

# Account Information Security

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

## A guide for Members



# Contents

<b>1.0</b>	<b>Introduction</b>	<b>02</b>
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
<b>2.0</b>	<b>Understanding the implementation process</b>	<b>06</b>
2.1	Helping your business with the implementation	06
2.2	An overview of the implementation process	07
<b>3.0</b>	<b>Guiding principles</b>	<b>09</b>
<b>4.0</b>	<b>Addressing your own systems</b>	<b>11</b>
4.1	Step One: Establish how PCI DSS relates to your own business	11
4.2	Step Two: Map out the data flows in your business	11
4.3	Step Three: Conduct a gap analysis and plan your remediation activity	12
4.4	Step Four: Remediation and certification	12
<b>5.0</b>	<b>Working with service providers</b>	<b>14</b>
5.1	Step One: Identify all service providers and ascertain their compliance status	14
5.2	Step two: Identify and address non-compliant service providers	14
5.3	Step three: Notify Visa of non-compliant service providers	14
5.4	Step four: Remediation activity	15
5.5	Step five: Certification	15
5.6	Step six: Implementing a compliant solution	15
<b>6.0</b>	<b>Assisting your merchants with their compliance</b>	<b>17</b>
6.1	Step one: Familiarising your merchants with PCI DSS	17
6.2	Step two: Establishing the way that different merchants process data	17
6.3	Step Three: Conducting a gap analysis and scoping the project	18
6.4	Step Four: Selecting the validation option	19
6.5	About the annual on-site audit	19
6.6	About the quarterly Vulnerability Scan	20
6.7	About the annual Self-Assessment Questionnaire	20
6.8	Step Five: Plan and implement remediation	20
6.9	Step Six: Certification	21
<b>7.0</b>	<b>Staying compliant</b>	<b>23</b>
<b>8.0</b>	<b>We are here to help</b>	<b>25</b>



# 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

Account Information Security (AIS) is the name for Visa’s compliance programme with respect to card account data security.

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 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 other major international payment card systems.

As an acquirer, PCI DSS should be a matter of priority for your own business. Indeed, under the terms of the Visa International Operating Regulations, an acquirer is held responsible, not only for the security of its own systems, but also for the systems of its entire merchant network, and of any agents or third party service providers.

Visa has created a set of tools and resources to make it as straightforward as possible for you to implement the PCI DSS:

- > Within your own systems
- > Within your merchants’ systems
- > Within the systems of any third party service providers

By implementing these standards, all parties become compliant with our own AIS programme, and they automatically meet the requirements and recommendations set out by other major 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 international payment card schemes and their acquiring banks.

Full details can be accessed at [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

## 1.3 Who does it apply to?

PCI DSS applies to every acquiring bank, every merchant that accepts payment cards, and every service provider which stores or transmits card or transaction data on their behalf.

Within the Visa International Operating Regulations, Visa has specified that all acquiring banks must be compliant.

Acquirers are also responsible for ensuring that:

- > All of the merchants they represent are compliant
- > All third parties are compliant

You should note that, from the perspective of the Visa International Operating Regulations, your organisation is ultimately responsible for all service providers (irrespective of whether you have a direct relationship with them, or your merchants have a relationship with them).

Such service providers may include:

- > Resellers
- > Till vendors
- > EPOS vendors
- > Software application providers



- > Payment service providers
- > Payment processing bureaus
- > Data storage providers
- > Web hosting providers
- > Shopping cart providers
- > Software vendors
- > Miscellaneous third party agents

Read though this guide for more details.

## 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 its customers and safeguard any information relating to them.

Irrespective of the requirements stipulated in the Visa International Operating Regulations, PCI DSS therefore makes sound business sense for every acquiring business.

In particular, it can:

- > Identify any risks in the way you store or transmit any cardholder account data
- > Provide a clear path of action and remediation to address any risks
- > Ensure that your service providers do not put your business at risk
- > Demonstrate to your merchants and their business partners that you are serious about their 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 and techniques 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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

PCI DSS minimises the 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 own business
- > The extent and nature of your merchant network
- > The number and type of service providers contracted by you and/or your merchants

Visa is eager to help you through the implementation process.

