

# Compliance in the Payment Card Industry



# Contents

Introduction	01
Requirement of the PCI DSS	01
PCI DSS regulations	
Level of PCI compliance	03
Steps to achieving and maintaining PCI DSS Compliance	03
Build a roadmap	03
Measured execution of each milestone project	03
Due diligence	03
Validation	03
Education	03
Assess performance and risk	03
Build a secure architecture	03
Develop appropriate storage, retrieval and disposal processes	04
Proactively monitor and manage the network	04
Customer data security is more than a compliance project	04
Conclusion	04
Further reading	04
Where do you start? Dimension Data's offerings	04
Our track record	04
Recommended assessments:	04
Malware Assessment Services	04
Firewall Assessment Services	05
Vulnerability Assessment	05
Wireless Security Assessment	06
PCI Self-assessment Questionnaire Assistance	06
Secure IP Telephony Assessment	06
Data Loss Prevention Assessment	07
Security Management Services	07
Technology Lifecycle Management Assessment Service	07

Whether you are a retailer, service provider or a bank, if you process any form of credit card data you need a thorough understanding of Payment Card Industry compliance. This guide aims to provide you with a clear and comprehensive understanding of the Payment Card Industry Data Security Standard requirements and offer you practical guidance to achieving and maintaining compliance.

### Background to the Payment Card Industry Data Security Standard

According to research from Retail Systems Research and Cisco, retailers identify customers within their databases individually 86% of the time. Additionally, detailed transactional data is linked to specific customers by 59% of surveyed retailers, and 29% augment those customer profiles with demographic information. Customer 'payment' data (for example, account or identification numbers) is stored for use in subsequent transactions, according to 45% of the total respondent group.

As businesses move towards more customer-centric offerings, retailers and suppliers are using customer-specific data for business analytics, employing new technologies, and sharing that data with business partners. A significant amount of personal data is collected and stored, from transaction data captured in stores, to contact centres and online offerings.

Credit cardholder information is increasingly becoming a target for cyber-thieves. Recent research indicates that only 25% of retailers know that they've suffered a breach before the acquiring banks or the payment network processors detect it. It can be as long as 12-18 months before evidence of a breach is detected, typically from counterfeit credit card transactions. This creates significant risk for retailers, as they are not only penalised for the actual card numbers that are abused, but also all account numbers that have been exposed by the security compromise. Penalties and other losses associated with an actual security compromise can be grave.

The PCI Security Standard Council drafted the Data Security Standard (PCI DSS) in response to these issues. This standard applies to any organisation that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data. As of late 2007, any organisation that accepts payment card transactions must comply with the standards.

The primary goal of the PCI DSS is to secure cardholder transaction and personal data. While credit card processing companies have made progress in ensuring compliance to the standard, compliance measures must be implemented beyond just retail points of sale. Today, data is processed, stored and transported using a wide range of wired and wireless networks and devices that span the entire organisation. From storefront and web store to the company data centre – even to the links that connect your company to payment processors – there are measures that must be in place to address compliance requirements.

### Requirements of the PCI DSS

The DSS specifies 12 compliance requirements, organised into six related groups known as 'control objectives'. A single violation of any of these requirements can render an organisation non-compliant. Each non-compliant incident results in fines, suspension and revocation of card processing privileges.

### PCI DSS regulations

#### Build and maintain a secure network

**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data

To comply with this standard, you need to demonstrate that your firewalls are correctly maintained and independently tested. This presents a challenge as more than 99% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.

**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

A firewall is a fundamental part of network security. You should be able to prove that the appropriate steps have been taken both during the implementation phase and again thereafter, during change management. Again, it's about process and people – not simply products that provide a technical solution.



**Requirement 3:** Protect stored cardholder data

All stored data must be encrypted. This can be achieved relatively quickly, using any one of several commercially available tools. Certain information should never be stored, e.g. PIN numbers and the full details on a card's magnetic strip.

**Requirement 4:** Encrypt transmission of cardholder data across open, public networks

The highly distributed nature of today's supply chain and service relationships creates a dependency on public networks. Be sure that your wireless network and remote access solutions are correctly configured. Most other transmissions can be configured to use VPN software such as SSL and IPsec. Mapping the route of the transmission will quickly reveal where encryption is required.

