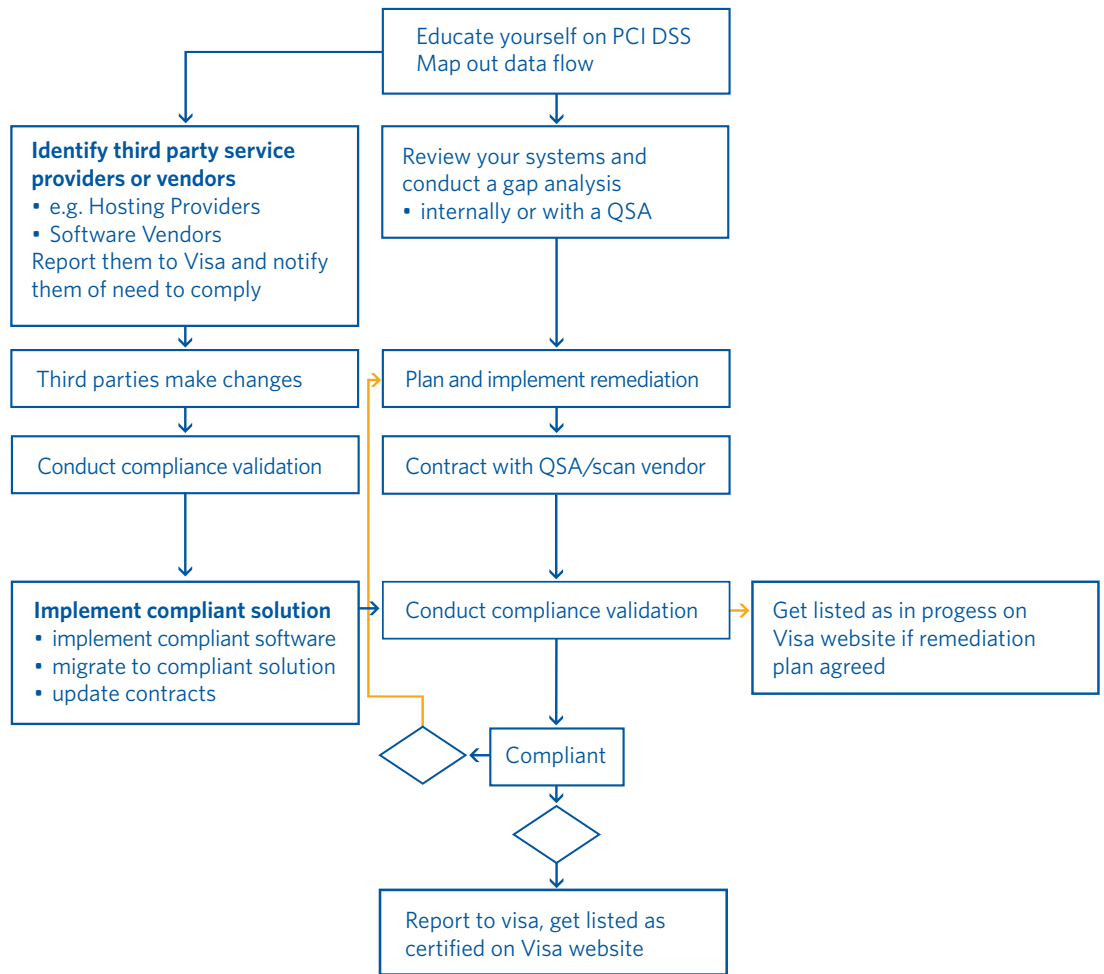


Products and applications will be audited according to the Payment Application Security Standard (currently Best Practices, which are derived directly from PCI DSS).

As a starting point, it will be necessary to map out the data flows (of cardholder account data) within your products or systems.

Based on this analysis, you can ascertain the extent to which you (and any vendors working on your behalf) already comply with PCI DSS, or what level of remediation may be necessary.

Step by Step Implementation for Service Providers



3.0 Guiding principles



3.0 Guiding principles

When planning for your PCI DSS compliance programme, or when considering any upgrade to your products or your systems, it may be useful to keep the following principles in mind:

1. Card acceptance systems which do not store any card account data beyond the initial authorisation of the transaction are always the most secure option.

If there is no business requirement for you or your customers (for example, merchants) to store such data, it should always be discouraged. Also, if neither you nor your customers store any data, it will not be necessary for you to validate compliance with PCI DSS.

2. Where there is a business reason for data to be stored, it should always be done so in accordance with PCI DSS
3. Any systems or products which are not compliant with PCI DSS will expose your own business, and your customers (merchants) to a significant (and entirely unnecessary) level of risk.

Visa is working across the service provider community to assist with adapting existing systems and/or applications, or to create a new generation of systems and/or applications which either:

- > Do not store any account data beyond the initial authorisation of the transaction
- Or
- > Do store data where there is a business reason to do so, but only in accordance with PCI DSS



4.0 Implementing PCI DSS

- 4.1 Step One: Establish how PCI DSS relates to you
- 4.2 Step Two: Map out the data flows
- 4.3 Step Three: Contact Visa and inform us of your status
- 4.4 Step Four: Conduct a gap analysis and plan your remediation activity
- 4.5 Step Five: Remediation activity
- 4.6 Step Six: Certification and validation
- 4.7 Step Seven: Notifying Visa and your customers



4.0 Implementing PCI DSS

4.1 Step One: Establish how PCI DSS relates to you

Implementing PCI DSS within your own business entails:

- > Finding out more about the way your business and/or applications work
- > Determining whether cardholder account data is handled securely
- > Putting remediation in place to address any associated risks

The first step should be to familiarise yourself with PCI DSS and relate its content to your own business.