This document is intended to:

- > Guide you, step-by-step through the process
- > Give you easy, immediate access to all related documentation
- > Provide details of those service providers which are already compliant or are working towards compliance
- > Provide details of Qualified Security Assessors

If you have any questions, please contact us at [datasecuritystandards@visa.com](mailto:datasecuritystandards@visa.com).



## 2.2 An overview of the implementation process

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

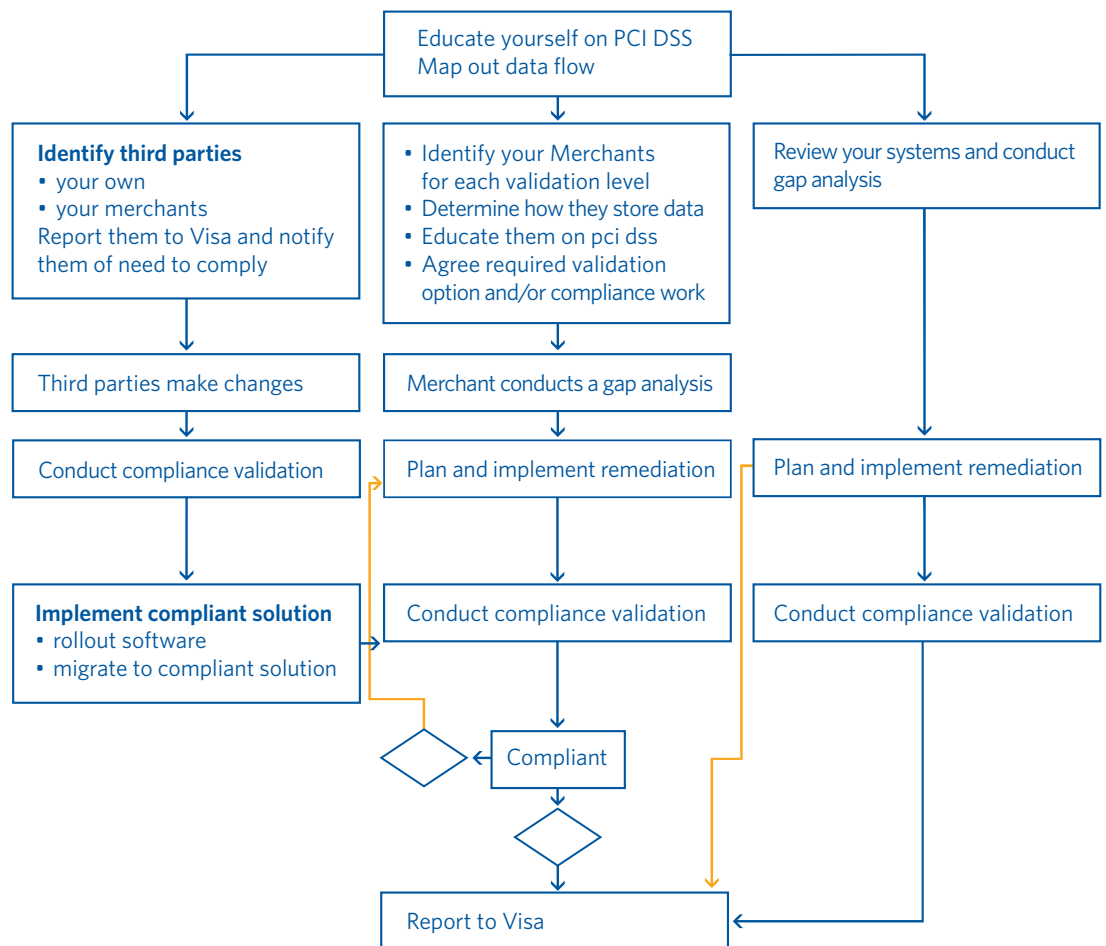
As this diagram suggests, PCI DSS entails three inter-related strands of work for you business, namely:

- > The compliance of your own business
- > The compliance of your merchants
- > The compliance of all service providers

Clearly, the first step is to familiarise yourself with the specific details of PCI DSS, which can be accessed at [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

This should give you an initial understanding of the scale of the project, help you to factor it into your business planning processes, and begin to consider the level of resource which will be required.

