



## » SERVICES



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2007



AWARDS  
2008  
EUROPE  
WINNER

Winners of 'Best Security Company'

PCI and Web  
Application  
Security

## PCI and Web Application Security

To protect sensitive cardholder data from the continuing and growing threat of theft and credit card fraud through web application vulnerabilities, the PCI DSS mandates that Requirement 6.6 of the standard be addressed through the two options of Application Code Review and Application Firewalls. Whilst the proper implementation of both options would provide the best multi-layered defence, it is acknowledged that the best option will be dependent upon how an organisation develops its web applications and other factors within the environment.

» PCI Requirements - The PCI DSS mandates that all merchants follow twelve requirements, listed in the following table:

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and security parameters
Protect Cardholder Data	3. Protect stored cardholder 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 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 Information Security Policy	12. Maintain a policy that addresses information security

The requirement for compliance with the Payment Card Industry's Data Security Standard DSS (PCI-DSS) 6.6 describes security steps that are intended to address threats to web applications. The Council crafted Requirement 6.6 to ensure web applications exposed to the public Internet are protected against the most common types of malicious input.

This requirement had been listed as a best practice since the launch of the DSS 1.1 in September of 2006, but as of June 30 2008 becomes a requirement for all companies that accept credit card transactions.

Requirement 6.6 gives merchants and service providers two mandatory options to ensure that input to web applications from untrusted environments is fully vetted.

1. An in-depth application code review
2. A web application firewall

The requirements mandate the use of either options but the standard recommends deploying both techniques. Organisations electing to undergo an application review have four choices:

1. Perform a manual review of application source code
2. Conduct manual web application security vulnerability assessment
3. Use automated source code scanning tools
4. Deploy automated web application security vulnerability assessment tools

The second option of the new requirement requires organisations to deploy a web application firewall between the web server and end-point devices. This is in addition to requiring standard network firewalls typically placed on an enterprise network's perimeter.

» Requirement 6: Develop and maintain secure systems and applications

This requirement is the core regulation addressing the need to validate the security of sensitive applications. It directly addresses the foundation of secure applications: the introduction of security processes and review throughout the software development lifecycle. Planning, design, development, and deployment: all the stages of the lifecycle must make security considerations a top priority to make compliance both possible and demonstrable.

- » 6.2 Establish a process to identify newly discovered security vulnerabilities.
- » 6.3 Develop software applications based on industry best practices and include information security throughout the software development life cycle.
- » 6.4.1 Documentation of impact.
- » 6.5 Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities.
- » 6.6 Ensure that all web-facing applications are protected against known attacks.



# NEXT GENERATION SECURITY SOFTWARE

## » SERVICES



PCI and Web  
Application  
Security

### Requirement 6: Develop and maintain secure systems and applications (Continued)

#### » Source Code Scanning Compliance Action

- » Provide the technology support to enable consistent, measurable assessment of the security state of source code, throughout the development phase:
  - » Comprehensive security knowledgebase.
  - » Precise metrics.
  - » Roles-based interfaces and reporting to deliver the required PCI compliance information to all stakeholders.
  - » In-depth reporting for audit documentation and traceability.
- » Produce PCI-specific reports to deliver management and technical data required by the PCI Standard:
  - » Specific reporting on source code impacts on data loss.
  - » Reporting on OWASP Top Ten compliance.
  - » Scan history to demonstrate ongoing compliance efforts.
  - » Reporting in both summary and detail to support specific vulnerability remediation, managerial decisionmaking and compliance reporting requirements.

» **Applications: A Potential Source of Security** - The increased focus on application security in the latest revisions of the PCI DSS can be traced directly to many of the recent high profile breaches, where insecure applications have proved to be the point of access for hackers, and the source of data loss.

» **Focus on Application Security: Requirement 6** - Application security represents one of the areas most challenging to organisations subject to PCI regulations. The most recent version of the PCI DSS, published in September 2006, strongly reflects the growing industry understanding about the impact of insecure applications on data privacy. The most significant addition to the Standard is the inclusion of a new mandate for the security of custom applications codified in Requirement 6: Develop and maintain secure systems and applications. Specifically, Requirement 6.6 states that all custom application code must be reviewed for common vulnerabilities by an organisation that specialises in application security or there must be a Web application firewall installed in front of Web-facing applications. This requirement will be considered a "best practice" until June 30, 2008, and then it becomes a requirement. This requirement, together with the other detailed requirements of the section, makes application security a cornerstone of the PCI compliance effort and the drive to protect cardholder data. It is a clear recognition that true data security must begin at the source.

» **Compliance Starts at the Source** - These new requirements clearly recognize that data security starts with software security. It is in source code that encryption is enforced, the security of network communications is established, access control is set. Or not. Therefore, it is in the source code that the drive for compliance with the PCI DSS, and the effort to secure private cardholder data, must begin. While the PCI DSS includes web application scanning and web firewalls as part of the potential solution set to address these issues, it is clear that source code scanning tools represent the most efficient, cost effective, and comprehensive solution to identify and address software vulnerabilities that affect data privacy.

» **Building PCI Compliance In** - The increasingly diligent attention on the security of source code springs from the fact that it is the central place where vulnerabilities to credit card data get introduced. It can also be the least expensive place to address them, when source code analysis is performed at the earliest point in the software development lifecycle. For organisations charged with PCI compliance, it makes both fiscal and governance sense to introduce source code scanning into the development lifecycle for custom and outsourced code. Leaving it solely to the responsibility of an outside organisation reduces the financial benefit of early discovery of vulnerabilities, and increases the likelihood of project delay and risk.

The leading source code analysis solutions use an extensive vulnerability knowledgebase powered by a scanning engine able to scan large amounts of source code efficiently. The knowledgebase should include not only the common coding errors that create opportunities for hackers, but also the identification of design and policy errors that pose the greatest danger to private data.

To truly address PCI compliance issues, as well as the total software security risk to credit card information, the source code scanner must look for coding errors as well as policy violations and design flaws. The Ounce Labs toolset, for example, covers both types of issues and their analysis includes:

- » Coding vulnerabilities (Buffer overflows, Format string vulnerabilities, Race conditions, Resource leaks, Input/Output validation and encoding errors, SQL injection, Cross-site scripting, OS injection)
- » Design flaws and policy violations (Cryptography, Network communication vulnerabilities, Application configuration vulnerabilities, Access control, Database and file system use, Dynamic code, Access control and authentication errors, Error handling and logging vulnerabilities, Insecure error handling, Insecure or inadequate logging, Native code loading, Data storage vulnerability, Insecure Components, Malicious Code, Unsafe native methods, Unsupported methods, Custom cookies/ hidden fields)

» **Where Source Code Meets PCI Compliance** - There are multiple regulations within the PCI DSS on which source code security has an impact. It is vital that organisations understand the intersection of source code and each application regulation to ensure that the compliance review is comprehensive.



# NEXT GENERATION SECURITY SOFTWARE

## » SERVICES



PCI and Web  
Application  
Security

### » 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](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](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](mailto:info@ngsconsulting.com)

### » Contact Details

Web: [www.ngssoftware.com](http://www.ngssoftware.com)

Support: [support@ngssoftware.com](mailto:support@ngssoftware.com)

Sales: [sales@ngssoftware.com](mailto: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](http://www.ngssoftware.com/au)  
Regional Sales: [australiasales@ngssoftware.com](mailto:australiasales@ngssoftware.com)

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

Tel: +61 (0) 448 692 022