Getting up to speed with PCI-DSS

The Claranet no nonsense guide

clara.net
Simplifying IT Management

Be PCI-DSS aware

The Payment Card Industry Data Security Standard (PCI-DSS) has been on the forefront of many retailers' mind for some time. But what's all the buzz about? The standard, which aims to implement effective data security measures for all those dealing with payment cards, has been around for a little while now. However, the quality of implementation of these standards has varied between those who have resources and expertise in-house and those who don't.

This document aims to bring you up to speed with the world of PCI-DSS, giving you a better understanding of what is involved and some quick tips that will keep you on top of staying compliant. It is in a question and answer format to keep straight to the point.

If you are one of those who are struggling to understand how PCI-DSS affects your organisation, then the 7 minutes it takes you to read this document should bring you up-to-speed.

clara.net
Simplifying IT Management

What is PCI-DSS?

The Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including VISA, American Express, Discover Financial Services, JCB International and MasterCard, to help facilitate the broad adoption of consistent global data security measures.

Who needs to be compliant with PCI-DSS?

All organisations that store, process or transmit payment card data are mandated by VISA, MasterCard and the other payment brands to achieve compliance with the PCI DSS Standard. This includes Banks, Payment Service Providers, on-line merchants and face-to-face merchants.

What are the deadlines for complying with PCI DSS?

Compliance is mandated by the payment card brands and not by the PCI Security Standards Council. However, for most merchants, the deadlines for validating compliance with the PCI DSS have already passed. You should check with your acquirer and/or merchant bank to check if any specific deadlines apply to you, based on merchant transaction volume as determined by the card payment brands. All entities that transmit process or store payment card data must be compliant with PCI DSS.

What do I do next?

Depending upon your organisation size and type, either complete a PCI DSS Self Assessment Questionnaire or have a Formal Assessment by a Qualified Security Assessor. If applicable, you will also need to have quarterly vulnerability scanning and send your acquirer a clean scan report every quarter.

Who needs to have an annual Formal Assessment?

Currently it is Merchants who do more than 6 million transactions per year, Payment Service Providers and most Banks.

If we don't need a Formal Assessment, what Self Assessment Questionnaire (SAQ) should we complete?

Your acquirer can help you decide which of the SAQ forms, A, B, C or D you will need to complete, however instructions can be found below, and on the PCI Security Council website at: **https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions**. Once you have completed the SAQ this needs to be sent to your acquiring organisation/Bank.

Why do I need to have quarterly network scanning?

The other requirement of the PCI DSS Standards, as mandated by VISA and MasterCard is for an Approved Scan Vendor to conduct quarterly network scans for you. This is if you host a Payment page, store credit card data electronically (even if it is only momentarily), or transmit payment card data via an API link. Network security scans are non-intrusive inspections that evaluate an organisation's network perimeter for information security vulnerabilities. A clean external network scan must be achieved and the requisite report presented to the relevant acquiring Bank before PCI DSS compliance can be awarded.

Who carries out the scan?

The external network scan needs to be carried out by an 'Approved Scan Vendor', who has been certified as suitable to test security systems for vulnerabilities.

Are there any other tasks mandated by the Payment Brands as part of the PCI DSS Standard?

Yes, organisations completing SAQ D or having annual Formal Assessments will need to have Penetration Testing of their network and internal scanning of devices connected to the internet.

Can you suggest a leading Qualified Security Assessor and Approved Scan Vendor that we can contact?

Yes, Sysnet are one of the leading Qualified Security Assessors (QSA) for PCI DSS. One of the reasons they have become successful in this field is due to their 'Vendor Neutral' status which means that they can independently advise on the effectiveness of your systems and applications.

"Meeting PCI DSS requirements is essential to us and something that we take very seriously. As our current web infrastructure is hosted with Claranet, their compliance is an absolute necessity. If our e-commerce strategy leads us to host more Ann Summers' websites in any of Claranet's data centres, it is reassuring to know that Claranet has already taken care of their PCI DSS compliance status and that this would be something we would not have to cover off ourselves."

Mel Wilcox, Head of IT, Service Delivery - Ann Summers

clara.net
Simplifying IT Management

Are there any quicker ways towards compliancy

Yes, using data centres that are PCI DSS compliant will automatically tick sections 9 and 12 of the standards (see appendix) freeing you from the responsibility of being compliant. Therefore, saving you considerable amounts of time and resources.

So what does Claranet and Sysnet bring to the table?

They can help in the following areas:

- Pre-assessment consultancy services to assist in understanding your PCI requirements (from workshops and seminars to customised training)
- Gap analysis report against the PCI DSS
- Assistance in completing your PCI Self Assessment Questionnaire (Level 2, 3, 4, Merchants)
- Pre-assessment in advance of Formal Assessment (Level 1 Merchants and Service Providers)
- Quarterly vulnerability scans and annual penetration testing of your network
- Independent and vendor neutral remediation advice to support your project
- Formal assessment and report on conformance with the PCI DSS and Issue PCI certificate (Level 1 merchants and service providers)
- Meeting sections 9 and 12 of the security standards through Claranet's PCI DSS compliant data centres
- Communication of the necessary documentation to the appropriate organisations to ensure your compliance is validated

If you would like to find out more about PCI DSS, have a specific question regarding your organisation, or would simply like to comment on this report, please email us at: business@uk.clara.net

Appendix

Merchant Levels as defined by the PCI DSS Standard

Level	Description
1	Any merchant with over 6,000,000 Visa transactions per year. Any merchant that has suffered a hack Any merchant that Visa identified as Level 1
2	Any merchant 1,000,000 to 6,000,000 Visa transactions per year
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year

Self Assessment Questionnaire Validation Type (The numbers 1-5 are not to be confused with Merchant Levels above)

Level	Description	SAQ: V1.2
1	Card-not-present (e-commerce or mail/tele-phone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

clara.net
Simplifying IT Management

PCI-DSS checklist

Build and Maintain a Secure Network
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

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
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

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

About Claranet

www.uk.clara.net

Claranet is a managed services provider with experience in providing IT services since 1996. We provide Network and Hosting services for our customers, enabling them to focus on their core business, not IT management.

The Claranet Group comprises 14 offices, 16 data centres and 550 staff. Our international MPLS core network enables high service levels across 6 European countries and the US. We operate 24-hour network operating centres covering all countries. Claranet is carrier-neutral with a proven track record in delivering services. Our customers include Airbus, Five TV, Amnesty International, DeVere Group and WPA.

Claranet strives for excellence and is committed to delivering the highest quality products and services. Our ISO9001 accreditation, PCI-DSS certification, acceptance into the Telecom Networks Framework Agreement and Microsoft Gold Partner confirms Claranet's position as an expert leader in the IT industry.

About Sysnet

www.sysnet.ie

Established in 1989, Sysnet is a leading provider of information security assurance and payment card industry compliance services worldwide. Sysnet offers a range of professional security services, including its proprietary web based compliance management product Securus, to a wide variety of businesses including Acquirers, International banks and government departments.

Sysnet is a market leader in IS0 27001 services, vulnerability management and audit and assessment consulting through the Payment Card Industry Data Security Standards (PCI DSS) program. Headquartered in Dublin, Sysnet has established relationships with Banks, Service Providers and Merchants in over 30 countries worldwide. All Sysnet engineers are certified information security professionals CISSP

clara.net
Simplifying IT Management