### Step by Step Implementation for Acquirers



## 3.0 Guiding principles



## 3.0 Guiding principles

When planning for your PCI DSS compliance programme, or when considering any upgrade to 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 any of your merchants to store such data, it should always be discouraged. Also, if your merchants do not store any data, it will not be necessary for them 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 which are not compliant with PCI DSS will expose your own business, your merchants and their service providers to a significant (and entirely unnecessary) level of risk.

Visa is actively working with a wide range of vendors and service providers to ensure that systems are available 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

You are strongly advised to ensure that solutions of this type are deployed by your entire merchant network. This will ensure that you and all of your merchants benefit from the optimum level of protection.



## 4.0 Addressing your own systems

- 4.1 Step One: Establish how PCI DSS relates to your own business
- 4.2 Step Two: Map out the data flows in your business
- 4.3 Step Three: Conduct a gap analysis and plan your remediation activity
- 4.4 Step Four: Remediation and certification



## 4.0 Addressing your own systems

Although Visa does not mandate any specific validation or certification processes, we do mandate that all acquirers should be compliant with PCI DSS.

We also recommend that, as well as implementing PCI DSS within your business, you should also conduct some form of validation.

This could take the form of an internal audit conducted by your internal IT department or of an external audit conducted by a Qualified Security Assessor - that is, a specialist auditor, certified by Visa and/or MasterCard to assist in PCI DSS compliance.

It is possible that Visa may mandate validation or certification at some point in the future.

Below is a step-by-step guide to establishing PCI DSS within your own business.

### 4.1 Step One: Establish how PCI DSS relates to your own business

Implementing PCI DSS within your own business 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 risks

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

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 minimum level of protection.

### 4.2 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. The immediate priority of this team should be to analyse the precise manner in card payments are processed within your systems, 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 nature of your business, it is likely that some such systems will be under the control of a third party service provider or vendor (such as a payment gateway provider).

Again, irrespective of where and how account data is stored and transmitted, your organisation is (from the perspective of the Visa International Operating Regulations) is ultimately responsible.



## 4.3 Step Three: Conduct a gap analysis and plan your remediation activity

Having mapped out the data flows within your business, you should have identified any of your own systems which 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, 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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

## 4.4 Step Four: Remediation and certification

Working alone 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.

If you have chosen to work with a Qualified Security Assessor, it is recommended that they independently audit and certify your business. This will validate that your systems are indeed compliant with PCI DSS.

Alternatively, you should ensure that a full testing and self-certification exercise is conducted by your own project team.

Having successfully completed the certification (or self-certification) phase you will be ready to report your successful compliance to Visa.

Under the terms of the Visa International Operating Regulations, it will be necessary to confirm your compliance to Visa on an annual basis. To ensure that you remain compliant, you should therefore conduct a regular audit or certification and incorporate it within your routine business processes.



## 5.0 Working with Service Providers

- 5.1 Step one: Identify all service providers and ascertain their compliance status
- 5.2 Step two: Identify and address non-compliant service providers
- 5.3 Step three: Notify Visa of non-compliant service providers
- 5.4 Step four: Remediation activity
- 5.5 Step five: Certification
- 5.6 Step six: Implementing a compliant solution



## 5.0 Working with Service Providers

The second stream of work involves liaison with those providers who are contracted directly to your own business and/or those who work on behalf of your merchants.

Again, as an acquirer, you are ultimately responsible for the activity of any such service providers. It is therefore incumbent on you to verify that all such service providers comply with PCI DSS.

### 5.1 Step one: Identify all service providers and ascertain their compliance status

The first step is to identify all service providers who work on behalf of your own business and/or your merchants.

Given that cardholder data security is such an important issue for the payment card industry, it is likely that all such 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.

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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

### 5.2 Step two: Identify and address non-compliant service providers

If you identify any service providers do not appear on this listing, it will be necessary for you to ensure that they take action. In particular, it is recommended that compliance with PCI DSS should become a contractual requirement for your own service providers. Additionally you should request that your merchants include such a clause in all contracts with any service providers.

