

Embarking on the Payment Card Industry Data Security Standard



The Payment Card Industry (PCI) Data Security Standard has evolved to its current release level of Version 1.2 Release: October 2008. It defines a set of twelve requirements that must be met by each entity in the payment transaction lifecycle. These requirements apply to all system components included in or connected to the cardholder environment. This whitepaper provides the background to the standard, to whom it applies, and how a business should approach compliance with the standard.

How can O-C Group Help?

O-C Group has been founded by a team of Payment Industry experts with decades of experience in the industry. Through their management of the full development lifecycle of mission critical systems, supporting real-time transaction processing, the team is uniquely skilled and experienced to provide your organisation with the knowledge and know how to refine your systems and procedures to prepare your organisation for a PCI audit.



For more information see our web site at <http://www.o-cgroup.com> or contact us at info@o-cgroup.com.

Phone: +353 1 415 1205

Who is affected

The PCI standard applies to all card scheme members, merchants, and service providers that store, process or transmits cardholder data.

A popular mis-conception is that the PCI standard is only applicable to E-Commerce activity. This is not true as all transactions are covered by the standard.

The following table defines the PCI service provider and merchant tiers and the validation required to achieve PCI compliancy.

Group	Tier	Volumes	Validation Required
Service Providers	1	Third Party Processors and Data Storage Entities processing more than 300,000 (Visa) transactions. All compromised entities	On-site Audit Annually Network Scan Quarterly
	2	Service providers processing less than 300,000 transactions annually.	Self Assessment Annually Network Scan Quarterly
Merchants	1	Greater than 6 million transactions per year	On-site Audit Annually Network Scan Quarterly
	2	Between 1 and 6 million transactions per year.	Self Assessment Annually Network Scan Quarterly
	3	20,000 to 1million transactions per year.	Self Assessment Annually Network Scan Quarterly
	4	All other merchants.	Self Assessment recommended Annually Network Scan recommended Quarterly

Impact of non-compliancy

Penalties for non-compliance include fines, operating restrictions and exclusion from the payment system. While the card associations do not fine merchants directly, typically the contract between the acquiring member and the merchant will allow fines to be recovered from the merchant. According to the latest available information, Mastercard are levying fines ranging from \$5000 to \$25,000 (or local currency equivalent) to acquirers for non-compliant merchants depending on the merchant level. Visa expects level 1, 2 or 3 merchants to demonstrate that they are actively engaged in a programme to become compliant. To do this, you need to undertake as a minimum, the following activities:

- Scope the systems that store, process or handle cardholder data
- Carry out a GAP analysis of these systems against PCI DSS requirements
- Contract with a QSA or conduct an internal audit
- Contact an Authorised Scanning Vendor (ASV) to conduct a quarterly vulnerability scan
- Develop a remediation plan to correct issues identified from the GAP analysis.

If a merchant does not complete the above action in a timely manner then Visa will levy the following fines ranging from €5,000 to €25,000 depending on the time period of receiving a notification letter.

Further penalties are applied if the merchant suffers a data compromise.

For Service Providers, the associations have the ability to close down non compliant service providers by revoking their ability to process transactions to the card scheme.

The Requirements

The PCI standard comprises of 6 categories and covers 12 requirements.

Category	Requirement
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect Stored Data. 4. Encrypt transmission of cardholder data and sensitive information across public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	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.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

How to approach PCI Compliance

If you are one of the above mentioned entities and have not been assessed for compliance, you need to start the process of certifying for compliance. In the long run, the best approach to this is to hire a PCI professional. This need not be a permanent appointment as his/her expertise is best deployed in ensuring that the control environment is optimal to achieving compliance. Thereafter the task becomes one of ensuring that the controls are at all times adhered to and that changes to the PCI requirements or changes to the systems are integrated into the control environment. Preparation is key in advance of any PCI audit. When embarking on PCI compliance it is helpful to develop a PCI Compliancy Roadmap. This involves

- Reading the available documentation from the card schemes which defines the requirements of the PCI standard.
- Identifying all credit card data and the path it takes through your systems.
- Conducting a pre-audit review to determine where gaps exist within your systems or processes.
- Developing and implementing a remediation plan.

In developing a remediation plan be cautious of substantial changes to your systems and procedures. Validate with your PCI professional that the approach taken is necessary. All too often, unnecessary work is undertaken to achieve compliance.

Once you have achieved compliance, the work is not complete. Ensure that all change is closely monitored as simple changes in your environment can open compliance gaps. Ensure that the controls in place are adhered to at all times. Additionally, pay particular attention to activities that may occur using text files, spreadsheets, faxes etc as this can often be overlooked and can be a source of non-compliance.

Benefits of Compliance

The PCI Security Standards comprise a number of security best practices. The implementation of these requirements does improve the overall security of your environment and improves the security awareness of your employees. In an environment, where business reputation is of paramount importance, the successful implementation of the PCI standard is a further endorsement of your policies and procedures. Beyond that the key benefits are:

- Protects your customer data.
- Improves customer confidence through higher levels of data security.
- Protects your organisation from financial losses.
- Derive benefit from an annual health check of your systems security.