#### **Maintain a vulnerability management programme**

**Requirement 5:** Use and regularly update anti-virus software

Cyber criminals' capabilities to break into networks are increasing at an alarming rate. Although organisations have anti-virus software to safeguard against attacks, they need to ensure that the frequently published updates reach every device. This can be difficult as it requires a centralised view of mobile devices coming into the corporate network.

Intrusion detection or prevention systems do not need regular patching (unlike anti-virus software). You should install these systems on devices storing credit card details to ensure maximum protection. Alternatively, to ensure that all anti-virus software is patched, draw a comparison between the total number of devices connected and the number that is being updated.

In addition, Network Access Control can ensure that AV patches have been applied to individual workstations as they attempt to connect to the network.

**Requirement 6:** Develop and maintain secure systems and applications

In an increasingly complex and integrated world of applications, middleware and servers, maintaining a comprehensive view of security is an ongoing challenge.

Review the alerts of all the software vendors used in your systems and apply their patches methodically. If the application has been customised, patching can be difficult as the extended code may be affected by the patch. In this situation, the application needs to be properly tested to establish whether the application is vulnerable and a plan put in place to address any issues. In addition, organisations with customised applications may consider conducting a vulnerability assessment.

#### **Implement strong access control measures**

**Requirement 7:** Restrict access to cardholder data by business need-to-know

Access to critical data should be restricted and recorded. For example, access should only be given to employees working with credit card details. Remember, it is possible to allow administrators and support staff appropriate access to the services they need without them seeing sensitive data through the use of encryption and directory access controls. It is important to note, however, that all access should be documented and regularly audited.

**Requirement 8:** Assign a unique identification to each individual with computer access

Assigning a unique identification to each individual who has access to a computer will ensure that actions taken on critical data and systems are performed by, and can be traced to, known and authorised users. All remote users should access the data via two factor authentications (e.g. tokens or smartcards). Inactive devices should be logged off after a period of inactivity.

**Requirement 9:** Restrict physical access to cardholder data

Physical access to the building should be gained via a reception area, where all visitors and contractors are required to sign in. All devices that store or could store credit card details need to be located in a secure environment and server rooms should be locked and CCTV installed. Be sure to restrict access to both wireless and wired network components. Increasingly, these physical security services can be integrated and delivered via the IP network to deliver closer monitoring and reporting. For example, IP CCTV coupled with the use of smartcards with proximity detection for physical access as well as network access.

#### **Regularly monitor and test networks**

**Requirement 10:** Track and monitor all access to network resources and cardholder data

The logs of the network and appropriate devices should be recorded and analysed for anomalies. The logs need to be stored so that legitimate access, intrusions and attempted intrusions can be tracked. The logs must be available as evidence in case of a breach.

**Requirement 11:** Regularly test security systems and processes

If your organisation is affected by PCI DSS regulations you should conduct regular vulnerability scans to expose weaknesses that could potentially be exploited. In addition, it is advisable to conduct internal and external vulnerability scans in the event of significant changes to the network, device operating systems or applications. All scans need to be checked against a baseline and the results recorded. Deal with any issues through a remediation plan and prioritise activities according to the potential risk associated with each area.

#### **Maintain an information security policy**

**Requirement 12:** Maintain a policy that addresses information security

A clear and comprehensive security policy ensures employees know what is expected of them. For example, you should send regular reminders to all employees regarding the sensitivity of data and their responsibilities with respect to its protection.

## Levels of PCI compliance

To help organisations adopt the PCI DSS, the PCI Security Standard Council has identified four different levels of PCI compliance and the actions that need to be undertaken within each:

**Level 1** – aimed at large businesses that process in excess of 6,000,000 credit card transactions per year. Organisations that fall into this category are required to have an annual on-site security audit, as well as quarterly system perimeter scans.

**Level 2** – aimed at organisations processing 150,000 to 6,000,000 credit card transactions per year. Organisations that fall into this category are required to provide a quarterly system perimeter scan and complete an annual compliance questionnaire.

