



» SERVICES



Winners of 'Best Security Company'

Meeting the PCI-DSS Standard

Meeting the PCI-DSS Requirement

Why the need for compliance?

To protect sensitive cardholder data from the continuing and growing threat of theft and credit card fraud, the major credit card providers including Visa, Mastercard, American Express, Diners Club and Discover, joined together to introduce the Payment Card Industry (PCI) Data Security Standard (DSS).

PCI Compliance

Credit card issuers divide merchants into four levels based upon the number of transactions processed every year:

| | |
|--------------------|--|
| » Merchant Level 1 | Greater than 6 million transactions |
| » Merchant Level 2 | Between 150,000 and 6 million transactions |
| » Merchant Level 3 | Between 20,000 and 150,000 transactions |
| » Merchant Level 4 | Less than 20,000 transactions |

Each level is subject to a different set of compliance activities, with the strictest rules applied to level 1 merchants. In addition to transaction volume, any merchant that suffered a hack or an attack that resulted in account data compromise will automatically be required to meet level 1 compliance requirements. Further, the card issuer may, at their discretion, require any merchant in the network to meet level 1 requirements.

A level 1 merchant needs to submit an annual Report on Compliance, validated by an approved independent auditor, or by an internal audit department, provided that a letter signed by an executive-level officer of the company accompanies the report. For level 1 merchants required to undergo an annual compliance review, the scope of validation is focused on systems or system components related to the authorisation and settlement wherever cardholder data is processed, stored, or transmitted.

Proving Compliance

Implicit and explicit in all of the above requirements is the need to document compliance activities. Documentation is required not only to track results, but also to prove that a process is in place, demonstrating due care in the effort to reach compliance and protect data. The adage "you can't manage what you can't measure" is particularly true in the arena of application security. The cornerstone of any implementation of source code scanning, therefore, must be the ability to produce specific and detailed reports of the results of scans and any subsequent remediation activities. Each constituent in the lifecycle compliance process, from managers to developers, QA, and compliance officers, must be able to derive the data they need to complete their role in the process.

The Three Cost Categories of PCI-DSS

Achieving PCI compliance, avoiding fines and retaining the privilege to accept credit cards requires merchants and service providers to address approximately 180 individual PCI requirements in 12 categories. Participating merchants must pay for their own PCI compliance assessments, the incremental cost of compliance depends upon the extent to which the infrastructure is already in a compliant or near-compliant state. Multiple assessments may also be needed to assure compliance, which is why it is essential for merchants to work with an experienced qualified security assessor (QSA) that has been approved by the PCI security standards council. The costs associated to PCI-DSS compliance can be divided into three categories:

1. **Upgrading systems (Infrastructure)** - Merchants and service providers must ensure that computer systems processing payment and cardholder information are upgraded in accordance with the PCI-DSS requirements. For many Level 1 and Level 2 merchants, much of the security infrastructure may already be in place. However, some may find the need to purchase and install new infrastructure components including and not limited to additional firewalls, upgraded anti-virus, anti-spyware and full-spectrum messaging security software, secure wireless systems, data encryption technologies, and file-integrity monitoring software.
2. **Verifying Compliance (Assessments)** - Level 1 Merchants must pay for their own PCI compliance assessment performed by an approved QSA or qualified security assessor. A Level 1 merchant or service provider must submit an annual "Report on Compliance," which is validated by the approved QSA, and multiple assessments can be required during the year to ensure compliance is being maintained. The scope of the assessment and verification is focused on systems or system components related to the authorisation and settlement wherever cardholder data is processed, stored, or transmitted.
3. **Sustaining compliance** - It is insufficient for merchants and service providers to merely "meet" the PCI-DSS requirements. Merchants and service providers must sustain continuous compliance as part of the overall IT operations strategy and framework. Key to this is ensuring that once systems are compliant, and policies and process are established, the IT organisation must ensure systems remain in that compliant state. This includes monitoring changes in PCI requirements, such as the recently added requirement – mandatory June 30, 2008 – for implementing an application layer firewall.



NEXT GENERATION SECURITY SOFTWARE

» SERVICES



Meeting the
PCI-DSS
Standard

» Service Offerings for PCI DSS Compliance Assessments

NGSSoftware is one of the world's leading information security research companies and a global leader in providing consultancy and software solutions for securing applications and data within the IT security marketplace. We also review current and future products for many large software providers.

We have developed trusted relationships with our clients, including some of the world's largest corporations. We provide our services to a substantial section of the world's largest banks, software companies, financial institutions, credit card providers, on-line retailers, manufacturers, Internet Service Providers, Telecoms companies and Government Departments/Agencies in the UK, US and Asia Pacific. Due to our relationships with Government Departments as well as major financial companies, the majority of our consultants have been required to undergo strict security and financial clearances.

NGSSoftware has a number of Qualified Security Assessors (QSA) and is an Approved Scanning Vendor (ASV). We provide a single source of approval recognized by all five founding members of the PCI Security Standards Council (American Express, Discover, JCB, MasterCard and Visa).

Our PCI QSA Consultants can provide advice, guidance, gap analysis and audit services to organisations that process credit card transactions to ensure their compliance efforts meet the requirements of the compliance specification in the following 6 categories:

1. Secure Network Design and Maintenance
2. Cardholder Data Protection
3. Vulnerability Management Program Maintenance
4. Strong Access Control Measures Implementation
5. Regular Network Testing and Monitoring
6. Information Security Policy Maintenance

As an ASV, we use our own award winning web application, network and database vulnerability scanners to detect potential exploits. We are recognised by the PCI Security Standards Council as an approved QSA, listed on their website: (https://www.pcisecuritystandards.org/qa_lookup/index.html).

We are approved to perform QSA services and onsite reviews and provide PCI compliance reports for all parties in the payments chain, including financial institutions, issuers of payment cards, authorised merchants, acquirer banks and all the appropriate data processing entities performing services for all the above.

Organisations that embrace our recommendations and use our services can not only ensure their compliance with the PCI DSS, but also efficiently and effectively enhance the security of their Web application environment.

Link to PCI Self Assessment Questionnaire – https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf

» Assessment Offer

If you feel that you are not receiving an adequate service from your existing security supplier, NGSConsulting would like to extend the opportunity of a no cost, no obligation 'mini-audit', provided under an NDA.

This allows our consultants to demonstrate their technical abilities and also allows future clients to assess the strengths and weaknesses of their existing suppliers.

For further details of this offer, contact info@ngsconsulting.com

» Contact Details

Web: www.ngssoftware.com

Support: support@ngssoftware.com

Sales: sales@ngssoftware.com

UK Head Office (London)
Next Generation Security Software Ltd
52 Throley Way
Sutton
Surrey, SM1 4BF
United Kingdom

Australian Office (Sydney)
Next Generation Security Software Pty Ltd
Level 19, 2 Market Street
Sydney, NSW, 2000
Australia
ABN: 83 119804803
Regional Web: www.ngssoftware.com/au
Regional Sales: australiasales@ngssoftware.com

Tel: +44 (0)208 401 0070
Fax: +44 (0)208 401 0076

Tel: +61 (0) 448 692 022