### 5.3 Step three: Notify Visa of non-compliant service providers

As part of our Account Information Security programme, Visa assists service providers through the compliance process. We therefore ask that you inform us of any non-certified service providers, so that we can begin to work with them.

During the compliance process it is possible that we may seek your support and intervention. We may, for example, ask you to put additional pressure on a particular service provider (for example, by leveraging your merchants' relationship with them, to ensure that they become compliant within a reasonable timeframe).



## 5.4 Step four: Remediation activity

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

The service provider will need 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.

Please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://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 remediation activity.

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

## 5.5 Step five: Certification

Once the agreed changes have been made, the service provider will be ready to go through a formal audit and 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 report.

Visa may also request to see the full audit document, which contains full details of the audit undertaken.

Please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity) for a copy of the standard audit document.

If the service provider is a software vendor, its products will be audited according to the Payment Application Best Practices. In all other instances, the service provider will be audited according to PCI DSS.

## 5.6 Step six: Implementing a compliant solution

Once a service provider confirms that its own systems are compliant with PCI DSS, all aspects of your card acceptance operations which the service provider manages will be deemed as compliant.

Even after a service provider is certified as compliant, the merchants they work with may still have to do work to also become compliant, and to certify their compliance if required.

This applies if the merchant has direct access to card data.

Similarly, for software vendors, 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.



## 6.0 Assisting your merchants with their compliance

- 6.1 Step one: Familiarising your merchants with PCI DSS
- 6.2 Step two: Establishing the way that different merchants process data
- 6.3 Step Three: Conducting a gap analysis and scoping the project
- 6.4 Step Five: Selecting the validation option
- 6.5 About the annual on-site audit
- 6.6 About the quarterly Vulnerability Scan
- 6.7 About the annual Self-Assessment Questionnaire
- 6.8 Step Six: Plan and implement remediation
- 6.9 Step Seven: Certification



## 6.0 Assisting your merchants with their compliance

Given the issues relating to the security of cardholder account data, it has become necessary for all merchants (regardless of the scale or the nature of their business) to become PCI DSS compliant.

Larger or more sophisticated merchants will probably already be aware of PCI DSS and its implications for their business. However they will require your help in putting together an action plan for compliance and in bringing it to completion.

Other merchants are likely to require additional help and support. It may be necessary to educate them on PCI DSS and how it relates to their business. It may also be necessary for you to guide them through the implementation process.

This is regardless of whether they require an audit or any other type of formal certification. All merchants, irrespective of the size or nature of their business still have to comply with PCI DSS.

### 6.1 Step one: Familiarising your merchants with PCI DSS

The first step is to ensure that all of your merchants are aware of PCI DSS and the way it relates to their own business.

As part of this process, it will also be necessary to ensure that all of your account managers and customer support representatives are fully aware of the programme.

In educating your merchants, you may wish to refer them to [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity) where a variety of information and resources is freely available.

It may also be advisable to provide training on data security to your merchants. You could choose to provide this training directly, or it could be sub-contracted to a Qualified Security Assessor.

### 6.2 Step two: Establishing the way that different merchants process data

Once your merchants are familiar with PCI DSS, you should work directly with each merchant to ascertain whether they have access to account data, and whether this data is processed securely.

In particular, each merchant should be able to provide you with details of how account data flows between the different systems within their own organisation, which of these systems store any data, and which third parties (if any) manage data on their behalf.



In order to conduct this exercise effectively, a merchant will need to understand that all aspects of its business (including e-commerce, mail order/telephone order and face-to-face sales channels) must be compliant. This principle applies even in cases where Visa only requires formal validation for one aspect of a merchant's business.

Since your business is ultimately responsible in the case of any compromise, you should ensure that all data flows are mapped out with extreme care, and that no links in the chain are overlooked.

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 the direct control of the merchant

Depending on the scale and nature of each merchant's 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).

Based on this analysis, it will be necessary for you to support the merchant through two streams of actions:

- > Any actions which are necessary to ensure that all service providers comply with PCI DSS (see previous section for details)
- > Any actions which are necessary to implement PCI DSS within the merchant's own business (Step 3 to Step 9 below)

## 6.3 Step Three: Conducting a gap analysis and scoping the project

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

These systems should be treated as their primary focus.

