

**PROFESSIONAL SERVICES OVERVIEW****Penetration Testing**

- Analysis of either external, internal, or both external and internal vulnerabilities with risk scores and a prioritized remediation list
- Testing of operating systems, network devices, services, and software such as databases and web applications
- Penetration Testing Training

Compliance Audits

- Gap analysis in preparation for PCI, HIPAA, GLBA, ISO 27001, NERC/FERC, and SOX compliance audits

Web Application Security Audits

- Audit the effectiveness of Web applications security controls
- Remediation advice to help Web applications withstand attack
- Web Application Security Training

Enterprise Security Best Practices

- Develop a plan identifying risk and tools recommendations to find and fix security issues
- Evaluation of your policies and procedures based on our extensive knowledge of industry best practices

Social Engineering

- Recommendations to help identify and remediate internal and external social weaknesses
- Social engineering security awareness training for employees

Wireless Security Audits

- Identifying security best practices to prevent unauthorized use of your Wireless LAN (802.11)
- Wireless reconnaissance, rogue access point location, penetration testing

Rapid7 NeXpose Consulting & Training

- Installation and deployment expertise tailored to your needs
- Rapid7 NeXpose Jumpstart Installation and Training includes site specific deployment architecture, planning, installation, reporting, and administration

PCI S DS 0109

Rapid7 Data Security Standard Compliance

Payment Card Industry Data Security Standard (PCI DSS) is a worldwide standard endorsed by Visa, Cardholder Information Security Program (CISP), MasterCard, Discover, Diners Club, and American Express and is designed to respond to the rising number of incidents of stolen cardholder account data. The goal of PCI DSS is simple, protect cardholder account data. The stark reality for the merchant, is that the due diligence required to meet this standard is far from simple. In order to prepare for a PCI DSS compliance audit merchants must test, remedy, retest, and document their final compliance findings addressing the twelve requirements of PCI DSS.

At a broad brush level, the PCI DSS encompasses requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The requirements scale based on the number of annual transactions. For example, a Level 1 merchant is the highest level. They process more than six-million transactions annually and typically conduct an annual audit using an independent Qualified Security Assessor (QSA). Levels 2 through 4 include merchants that usually use the PCI DSS Self-assessment Questionnaire for their annual audit.

At all levels, merchants and service providers contract with a PCI Approved Scanning Vendor (ASV) to conduct vulnerabilities scans of any of their networks that transmit, process, or store cardholder data. In addition, to prepare for an annual PCI compliance audit, many merchants engage an external security assessment team to perform annual internal and external penetration tests as part of their vulnerability plan mandated by PCI DSS Requirement 11.

Why Rapid7?

Rapid7 has successfully completed the PCI Council Approved Scanning Vendor Compliance Testing Program, which certifies Rapid7 to help merchants achieve compliance with PCI DSS. With Rapid7 NeXpose, our Professional Services staff can perform an independent scan and produce the certified document for your records. Rapid7 consultants can also assist with the completion of your PCI DSS Self-assessment Questionnaire that solicits information about the internal security practices of your business, both on the Web and on your internal network.

Beyond scanning and preparing your Self-assessment questionnaire, Rapid7 is a full-service enterprise security assessment team. Rapid7 consultants can develop a confidential, independent assessment of your IT environment. Our consultants can perform penetration tests, develop a gap analysis, and help define your security policies capitalizing on their experience and objectivity.

ABOUT RAPID7

Rapid7 Rapid7 is a leader in vulnerability management and compliance, delivering a single unified solution across an organization's entire infrastructure. Rapid7 NeXpose is the only solution that includes support for web applications, databases, operating systems, and network devices in a single system. It separates real threats from the noise common to most vulnerability management systems, giving direct, actionable visibility into the real threats to mitigate risk and remain compliant. For more information on NeXpose products and services, visit www.rapid7.com

PCI DSS TWELVE REQUIREMENTS

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

Source: PCI Security Standards Council (www.pcisecuritystandards.org)