

Account Information Security

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

A guide for Merchants



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	07
3.0	Step One: Familiarise Yourself with the Payment Card Industry Data Security Standard	09
4.0	Step Two: Map out the data flows in your business	11
5.0	Step Three: Check and monitor the status of your service providers	13
5.1	Assisting your service providers with implementation	13
5.2	Certification for service providers	14
5.3	Implementing a compliant solution	14
6.0	Step Four: Conduct a gap analysis and scope the project	16
7.0	Step Five: Select your validation option	18
7.1	About the annual on-site audit	18
7.2	About the quarterly Vulnerability Scan	19
7.3	About the annual Self-Assessment Questionnaire	19
8.0	Step Six: Plan and implement remediation	21
9.0	Step Seven: Certification	23
10.0	Staying compliant	25
11.0	We are here to help	27



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 vendors that process payments on their behalf.

In response Visa has worked together with MasterCard to create the Payment Card Industry Data Security Standards (PCI DSS). This is a set of industry-wide requirements and processes, supported by every major international payment card system.

Account Information Security (AIS) is the name of Visa's PCI DSS compliance programme.

Every business that accepts card payments can benefit from compliance with PCI DSS - protecting your customers and safeguarding your reputation.

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 the 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 every major international payment card system.

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, your business will automatically comply with the requirements and regulations set out by international card payment schemes and acquiring banks.

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

1.3 Who does it apply to?

PCI DSS applies to every acquiring bank, merchant, and third party that accepts or processes payment cards.

Visa has specified in its Regulations that all member banks must be compliant with PCI DSS. Acquiring banks are also responsible for ensuring that all of the merchants they represent are compliant.

The steps you need to take to achieve compliance with PCI DSS will depend on the scale of your business and the nature of your card acceptance systems.

For example, if you do not actually store any cardholder account data in your own systems, it will be up to any payment service providers that process transactions or access card data on your behalf to validate compliance.

If this is the case, compliance with PCI DSS should still be a process that you drive. It is in your best interests to bring any third parties you work with into compliance as soon as possible.



Such third party service providers may include:

- > Resellers
- > Software Application Providers
- > Acquirers
- > Payment Service Providers
- > Card Processing Bureau's
- > Data Storage Entities
- > Web Hosting Providers
- > Shopping Cart Providers
- > Miscellaneous Third Party Agents
- > Software vendors

Read though this guide for more details.

1.4 The benefits for your business

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

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

Compliance with PCI DSS therefore makes sound business sense for any retail business:

In particular, implementation of PCI DSS can:

- > Identify any risks in the way you store or transmit customer data
- > Provide a clear path of action and remediation to address any data security risks
- > Ensure that your service providers do not put your business at data security risk
- > Demonstrate to your customers that you are serious about their data security

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

- > Protect against potential financial liabilities (including the full cost of any fraud perpetrated on compromised card accounts)
- > Protect against the risk of investigative and legal costs
- > Protect against the risk of invasive media attention

The fact is that, as the technologies used by retailers and their partners 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 compliance minimises the data security risk to your business.



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 size and nature of your business
- > The configuration of your card acceptance systems and processes
- > The service providers you work with and their respective roles

By working with our acquiring banks, Visa is eager to help you through the implementation process.

This document is intended to:

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

If you have any questions, please call your acquiring bank. Alternatively you can contact Visa direct at datasecuritystandards@visa.com.



2.2 An overview of the implementation process

The diagram below provides you with an overview of the PCI DSS implementation process.