**Level 3** – aimed at organisations that process 20,000 to 15,000 credit card transactions a year. Organisations that fall into this category are required to provide a quarterly scan and complete an annual compliance questionnaire.

**Level 4** – aimed at organisations that process less than 20,000 credit card transactions a year. While there is no contractual obligation to provide scans or complete questionnaires, it is recommended that organisations that fall into this category conduct annual scans of their perimeter, at a minimum.

## Steps to achieving and maintaining PCI DSS Compliance

The PCI DSS is regularly updated by the PCI Security Standard Council. It is important therefore, that you ensure that you keep abreast of any changes.

### Build a roadmap

To achieve compliance you need to determine your existing status and build a roadmap to achieve your future goals. Consider including the following best practice milestones within your roadmap:

Logging and monitoring are **key technology enablers** in ensuring a **secure network**, as are frequent **network penetration tests**.

### Measured execution of each milestone project

Each project should have an agreed start and end date and should be assigned the appropriate resources within your business to ensure successful implementation. Milestone projects should also be assigned with a project owner/ manager who has overall responsibility for providing regular updates on the project status and identifying, documenting and mitigating any risks associated with the successful implementation of the project. Ensure that senior management has visibility of the compliance effort and status.

### Due diligence

Task a resource within the IT department, or if appropriate, the entire business, with keeping abreast of new threats and any impending changes/additions to the PCI DSS requirements. This will ensure that you can adapt your roadmap and milestone projects accordingly.

### Validation

Validation should be an ongoing effort with quarterly and annual tasks, including onsite assessments and audits, self-assessment questionnaires and quarterly security scanning of all internet-accessible systems and applications. Not only will this allow you to test the success of implemented projects and their ability to meet each of the 12 PCI DSS requirements, but also provide confidence when it comes to being PCI DSS audited. After achieving full PCI compliance, regularly assess your security policies and scan your infrastructure to ensure that you remain compliant and secure.

### Education and awareness

The PCI DSS has the potential to affect business operations at senior management level. Therefore, be sure to keep senior management or IT and line-of-business management and technical employees informed on how PCI affects their areas of influence.

Of course, the major responsibility lies with the IT department, where operational capabilities may vary as required by DSS. Take practical steps to create awareness within this group. Education can include PCI DSS awareness workshops, e-learning or other self-paced training during the early stages of implementing your roadmap.

### Assess performance and risk

Be sure to conduct a thorough assessment of where personal account data is held. Only then can you fully understand where weaknesses may lie and how to address them. Upon completion of the assessment, map PCI mandatory requirements and government regulations to your current business processes and systems. (This is an important step since mandates and regulations may overlap.) You will then be in a position to prioritise changes to both operational processes and systems.

### Build a secure architecture

Ideally, all consumer-specific data – not just payment data – should be encrypted. While the PCI DSS has very specific requirements regarding encryption of personal account numbers, forward-thinking organisations should view this as an opportunity to remain a step ahead of industry mandates and potential legislation. While regulations such as the Sarbanes Oxley Act (SOX) and the PCI DSS, are obvious points of reference, consider if broader security and privacy issues could exist, based on the types of data you currently collect, and secure it accordingly.

### **Develop appropriate storage, retrieval and disposal processes**

It is not uncommon for retailers of all sizes to retain sensitive data for more than two years. Organisations should adopt a systematic approach to destroying transactional data once the business need for keeping it has passed.

### **Proactively monitor and manage the network**

While larger organisations are generally more focused on ensuring that sensitive data remains secure throughout the lifecycle of business applications, businesses of all sizes find tracking and monitoring access to the network a challenge. This can be mitigated by enacting clear policies of network administration, but again, can only be accomplished once you have a clear and comprehensive understanding of your current practices. Logging and monitoring are key technology enablers in ensuring a secure network, as are frequent network penetration tests.

### **Customer data security is more than a compliance project**

Since customer data security ultimately is an issue that can affect the company's brand and its ability to execute on its business strategy, it should make a regular appearance on the board meeting agenda.