During these initial stages of the implementation process you should work with the merchant in order to:

- > 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 advise the merchant on 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](http://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.



Visa is not in any way prescriptive regarding your choice of Qualified Security Assessors. Instead, we believe that you are in the best position to make a recommendation to your merchants given your knowledge of their business.

## 6.4 Step Four: Selecting the validation option

Depending on the scale of each merchant's business, and the configuration of their card acceptance systems, there are three different ways in which to test and validate their compliance with PCI DSS.

- > Larger Merchants (that is, those which typically process more than 6 million Visa and/or MasterCard transactions each year) would be expected to:
  - Complete an annual on-site audit (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))
  - Complete a quarterly Vulnerability Scan (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))
- > Larger e-commerce merchants (that is, those which typically process between 20,000 and 6 million Visa and/or MasterCard transactions each year) would be expected to:
  - Complete an annual Self-Assessment Questionnaire (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))
  - Complete a quarterly Vulnerability Scan (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))
- > Other Merchants (that those which typically process less than 6 million Visa and/or MasterCard transactions each year) are recommended to:
  - Complete an annual Self-Assessment Questionnaire (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))
  - Complete a quarterly Vulnerability Scan (please see [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity))

Based on your own experience within your market, you may be in a position to recommend which of these options is most appropriate for a particular merchant.

## 6.5 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.

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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

If the merchant currently uses a security consultant to perform any on-site reviews on its 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 the merchant's own personnel.



Given your own experience of particular merchants you may be in the best position to advise them on the most appropriate route.

## 6.6 About the quarterly Vulnerability Scan

A Vulnerability Scan ensures that a merchant's systems are protected from external threats (such as hacking or malicious viruses). The scanning tools test all of their 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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

Regular scans are necessary to ensure that the merchant's 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.

## 6.7 About the annual Self-Assessment Questionnaire

The Self-Assessment Questionnaire is a free, confidential tool that can be used to gauge the merchant's 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, a merchant will be able to make a good assessment of their risk exposure.

Most businesses will want to download the printable version of Self-Assessment Questionnaire (available from [www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity](http://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 comply with PCI DSS, merchants will need to provide positive answers to each of the questions or to indicate (where this is a valid option) that they do not apply to their business.

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

## 6.8 Step Five: Plan and implement remediation

Once a decision has been made on the validation option, it will generally be necessary for the merchant to conduct a more thorough gap analysis and develop a comprehensive remediation plan.

Again, this can be done internally, or the merchant could 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 the merchant's remediation activities and planned timelines.

Similarly, Visa may be able to comment on remediation activities and timelines.

At this stage, the merchant should also task the individuals in their 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.

You should always recommend that the merchant should commence any remediation work on its 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 they can as soon as they can, the merchant will be taking a vital step forward in protecting its business (and its customers) against the risk of data compromise.

## 6.9 Step Six: Certification

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

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

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

The merchant should then report back to you, confirming that you have achieved compliance. You should, in turn, report the merchant's status to Visa and any other payment card systems.

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



## 7.0 Staying compliant



## 7.0 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 merchants and service providers) 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 (and advise your merchants to do the same).

For example, you/they should:

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

As well as ensuring that your own systems and processes remain compliant, you should work with your merchants to ensure that service providers also continue to be compliant.

A good way to facilitate this is to ensure that explicit clauses are incorporated into all contracts and terms and conditions which bind them to compliance.

You should also ensure that, as a matter of business policy, your merchants should avoid dealings with any service providers or business partners that are not working towards compliance, or that are unwilling to abide by PCI DSS.



## 8.0 We are here to help



## 8.0 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](http://www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity).

We are fully committed to making it as easy and straightforward as possible for you to implement PCI DSS within your own business - and also to assist you in extending it to your entire merchant base and the wider service provider community.

If you have any specific questions, please do not hesitate to contact us at [datasecuritystandards@visa.com](mailto:datasecuritystandards@visa.com).