Full details of PCI DSS can be accessed at

www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

PCI DSS is based on established best practice for securing data (such as ISO17799). By familiarising yourself with its content, you will understand what is deemed, by all international payment cards systems, to be an acceptable degree of protection.

Note: For Payment Application Providers, you should also familiarise yourself with the Payment Application Security Standard (currently Best Practices, dDerived directly from PCI DSS), these can be accessed at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

4.2 Step Two: Map out the data flows

Once you are familiar with PCI DSS, the next step should be to put a project team in place.

The immediate priority of this team should be to analyse the precise manner in which card payments are processed within your systems (and/or applications), and to map out all of the related data flows.

This exercise should reveal two critical facts:

- > It should identify any systems in which cardholder account data is stored
- > It should reveal which of these systems are under your direct control

Note: depending on the nature of your business, it is possible that some such systems will be under the control of a third party service provider. If this third party provider works on your behalf, it will be your responsibility to ensure that they are PCI DSS compliant.



4.3 Step Three: Contact Visa and inform us of your status

If you have not already done so, this would be an appropriate point to establish contact with Visa.

We have a specific programme in place to assist service providers with PCI DSS compliance and can provide support and advice to your business.

4.4 Step Four: Conduct a gap analysis and plan your remediation activity

Having mapped out the data flows, you should have identified if and how any of your systems (and/or applications) store cardholder account data.

During these initial stages of the implementation process you should:

- > Get an indication of the extent of remediation work which may be required in order to comply with PCI DSS
- > Assess the level of resource which may be required and the likely timeframes for completion of the process

At this stage you should also consider if and how to engage the services of a Qualified Security Assessor - that is, a specialist auditor, qualified by Visa to assist in PCI DSS compliance.

Visa maintains a listing of all Qualified Security Assessors (QSAs). A copy of this listing can be found at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

Visa also maintains a listing of all service providers which are actively working towards compliance with PCI DSS. Through liaison with you and/or your Qualified Security Assessor, your business could also be included in this listing.

4.5 Step Five: Remediation activity

Working independently or in partnership with a Qualified Security Assessor, your business will implement the necessary remediation activity, making all of the required systems, procedural and legal changes.

Once the changes have been made, your own business should be fully compliant with PCI DSS.



4.6 Step Six: Certification and validation

Once the necessary changes have been made, you will be ready to go through a formal assessment and certification process.

> Payment Application Providers

Your applications will need to be independently assessed by a Qualified Security Assessor according to the Payment Application Security Standard (currently Best Practices).

Once the assessment has been successfully completed, the Qualified Security Assessor will notify Visa that the assessed version of your application is compliant

> Payment Service Providers

Your business and all of its operations will need to be independently assessed by a Qualified Security Assessor according to PCI DSS.

During the assessment process (which consists of either completion of a questionnaire, or in most cases an onsite audit), the Assessor will follow a standard testing procedure, built around the 12 PCI DSS requirements. A copy of the complete Security Audit Procedures that an Assessor will perform during an on-site audit can be accessed at

www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

It will generally be necessary to repeat this on site audit on an annual basis.

At this stage, it will also be necessary for you to complete a Vulnerability Scan. This will ensure that your systems are protected from the external threats (such as hacking or malicious viruses). The scanning tools test all of your network equipment, hosts, and applications for known vulnerabilities.

Scans are intended to be non-intrusive, and are conducted by an authorised network security scanning vendor. A full listing of providers is available at

www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

It will be necessary for follow-up scans to be repeated on a quarterly basis - ensuring that your systems and applications continue to afford adequate levels of protection.

4.7 Step Seven: Notifying Visa and your customers

Once your business and/or applications are successfully certified as PCI DSS compliant, you will be in a position to promote the fact to your customers.

Also, once your compliance has been validated, we can include your details in the listing of compliant service providers/product versions which is maintained at

www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity (following an optional quality review of your compliance report by Visa Europe).



5.0 Staying compliant



5.0 Staying compliant

Implementing the PCI DSS should not be regarded as a box-ticking exercise. Instead it is intended to protect your business (and your customers) against real risks.

By undertaking any necessary remediation work you bring immediate protection to your business. However, it is important for you to ensure that this level of protection is always maintained. In particular, it is recommended that you put processes in place within your business to ensure that you do not fall out of compliance.

For example, you should:

- > Review your access control policy regularly
- > Integrate vulnerability scans into your regular business routines
- > Ensure that any new systems or applications are fully compliant
- > Create processes and procedures to make sure your anti-virus systems are regularly updated

To provide an additional safeguard, it will be necessary for most payment service providers (according to their assigned PCI DSS level) to undergo an annual onsite audit and quarterly vulnerability scans.

For payment applications, each new product version will need to be certified before it is listed.



6.0 We are here to help



6.0 We are here to help

For any further information relating to PCI DSS, please refer to our website at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

By working with our acquiring banks, Visa is committed to making it as easy, convenient and secure as possible for your business to accept payment cards.

If you have any questions, please contact us direct at datasecuritystandards@visa.com.