Organisations typically deploy a host of devices and software versions into their infrastructures over a number of years. It is therefore essential to understand your existing network infrastructure and all its components, how current and secure your network components are, and whether the infrastructure is suitable for both existing business requirements and future plans.

It is imperative that organisations build a platform to achieve and maintain PCI compliance. Organisations who keep their executives informed regarding the organisation's current security practices, where dangers lie, and how their practices need to adapt, have a far greater chance of defining the financial risk that surrounds non-secured customer-specific data and securing appropriate executive-level commitment and investment.

Dimension Data's service provides a **unique industry approved solution** to answer these questions and to **maintain the integrity and effectiveness** of your IT security on an ongoing basis.

#### **Conclusion**

Simply securing the physical connections inside and outside your network is not enough to ensure compliance. Without an appropriate means to control your data, you will put your organisation at risk.

A centralised control framework will enable you to effectively implement policies while providing a link to business controls, including controls over financial reporting. It helps protect sensitive information from unauthorised disclosure, safeguards the accuracy and completeness of information, ensures that information and vital IT services are available when required, and provides information and services with a high level of efficiency.

#### **Further reading**

#### **Where do you start? Dimension Data's offerings**

Dimension Data has significant experience in addressing the security issues faced by businesses today. Our experts include technical engineers, security consultants and BSI Lead Auditors. Their certifications include CISSP, CISM, CCSA, CCSE, RSA, QSA and SANS GIAC.

#### **Our track record:**

- More than 5,000 security clients around the world
- Over 10,000 product implementations successfully completed
- In excess of 5,000 consulting engagements worldwide
- We have formed solid relationships with leading security vendors, including Microsoft, Cisco, Blue Coat, Check Point, RSA, McAfee and Nokia, as well as with various PCI specialists

- We have conducted in excess of 90 CxO Security Assessments around the world
- Dimension Data is a PCI Qualified Security Assessor, currently certified to operate in Europe

To meet the key PCI DSS requirements, Dimension Data recommends that your business conducts regular assessment reviews. A series of assessments can determine your current status and enable you to conduct a gap analysis of your 'to be' state. Your 'to be' state should align fully with the 12 key PCI DSS requirements.

Recommended assessments:

#### **Malware Assessment Services**

**Malware Assessment Services address the following requirements of the DSS:**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 11: Regularly test security systems and processes

#### **Malware Existence Assessment**

This consultative service tests the network and the devices on it for malware, without the need to install software on devices. The assessment does not affect your existing anti-virus software.

#### **Anti-virus Performance Assessment**

Anti-virus software and their management tools change on a regular basis. Often times, administrators are not trained on how to take advantage of these updates. Through this assessment, Dimension Data determines the performance of the anti-virus and its management software. We ensure that all devices are updated and all the features of the installation have been optimised.

### **Intrusion Prevention Solution (IPS) Requirement Proof of Concept**

IPS is a proactive behavioural analysis tool that follows specific rules. If these rules are broken, the IPS will take predefined steps to stop the activity. The service provides recommendations regarding Host IPS (HIPS) or Network (NIPS) selection, whether to install HIPS on all devices, and determines whether the NIPS sit at the gateway or on critical subnets. Dimension Data recommends the most appropriate vendor offering to meet your requirements. In addition, we implement a Proof of Concept to demonstrate the capabilities against defined criteria.

### **IPS Assessment and Tuning Service**

IPS has a series of rules that are run against known and unknown activities. Applications and operating systems are constantly upgraded and patched and attention therefore needs to be given to the management of the rules. 'Tuning' IPS is critical to the effective operation of the solution and the protection it can provide. Incorrect 'tuning' could block a legitimate application or allow a rogue process. This service reviews the IPS installation and the rules to ensure maximum protection.

### **Firewall Assessment Services**

#### **Firewall Assessment Services address the following requirements of the DSS:**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

### **Firewall Architecture Review**

This review provides you with the opportunity to compare the architecture and operational deployment of your firewall infrastructure to industry best practice standards. Each review encompasses a single firewall management station and the enforcement gateways that it controls.