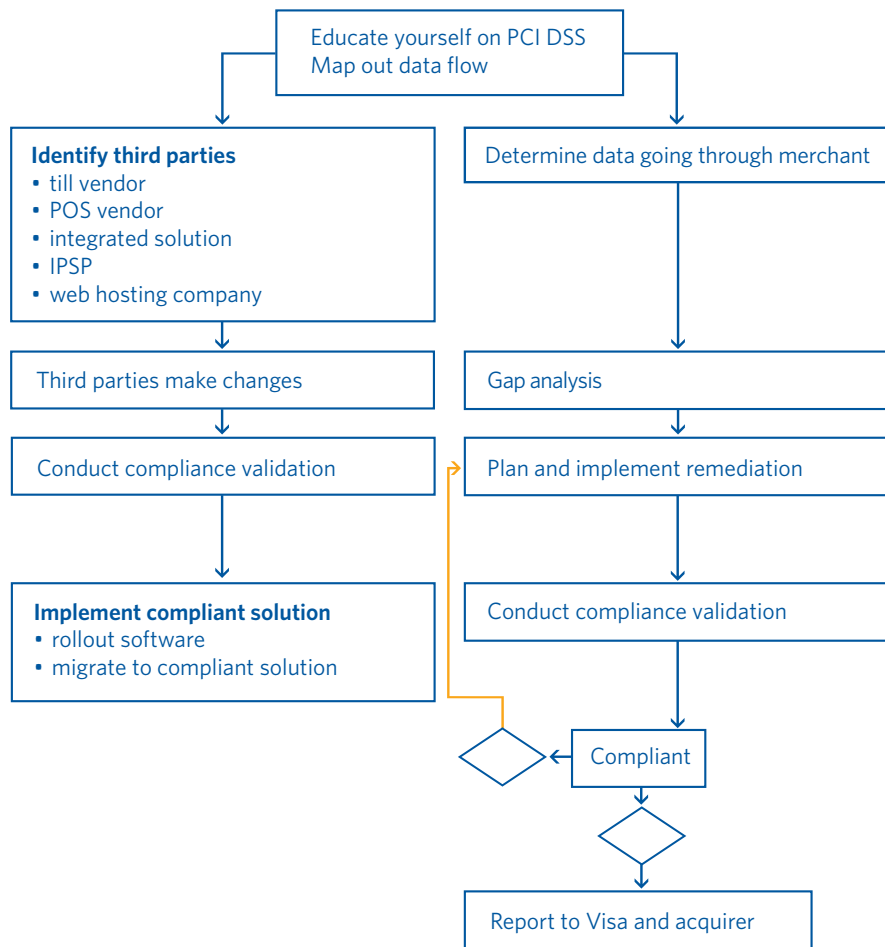
The first step is to familiarise yourself with the specific details of PCI DSS (which can be found at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity), and then to map out the data flows (of cardholder account data) within your own business.

This will reveal:

- > The extent to which any cardholder account data may be stored within or transmitted through your own systems
- > The extent to which any cardholder account data may be stored by or transmitted by any vendors that work on your behalf

Based on this analysis, you can ascertain whether you (and any vendors working on your behalf) already comply with PCI DSS, or whether any remediation is necessary to comply.

Step by Step Implementation for Merchants



3.0 Step One: Familiarise Yourself with the Payment Card Industry Data Security Standard



3.0 Step One: Familiarise Yourself with the Payment Card Industry Data Security Standard

Implementing PCI DSS entails:

- > Finding out more about the way your business works
- > Determining whether it handles cardholder account data securely
- > Putting remediation in place to address any associated data security risks

The first step should be to familiarise yourself with PCI DSS, the full details of which 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 international payment cards systems, to be an acceptable degree of protection.



4.0 Step Two: Map out the data flows in your business



4.0 Step Two: Map out the data flows in your business

Once you are familiar with PCI DSS, the next step should be to put a project team in place within your business. The immediate priority of this team should be to analyse the way that card payments are processed within your business, 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

Depending on the scale and nature of your business, it is likely that some (or perhaps all) such systems will be under the control of a third party service provider or vendor (such as a till vendor, a POS vendor, an integrated solution provider, an Internet Payment Service Provider, a payment gateway provider, or a web hosting company).

In such circumstances it is likely (under the agreement which you have in place with your acquiring bank) that your business will be responsible for the activity of these third party providers.

You should now be able to identify two streams of actions:

- > Any actions which are necessary to ensure that all of your service providers comply with PCI DSS (Step 3 in section 5 of the guide)
- > Any actions which are necessary to implement PCI DSS compliance within your own business (Step 4 to Step 10 section 6 onwards)

Note: Step 3 in section 5 of the guide relates to the way you should work with any service providers. If you do not work with any such service providers, go directly to Step 4 section 6 onwards.



5.0 Step Three: Check and monitor the status of your service providers

- 5.1 Assisting your service providers with implementation
- 5.2 Certification for service providers
- 5.3 Implementing a compliant solution



5.0 Step Three: Check and monitor the status of your service providers

Under the terms of the agreement you have in place with your acquiring bank, your business may be directly responsible for the data security activities of any payment service providers who work on your behalf. It is therefore incumbent on you to verify that all such service providers comply with PCI DSS.

Given that cardholder data security is such an important issue for the payment card industry, it is likely that all of your service providers will be aware of PCI DSS. Many providers are already compliant, and many others have a formal programme in place to become compliant.

It is advisable that you regularly track the progress towards compliance of your service providers. In the case of compromise (depending on the contractual agreement between yourself and your acquiring bank), you may be held responsible for costs associated with the compromise.

Visa maintains a complete listing of all service providers that are compliant or which are working towards compliance. This can be accessed at

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

If your service providers do not appear on this listing, it will be necessary for you to ensure that they take action. In particular, Visa recommends that compliance with PCI DSS should become a contractual requirement for all of your service providers.

As part of our Account Information Security (AIS) programme, Visa assists service providers through the compliance process. We therefore recommend that you inform your acquiring bank of any non-compliant service providers, who will then register them with Visa.

During the compliance process your acquiring bank may seek your support and intervention. It may, for example, ask you to put additional pressure on a particular service provider (for example by seeking assurances from them that they will become compliant within a reasonable timeframe).

5.1 Assisting your service providers with implementation

Visa will typically work proactively with a service provider in order to guide them through the compliance process.

In most cases, the service provider will engage the services of a Qualified Security Assessor - that is, a specialist auditor, certified by Visa and/or MasterCard to assist in PCI DSS compliance.

Please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity for a listing of Qualified Security Assessors.

The Qualified Security Assessor will work with the service provider to map their data flows. Based on this information, they will then conduct a gap analysis to identify the areas where remediation work is needed, and agree on the remediation activity required to bring the service provider into compliance with PCI DSS.

The service provider will then plan and implement the agreed activities, and make the necessary system, procedural, and legal changes, in preparation for certification.



5.2 Certification for service providers

Once the agreed changes have been made, the service provider will be ready to go through a formal audit and PCI DSS certification process, conducted by a Qualified Security Assessor.

In order to complete the audit, the assessor will present Visa with a copy of a completed audit document. The audit document provides full details of the audit procedure.

Please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity for a copy of the standard audit document.

If the service provider is a software vendor, its software products will be audited according to the Payment Application Best Practices.

These Best Practices, which are derived from PCI DSS, and ensure that the payment software used by a merchant is compliant with PCI DSS, can be accessed at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

In all other instances, the service provider will be audited according to PCI DSS.

5.3 Implementing a compliant solution

Once the Qualified Security Assessor has confirmed that a software vendor is compliant with PCI DSS, the vendor will be able to provide compliant products to its clients and assist in their deployment.

Similarly, as soon as a service provider confirms that its own systems are compliant with PCI DSS any of your data that is managed by that service provider will be deemed to be PCI DSS compliant.

In some instances, additional remediation work may be required relating to any cardholder account data which is stored by your own systems. At this point, your own business should also be ready to be audited for compliance.



6.0 Step Four: Conduct a gap analysis and scope the project



6.0 Step Four: Conduct a gap analysis and scope the project

Having mapped out the data flows within your business, you should have identified any of your own systems which store cardholder account data.

These systems should be treated as your primary focus.

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
- > Put a project team in place to discuss respective roles and responsibilities (such as communication with the acquiring bank, communication with service providers, specification of technical changes, establishing training needs, and so on).

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

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

Some merchants may prefer to engage a Qualified Security Assessor from the outset. Others may prefer to conduct the initial scoping work internally, and to bring in a Qualified Security Assessor at a later stage for a more thorough review.



7.0 Step Five: Select your validation option

- 7.1 About the annual on-site audit
- 7.2 About the quarterly Vulnerability Scan
- 7.3 About the annual Self-Assessment Questionnaire



7.0 Step Five: Select your validation option

Depending on the scale of your business and the configuration of your card acceptance systems, there are different ways in which to test and validate your compliance with PCI DSS.

- > Larger Merchants (that is, those which typically process more than 6,000,000 Visa or Mastercard transactions per year) are required to:
 - Complete an annual on-site audit (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)
 - Complete a quarterly Vulnerability Scan (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)
- > E-commerce Merchants (which typically process between 20,000 and 6,000,000 Visa or Mastercard transactions per year) are required to:
 - Complete an annual Self-Assessment Questionnaire (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)
 - Complete a quarterly Vulnerability Scan (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)
- > Other Merchants (POS or Mail/Telephone Merchants) which typically process less than 6,000,000 Visa or Mastercard transactions per year) are recommended to:
 - Complete an annual Self-Assessment Questionnaire (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)
 - Complete a quarterly Vulnerability Scan (please see www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity)

Based on its experience with other merchants in your market, your acquiring bank may be able to recommend which of these options is most appropriate for your business.

7.1 About the annual on-site audit

The annual on-site audit is an independent risk assessment, which is generally conducted by a Qualified Security Assessor.

During the audit process, the Assessor will follow a standard testing procedure, built around the 12 PCI DSS requirements www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

A copy of the complete Security Review Procedures that an Assessor will perform during an on-site audit can be accessed at www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.

If you currently use a security consultant to perform any on-site reviews on your behalf, it is possible that they could also conduct the PCI DSS on-site audit. Similarly it may be possible for the audit to be conducted by your own personnel. Please enquire with your acquiring bank.



7.2 About the quarterly Vulnerability Scan

A Vulnerability Scan ensures that your systems are protected from the threat of 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.

Regular quarterly scans are necessary to ensure that your systems and applications continue to afford adequate levels of protection. If the scans identify any vulnerabilities, a follow-up scan will be necessary to ensure that the remediation was successful.

7.3 About the annual Self-Assessment Questionnaire

The Self-Assessment Questionnaire is a free, confidential tool that can be used to gauge your level of compliance with PCI DSS.

The Self-Assessment Questionnaire is an online tool which is made up of a series of 'yes'/'no' questions. Once it has been completed, you will have made a good assessment of your assessed risk level. If the assessment indicates that remediation work is needed, you will need to undertake this work in order to comply with PCI DSS.

Most businesses will want to download the printable version of Self-Assessment Questionnaire (available from www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity) before submitting their answers online. This means that questions can be distributed to the appropriate people within the organisation in order to obtain accurate answers.

In order to validate your compliance with PCI DSS, you will need to pass the self-assessment questionnaire. To pass the questionnaire you should be in a position to answer all questions positively or indicate, when permitted, that they do not apply to you. You will need to incorporate the questionnaire into your normal business routines, and ensure it is repeated yearly.

You may wish to complete the entire audit or Self-Assessment Questionnaire process internally, or you could work with a Qualified Security Assessor to manage it (or advise on aspects of it) on your behalf.



8.0 Step Six: Plan and implement remediation



8.0 Step Six: Plan and implement remediation

Once you have decided on your validation option, it will generally be necessary to conduct a more thorough gap analysis and develop a comprehensive remediation plan to bring you into compliance with PSI DSS.

Again, this can be done internally, or you may choose this stage to enlist the services of a Qualified Security Assessor. Bringing in an Assessor at the early stages can add significant value to the project. In particular, they may be able to provide a knowledgeable perspective on the suitability of your remediation activities and planned timelines.

At this stage, you should also task the individuals in your project team with specific remediation activities, and agree acceptable timelines. Some of the necessary remediation activities may be reliant on a third party or vendor becoming compliant, whilst others can be undertaken internally.

It is recommended that you commence any remediation work on your own systems as quickly as possible. From a project management perspective it may seem more appropriate to wait until such time as any service providers become compliant. However, it should be remembered that the underlying purpose of this exercise is not to certify compliance, but to achieve it and maintain it.

By doing whatever you can as soon as you can, you will be taking a vital step forward in protecting your business (and your customers) against the risk of data compromise.



9.0 Step Seven: Certification



9.0 Step Seven: Certification

In order to go through the final certification stage, it will be necessary for you to:

- > Complete the remediation on any and all of the systems which are under your control
- > Confirm that any and all of your service providers have achieved full compliance (and for their compliant products and services to have been implemented within your own card acceptance systems)

With this done it will be time for you - either independently or jointly with a Qualified Security Assessor - to conduct the on-site audit (or complete the Self Assessment Questionnaire).

The Qualified Security Assessor will discuss the outcome of the audit with your organisation, and certify your achievement of compliance if the audit has been successful.

You can then report back to your acquiring bank, confirming that you have achieved compliance. The acquiring bank will, in turn, report your status to Visa and any other payment card systems.

As well as being adequately protected against all associated business risks, you will be able to confirm your compliance in your own messaging and marketing collaterals.

In order to remain compliant it will be necessary to conduct an audit annually, and to repeat the vulnerability scans quarterly.



10.0 Staying compliant



10.0 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 data security 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 order to remain compliant it will be necessary to conduct an audit annually, and to repeat the vulnerability scans quarterly. In addition, 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

As well as ensuring that you own systems and processes remain compliant, you should also ensure that your service providers continue to be compliant. One way to do this is to ensure that explicit clauses are incorporated into your contracts and terms and conditions which bind them to compliance with PCI DSS.

As a matter of business policy, it is also advisable to avoid dealings with any service providers or business partners that are not working towards compliance, or that are unwilling to comply with PCI DSS.



11.0 We are here to help



11.0 We are here to help

For any further information relating to PCI DSS (or any other aspect of your payment card acceptance arrangements), you can visit 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 your first point of contact should be your acquiring bank. Alternatively you can contact Visa direct at datasecuritystandards@visa.com.