Dimension Data's consultant scans **internal or external systems** and applications to detect any vulnerabilities which could be **exploited by attackers**. The **Vulnerability Assessment** is non-intrusive and vulnerabilities are not exploited.

### **Firewall Policy and Compliance Review**

This service offers you the opportunity to compare your firewall policy to corporate policy and industry best practice standards. The Compliance Review allows you to compare your firewall policy rules across predefined templates, ensuring that compliance rules are in place.

### **Firewall Threat Performance Review**

Auditing and validating the effectiveness of your network security defences can be a complex, daunting and time consuming task. How do you quickly and easily prove your ability to protect against the latest threats and security evasion techniques, without creating administrative complexity? How do you effectively audit and prove your communication policy for regulatory compliance? Dimension Data's service provides an industry approved solution to answer these questions and to maintain the integrity and effectiveness of your IT security, on an ongoing basis.

### **Vulnerability Assessment**

#### **Vulnerability Assessments address the following requirements of the DSS:**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 11: Regularly test security systems and processes

### **IP Address Footprinting**

As the IT infrastructure of your organisation evolves, the number of active IP addresses grows. With more applications being web enabled, it is important that all external IP addresses are logged and monitored. The speed with which IT evolves can often outpace your ability to keep records up to date. This is why Dimension Data

developed the IP Address Footprinting service as a means to identify and ultimately manage IPs.

### **Vulnerability Assessment (internal and external)**

During a Vulnerability Assessment, a Dimension Data consultant scans internal or external systems and applications to detect any vulnerabilities that could be exploited by attackers. The Vulnerability Assessment is non-intrusive and vulnerabilities are not exploited.

### **Penetration Testing**

Penetration Testing, also known as Ethical Hacking, goes beyond a basic Vulnerability Assessment. With this assessment, you learn which vulnerabilities pose a real imminent threat and represent business critical exposures. During Penetration Testing all discovered vulnerabilities are exploited to reveal their actual impact. A Penetration Test provides an in-depth analysis and covers the maximum potential attack vectors on the infrastructure components.

### **System Security Review (Secure OS)**

In addition to Vulnerability Assessment or Penetration Testing, configuration systems (network and security devices, servers and workstations) can be assessed thoroughly through a hands-on analysis. The targeted systems are assessed for proper hardening and compliance with the latest industry best practice recommendations and standards.

### **Security Infrastructure Study**

Dimension Data reviews your security infrastructure design for compliance with industry best practice principles – e.g. defence-in-depth, segregation between different business flows, the corporate network and DMZ, partners and branch offices. The infrastructure is evaluated according to your current and future business requirements and objectives.

**Penetration Testing** assesses the likelihood of future damage or disruption to the **IT infrastructure** by identifying the risks and by **formulating appropriate changes for improvement.**

### **Wireless Security Assessment**

**The Wireless Security Assessment covers the following requirements of the DSS:**

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

The objective of the assessment is to detect the current strengths and weaknesses of your installed wireless infrastructure and, if you wish, the wireless client systems for both internal and external risks. Penetration Testing assesses the likelihood of future damage or disruption to the IT infrastructure by identifying the risks and by formulating appropriate changes for improvement.

### **PCI Self-assessment Questionnaire Assistance**

**The PCI Self-assessment Questionnaire covers all of the requirements of the DSS, namely:**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

The PCI Self Assessment Questionnaire v1.1, launched in 2008, is designed to simplify the PCI assessment process for merchants who are not required to have onsite assessments.

Depending on the merchant validation type, the questionnaire will differ, e.g. type 1 validation (card-not-present) will only be asked 11 questions whereas a merchant with validation type 4 (merchants with POS systems connected to the Internet with no electronic cardholder data storage) will be presented with 33 questions.

Dimension Data helps you submit a completed questionnaire regardless of the validation method that you use.

### **Secure IP Telephony Assessment**

**The Secure IP Telephony Assessment addresses the following requirements of the DSS:**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Most IP telephony installations are planned with cost and performance in mind, with security further down the priority list. The Secure IP Telephony Assessment service examines your IT and business needs and recommends the most effective security strategy for voice and video traffic. Like all IT threats, IP telephony and video threats are continuously evolving. Assessments should therefore be undertaken on a regular basis.

## Data Loss Prevention Assessment

### The Data Loss Prevention Assessment addresses the following requirements of the DSS:

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

The Dimension Data, Data Loss Prevention Service has been designed as a first step to help you transform your data security posture from reactive to proactive. This service leverages the RSA Data Loss Prevention Suite, which provides automated discovery of unprotected sensitive information and a snapshot of potential exposure. The result is rapid identification of sensitive data on target file shares and desktop infrastructure components. The RSA Data Loss Prevention Risk Advisor Service can also encompass a high-level mapping of business functions to sensitive data, to help determine how sensitive information was originally put at risk.

## Security Management Services

### Security Management Services address the following requirements of the DSS:

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 10: Track and monitor

all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Dimension Data delivers provisioning of firewall, VPN and intrusion prevention system services across Cisco routers, security appliances and switch services modules. Unlike point security products from multiple vendors, which often do not interoperate and can leave vulnerable gaps, Dimension Data provides a comprehensive solution for provisioning, monitoring, mitigation and identity, to keep networks safer, more resilient and easier to operate.

**The Dimension Data Data Loss Prevention (DLP) Service** has been designed as a **first step** to help you transform your **data security posture** from reactive to proactive.

## Technology Lifecycle Management Assessment Service

### The Dimension Data Technology Lifecycle Management Assessment addresses the following requirements of the DSS:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Dimension Data's Technology Lifecycle Management Assessment is a foundation assessment covering the critical aspects of your network. This assessment can establish and ensure PCI compliance by providing a series of discovery assessments, as well as identifying key areas within your security policy that may need to be updated.

We provide a summary of our findings, together with recommendations on how you can make improvements to your current network infrastructure, ensuring that it is both secure and in line with your PCI compliance requirements.

### The deliverables of this assessment include:

- A network infrastructure asset register. This comprehensive list of all devices (hardware and software) on your network helps you to appropriately plan in advance for hardware upgrades.
- An asset support review, which identifies all devices (hardware and software) on your network that do not have a current Cisco support contract.

Dimension Data's Technology Lifecycle Management Assessment is a foundation assessment covering the **critical aspects of your network**. This assessment can establish and ensure PCI compliance by providing a series of discovery assessments, as well as identifying key areas within your security policy that may need to be updated.

- An IOS vulnerabilities review that identifies security vulnerabilities that may exist, helping you to plan upgrades to mediate risks.
- A configuration best practice review, which outlines configuration errors and variations from industry security best practice to improve availability and mean-time-to-repair.
- A Vulnerability Assessment, a non-intrusive examination of your internal and external network systems and network applications to uncover security vulnerabilities.
- Penetration testing that provides in-depth vulnerability information on systems and applications, as well as a controlled analysis of the effectiveness of implemented security mechanisms, including both the technical and organisational incident response capabilities.
- A Firewall Review Service which provides a detailed and documented review of your firewall architecture and policy. Using our global experience of firewall deployments and industry best practice, we highlight the strengths and weaknesses of your existing firewall deployment and where appropriate remediation should be made. We provide analysis of the results and provide advice on how to address the risks for PCI and other forms of compliance
- A Secure Unified Communications Assessment, which leverages our security and IP telephony experience to offer you a Secure IP Telephony Assessment Service conducted on your IP telephony environment. The existing environment is compared against a documented set of guidelines and best practices that we have compiled for securing enterprise IP telephony infrastructures against exploits, fraud, misuse and abuse. With the accelerating use of IP telephony in contact centres as part of a multi-channel retail and customer service model, the implications for PCI compliance are many and varied.

#### References

- <http://www.pcicomplianceguide.org/step2a.html>
- <https://www.pcisecuritystandards.org/>

The existing environment is compared against a **documented set of guidelines and best practices** that we have compiled for **securing enterprise IP telephony infrastructures against exploits, fraud, misuse and abuse**.

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • GHANA • KENYA  
MOROCCO • NAMIBIA • NIGERIA  
SAUDI ARABIA • SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES