PCI DSS Compliance Guide

PCI DSS Compliance Guide

What is the PCI DSS?

Negative media coverage, a loss of customer confidence, and the resulting loss in sales can cripple a business. As a result, all entities that handle credit cardholder information are being challenged to adopt more effective data protection measures.

The Payment Card Industry (PCI) Data Security Standard (DSS) was created to confront the rising threat to credit cardholder personal information. The PCI DSS consists of the PCI Compliance Principles and Requirements for securing credit cardholder data in both hardcopy and electronic formats. The PCI DSS has been adopted by companies in the credit card industry as the global standard for the protection of customer information. The PCI Security Standards Council (SSC) owns, develops, maintains and distributes the PCI DSS. The SSC also provides oversight for the Approved Scanning Vendor program that certifies companies as Approved Scanning Vendors (ASV). The PCI DSS encompasses twelve requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

The goal of PCI DSS is simple; protect cardholder account data. In the pursuit of this goal, the PCI SSC has gained endorsement of the PCI-DSS by the five major payment card brands: Visa's Cardholder Information Security Program (CISP), MasterCard, Discover Financial Services, American Express, and JCB International.

Who needs to be PCI compliant?

The PCI SSC works with the five major payment card brands to ensure that merchants and service providers are PCI compliant. As a global standard, the PCI DSS applies to any entity worldwide that stores, processes or transmits credit cardholder data. This includes financial institutions, merchants and service providers in all payment channels. Financial institutions include banks, insurance companies, lending agencies, and brokerages. Merchants include restaurants, retailers (brick-and-mortar, mail/telephone order, e-commerce), transportation operators, and virtually any point-of-sale that processes credit cards across all industries. Examples of service providers include transaction processors, payment gateways, customer service entities, (i.e. call centers), managed service providers, web hosting providers, data centers, and Independent Sales Organizations.

The five major payment card brands enforce PCI compliance validation by requiring merchant banks to meet specific auditing and reporting criteria for their respective merchants and service providers. Each payment card brand has its own compliance program to uphold the PCI standard by enforcing PCI auditing and reporting requirements that must be met by the acquiring banks for merchants (also called merchant banks) in order to provide access to their payment network. The merchant bank then needs to produce evidence that merchants using their bank, along with any service providers used by those merchants, are in fact PCI compliant. This chain of

liability at each level is designed to protect credit cardholder data by using PCI-DSS to mitigate the risk of data breaches in the rapidly evolving threat landscape.

Merchants

Merchants are subject to the following validation requirements from each payment card brand:

Visa

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan & Penetration Test by Approved Scanning Vendor (ASV)
1	• Any merchant, regardless of acceptance channel, processing **more than 6 million transactions** per year • Any merchant that suffered a security breach, resulting in an account compromise • Any merchant that Visa otherwise deems a Level 1	RAPID7 Δ		RAPID7
2	• Any merchant processing between **1 to 6 million transactions** per year		RAPID7	RAPID7
3	• Any merchant processing **between 20,000 to 1 million transactions** per year		RAPID7	RAPID7
4	• Any merchant processing **less than 20,000 transactions** per year (i.e. all other merchants not in Levels 1, 2, or 3, regardless of acceptance channel)		RAPID7 Recommended, not required	RAPID7 Recommended, not required

Source: *http://usa.visa.com/merchants/risk_management/cisp_merchants.html*

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Mastercard

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan & Penetration Test by Approved Scanning Vendor (ASV)
1	• Any merchant, regardless of acceptance channel, processing **greater than 6 million transactions** per year • Any merchant that suffered a security breach, resulting in an account compromise • Any merchant that Mastercard otherwise deems a Level 1	RAPID7 Δ		RAPID7
2	• Any merchant processing greater than **1 million, but less than or equal to 6 million transactions** per year	RAPID7 * At merchant discretion	RAPID7*	RAPID7
3	• Any merchant processing **greater than 20,000, but less than or equal to 1 million transactions** per year		RAPID7	RAPID7
4	• All other merchants (i.e. any merchant processing **20,000 or less transactions**)		RAPID7 Recommended, not required	RAPID7 Recommended, not required

Source: http://www.mastercard.com/us/sdp/merchants/merchant_levels.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

* MasterCard announced revised requirements for Level 2 merchants. Effective 30 June 2011, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC-offered merchant training programs and pass any associated PCI SSC accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved QSA rather than complete an annual self-assessment questionnaire.

AMEX

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan & Penetration Test by Approved Scanning Vendor (ASV)
1	• Any merchant, regardless of acceptance channel, processing **more than 2.5 million transactions** per year • Any merchant that has had a data incident • Any merchant that American Express otherwise deems a Level 1	RAPID7 Δ		RAPID7
2	• Any merchant processing between **50,000 to 2.5 million American Express Card transactions** per year		RAPID7	RAPID7
3	• Any merchant processing **less than 50,000 American Express Card transactions** per year		RAPID7 Recommended, not required	RAPID7 Recommended, not required

Source: https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Discover

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan & Penetration Test by Approved Scanning Vendor (ASV)
1	• All merchants processing a total of **more than 6 million card transactions** annually on the Discover network. • Any merchant Discover, in its sole discretion, determines should meet the Level 1 compliance validation and reporting requirements • All merchants required by another payment brand to validate and report their compliance as a Level 1 merchant	RAPID7 Δ		RAPID7
2	• All merchants processing a total **of 1 million to 6 million card transactions** annually on the Discover network. • All merchants required by another payment brand to validate and report their compliance as a Level 2 merchant		RAPID7	RAPID7
3	• All merchants processing a total of **20,000 to 1 million card-not-present only transactions** annually on the Discover network • All merchants required by another payment brand to validate and report their compliance as a Level 3 merchant		RAPID7	RAPID7
4	• All other merchants		RAPID7 Recommended, not required	RAPID7 Recommended, not required

Source: http://www.discovernetwork.com/fraudsecurity/disc.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Discover authorizes use of either an annual on-site review by QSA **or** the merchant's internal auditor.

JCB International

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan & Penetration Test by Approved Scanning Vendor (ASV)
Merchants who handle cardholder data and transaction data **via the Internet or Internet-accessible network**	• All merchants processing a total of **1 million JCB transactions or more** per year	RAPID7 Δ Recommended, not required		RAPID7 Recommended, not required
	• All merchants processing **less than 1 million JCB transactions** per year		RAPID7 Recommended, not required	RAPID7 Recommended, not required
Merchants who **do not handle cardholder data and transaction data via the Internet nor Internet-accessible network**	• All merchants processing **1 million JCB transactions or more** per year	RAPID7 Δ Recommended, not required		
	• All other merchants		RAPID7 Recommended, not required	

Source: http://www.jcb-global.com/english/jdsp/index.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Service providers

Service providers are organizations that process, store, or transmit cardholder data on behalf of credit card clients, merchants, or other service providers. The major payment brands have different "terms" for service providers. Service providers are subject to the following validation requirements, as specified by each brand:

Visa

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan and Penetration Test by Approved Scanning Vendor (ASV)
1	• VisaNet processors or any service provider that stores, processes and/or transmits **over 300,000 transactions** per year	RAPID7 Δ		RAPID7
2	• Any service provider that stores, processes and/or transmits **less than 300,000 transactions** per year		RAPID7	RAPID7

Source: http://usa.visa.com/merchants/risk_management/cisp_service_providers.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Mastercard

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan and Penetration Test by Approved Scanning Vendor (ASV)
1	• **All TPPs** • All **DSE's** that store, transmit, or process **greater than 300,000 total combined MasterCard and Maestro transactions** annually	RAPID7 Δ		RAPID7
2	• Includes all **DSE's** that store, transmit, or process **less than 300,000 total combined MasterCard and Maestro transactions** annually		RAPID7	RAPID7

Source: http://www.mastercard.com/us/sdp/serviceproviders/serviceprovider_levels.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

AMEX

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan and Penetration Test by Approved Scanning Vendor (ASV)
1	• **All TPPs**	RAPID7 Δ		RAPID7

Source: https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_Provider_US.pdf

Δ
Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs). AMEX authorizes use of use either an annual on-site review by QSA **or** internal auditor of the Service Provider if certified (i.e. signed) by the chief executive officer, chief financial officer, or principal of the Service Provider.

Discover

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan and Penetration Test by Approved Scanning Vendor (ASV)
1	• **All Service Providers**	RAPID7 Δ	RAPID7 ◊	

Source: http://www.discovernetwork.com/fraudsecurity/disc.html

Δ
Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).
◊
Discover authorizes use of either an annual on-site review by QSA **or** an annual SAQ using PCI-DSS v1.2.

JCB International

Level	Criteria	Annual Report on Compliance (ROC) Audit by Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)	Quarterly Internal & External Vulnerability Scan and Penetration Test by Approved Scanning Vendor (ASV)
1	• **All Payment Processors** who **handle** cardholder data and transaction data **via the Internet or Internet-accessible network**	RAPID7 Δ Recommended, not required		RAPID7 Recommended, not required
2	• **All Payment Processors who do not handle** cardholder data and transaction **data via the Internet nor Internet-accessible network**	RAPID7 Δ Recommended, not required		

Source: http://www.jcb-global.com/english/jdsp/index.html

Δ Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

How Rapid7 Helps

Rapid7 has extensive experience partnering with financial institutions, merchants and service providers nationwide such as Stein Mart, Trader Joe's, Olympia Sports, The Blackstone Group, LendingTree, and E*TRADE FINANCIAL, to help them with their security and compliance requirements. Rapid7's PCI Compliance Solutions meet the data security standards required for merchants and service providers to achieve PCI compliance by addressing PCI DSS v1.2 Requirement 6.5, 6.6, 11.2 and 11.3 as follows:

- **Performing quarterly internal and external vulnerability scans** - Rapid7 has been recertified as an Approved Scanning Vendor (ASV) by the PCI Security Standards Council, authorizing us to help you achieve compliance with the PCI Data Security Standard (DSS). Rapid7 PCI Compliance Services perform an independent, quarterly ASV vulnerability scans and produce the certified documentation for your records. In addition, Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs). (Requirement 11.2)

- **Leveraging Rapid7 Managed PCI Services to provide the added value of automated quarterly scans including external vulnerability scanning** - Includes up to twelve rescans per quarter without at no extra charge, full remediation plans, eight hours of consulting time with one of our professional security consultants (2 hours per quarter) to review scan results and discuss remediation recommendations as well as any requested scan & report configuration changes. (Requirement 11.2)

- **Performing Rapid7 PCI Compliance Services** - Offering annual internal and external penetration testing services required by PCI DSS in order to detect deficiencies more quickly and provide detailed recommendations for fixes that would prevent attacks. (Requirement 11.3)

- **Performing Rapid7 PCI Gap Analysis** - For a detailed audit of your networked environment, Web application development secure coding policies, physical security control policies, training polices, and personnel policies, in addition to providing guidance on network segmentation to show you how to reduce the scope of your PCI audit and limit your cardholder segment. (Requirement 6.5)

- **Performing Web application assessment testing** - To identify vulnerabilities based on the OWASP Top 10 vulnerability list, in addition to providing Security Awareness Training, OWASP web development training and CEH/Penetration test training on request. (Requirement 6.6)

- **Providing assistance in completing the appropriate PCI Self-Assessment Questionnaire (SAQ)** - When required for PCI certification.

Rapid7 Solutions for the Payment Card Industry Data Security Standard (PCI DSS)

To meet PCI compliance, merchants adhere to the twelve PCI DSS requirements outlined below.

PCI Requirements	Detailed Requirements	Rapid7 Solution
Requirement 1 Install and maintain a firewall configuration to protect cardholder data	1.1 Establish firewall and router configuration standards that include: network connectivity diagrams; documentation of formal testing of firewall and router rules, review and change processes; documentation of roles engaged in network component logical management; and business justification for use of all services, protocols, and ports allowed 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	Use Rapid7 NeXpose to: ➢ Provide customizable scan settings that can be used to setup a baseline configuration of policies and settings to use when performing on-going scanning of firewalls, routers, switches, hubs, ports and network services. Generate a comprehensive mapping of network devices and services in order to detect devices and services that may allow connections between an untrusted network and any system components in the cardholder environment. (Requirement 1.1) ➢ Scan and monitor firewall configuration and router for vulnerabilities, and adherence to baseline configuration and policy settings, specifically to detect configuration violations that allow unauthorized connections between cardholder data environments and untrusted networks. (Requirement 1.2) Use Rapid7 PCI Consulting Services to: ➢ Recommend best practices to optimize network security components, including firewall and router configuration standards Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 1.3 and 1.4)
Requirement 2 Do not use vendor-supplied defaults for systems	2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are	Use Rapid7 NeXpose to: ➢ Utilize our customized policy compliance framework to monitor for access violations, including number of login attempts, password length, allowable special characters etc. Audits users and groups on your systems, and discovers unnecessary accounts to be eliminated (i.e. default vendor-supplied accounts, terminated employee accounts), allowing you to review results either in the UI or in a report format so you can then use the data to inform your information access and management policies.

PCI Requirements	Detailed Requirements	Rapid7 Solution
	consistent with industry-accepted system hardening standards. 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. 2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	(Requirement 2.1) ➢ Utilize our customized policy compliance framework to configure and implement automated monitoring access controls based on your own internal policies or based on best practices defined by external groups (i.e. SANS, CIS or NIST). (Requirement 2.2) Use Rapid7 PCI Consulting Services to: ➢ Evaluate configuration of all non-console administrative access to ensure appropriate use of encryption in security controls, and to identify vulnerabilities that could lead to tampering with encryption keys in files and other encryption controls. (Requirement 2.3) ➢ Evaluate and recommend if shared hosting providers meet requirements defined in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.* (Requirement 2.4)
Requirement 3 Protect stored cardholder data	3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy. 3.2 Do not store sensitive authentication data after authorization (even if encrypted). 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). 3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: One-way hashes based on strong cryptography; Truncation; Index	Use Rapid7 PCI Consulting Services to: ➢ Evaluate cardholder data policy to ensure appropriate data retention and disposal policies documentation as part of Rapid7 PCI Gap Analysis. Test if documentation is followed in practice by adding Rapid7 Social Engineering services to your Gap Analysis. (Requirement 3.1) ➢ Identifies gaps in your security program, determines if security policies are being followed in actual day-to-day operations (i.e. data storage policies, PAN masking, and protection of cryptographic keys as part of PCI Gap Analysis and Penetration Testing. (Requirements 3.2 to 3.5) ➢ Evaluate key-management processes and procedures for encryption of cardholder data, and provide recommendations as part of Rapid7 PCI Gap Analysis. (Requirement 3.6)

PCI Requirements	Detailed Requirements	Rapid7 Solution
	tokens and pads (pads must be securely stored); Strong cryptography with associated key-management processes and procedures 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse. 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	
Requirement 4 Encrypt transmission of cardholder data across open, public networks	4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. 4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	Use Rapid7 NeXpose to: ➢ Utilize our customized policy compliance framework to configure and monitor traffic over secured and unsecured ports. Identify all open ports, and logs all information, including any evidence that any Web applications, software enterprise applications, or databases are not using the ports assigned as secure ports for transmitting secure cardholder data. (Requirement 4.1) Use Rapid7 PCI Consulting Services to: ➢ Recommend best practices to optimize data security, including end-user messaging policies. Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 4.2)
Requirement 5 Use and regularly update antivirus software	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit	Use Rapid7 NeXpose to: ➢ Provide customizable scan settings for continuous, automatically generated, comprehensive mapping of all assets, including applications such as anti-virus software. (Requirement 5.1) ➢ Utilize our customizable risk scoring, policy auditing, and vulnerability scanning to alert you of policy violations or misconfigurations, including versioning and patch levels. (Requirement 5.2)

PCI Requirements	Detailed Requirements	Rapid7 Solution
Requirement 6 Develop and maintain secure systems and applications	6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. 6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues. 6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle 6.4 Follow change control procedures for all changes to system components. 6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide.* 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks	Use Rapid7 NeXpose to: ➢ Scan all system assets to ensure security patches and configurations are maintained based on user-specified parameters for all system components and software, including Web applications, enterprise software, network components, and databases. (Requirement 6.1) ➢ Perform both scheduled and ad-hoc internal vulnerability scans to monitor the security posture based on vulnerabilities, configuration, and compliance status of your entire infrastructure, including network devices, databases, Web applications, off-the-shelf commercial/enterprise applications, open source applications, in-house custom applications, servers, operating systems, services and all IP-enabled devices using the most up-to-date vulnerability checks provided by Rapid7's update services. NeXpose checks for updates every 6 hours; there is a 24-hour SLA for Windows machines when new Microsoft vulnerability bulletins are released. Provides up-to-date vulnerability checks, including reliable 24 hour response to Microsoft Patch Tuesday, plus new vulnerabilities updates twice per month. (Requirement 6.2 and 6.6) ➢ Perform ad-hoc vulnerability scans to monitor the security posture based on vulnerabilities, comparison to desired baseline configuration, and compliance status of specific systems, including any custom Web applications or custom installed applications. NeXpose allows administrators to setup custom asset groups. Applications under development can be put in an asset group in a testing area outside the production environment, and scanned for vulnerabilities to validate that secure coding guidelines are incorporated into the change control procedures. Fix weak code throughout the entire software development cycle, and continue on an on-going basis to address new threats. (Requirement 6.3 to 6.4, and 6.6) Use Rapid7 PCI Consulting Services to: ➢ Review custom Web application coding to ensure secure best practices based on secure coding

PCI Requirements	Detailed Requirements	Rapid7 Solution
		guidelines by testing the application using the Full OWASP Testing Methodology framework from the Open Web Application Security Project Guide as part of an onsite PCI Gap Analysis. Complete Web application assessment testing to identify vulnerabilities based on the OWASP Top 10. (Requirement 6.5)
Requirement 7 Restrict access to cardholder data by business need-to-know	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Use Rapid7 PCI Consulting Services to: ➢ Recommend best practices to optimize data security, including system access policies to limit access to system components and cardholder data to only those whose job role absolutely requires such access. Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 7.1) Use Rapid7 NeXpose to: ➢ Leverage our customized policy compliance framework to set up automated monitoring access controls (including adherence to policies for role-based access) to validate enforcement of access restrictions. (Requirement 7.2)
Requirement 8 Assign a unique ID to each person with computer access	8.1 Assign all users a unique ID before allowing them to access system components or cardholder data. 8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: Password or passphrase; Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in	Use Rapid7 NeXpose to: ➢ Leverage our customized policy compliance framework to set up automated monitoring access controls, including number of login attempts, password length, allowable special characters, and other login ID access control policies. (Requirement 8.1 - 8.2, 8.4) Use Rapid7 PCI Consulting Services to: ➢ Recommend best practices to optimize data security, including usage of two-factor authentication for remote access to the network, secure dial-in service, terminal access controls with tokens, or VPNs with individual certificates. (Requirement 8.3) ➢ Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day

PCI Requirements	Detailed Requirements	Rapid7 Solution
	service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*). 8.5 Ensure proper user authentication and password management for non-consumer users and administrators.	operations, and recommend ways to address any deficiencies. (Requirement 8.5)
Requirement 9 Restrict physical access to cardholder data	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. 9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. 9.3 Make sure all visitors are properly authorized before entering areas where cardholder data is processed or maintained 9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law. 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review	Use Rapid7 PCI Consulting Services to: ➢ Review existing policies, procedures and tools in use for securing the physical access to cardholder data. Recommend best practices for physical access security measures to limit and monitor physical access to systems in the cardholder environment. (Requirement 9.1 - 9.2, and 9.5 - 9.10) ➢ Evaluate and document security controls, identify gaps in your security program, and determine if security policies are being followed in actual day-to-day operations by adding Rapid7's Social Engineering Services to your PCI Gap Analysis. Rapid7 Security Experts will test is physical access controls are working as described in the documentation, then present a detailed report of their findings and recommend ways to address any deficiencies. (Requirement 9.3 - 9.4)

PCI Requirements	Detailed Requirements	Rapid7 Solution
	the location's security at least annually. 9.6 Physically secure all paper and electronic media that contain cardholder data. 9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data. 9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals). 9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data. 9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons	
Requirement 10 Track and monitor all access to network resources and cardholder data	10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: All individual accesses to cardholder data; All actions taken by any individual with root or administrative privileges; Access to all audit trails; Invalid logical access attempts; Use of identification and authentication mechanisms; Initialization of the audit logs; Creation and deletion of system-level objects 10.3 Record at least the following audit trail entries for all system components for	Use Rapid7 NeXpose to: ➢ Leverage our customized policy compliance framework to set up automated monitoring access controls, including monitoring of any access to system components done with administrative privileges, and other login ID access control policies. Results are documented in a detailed step-by-step remediation plan based on their prioritized risk rating. (Requirement 10.1) ➢ Compare how previous states of devices on the network compare with the baseline, as well as any other record in the log. .. Configure alerts using the built-in ticketing system so that alerts automatically document when a high risk change has been made to any asset configuration, which then provides a complete audit trail of configuration changes that can be used for event reconstruction. (Requirement 10.2)

PCI Requirements	Detailed Requirements	Rapid7 Solution
	each event: User identification, Type of event, Date and time, Success or failure indication, Origination of event, Identity or name of affected data, system component, or resource 10.4 Synchronize all critical system clocks and times. 10.5 Secure audit trails so they cannot be altered. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 10.6 Review logs for all system components at least daily. 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	➢ Implement an automated end-to-end security solution to automatically track all assets added or removed, any asset configuration changes against an expected baseline state and identify unauthorized devices and services. Document all security incidents and subsequent effects of vulnerability remediation to establish historical audit log record, including fully configurable automated notifications and ticketing system for customizable case escalation, ticket creation, and notification, including ability to integrate with third-party ticketing systems through the flexible NeXpose API. (Requirement 10.2) ➢ Ensure continuous logging of historical scan data showing device's previous state, including the monitor of system log files to detect if they are detectably altered or removed. Uses automated utility to save duplicates of data to backup server. (Requirement 10.5-10.7) Use Rapid7 PCI Consulting Services to: ➢ Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. Recommend best practices to optimize data security, including the optimal blend of auditing processes, logging technologies, and specific security controls to reduce the risk of systems becoming compromised by unauthorized access (Requirement 10.3-10.4, 10.6)
Requirement 11 Regularly test security systems and processes	11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). *Note: Quarterly external vulnerability*	Use Rapid7 NeXpose to: ➢ Enable internal security staff to conduct ad-hoc internal vulnerability scans after significant network changes, (such as new system component installations, changes in network topology, firewall rule modifications, or product upgrades. Provides complete vulnerability management to evaluate potential risks to private data by scanning the entire infrastructure (networks, databases, desktop applications, Web applications, servers, VPNs), data storage, data transmission, policy settings, patching levels, and configuration settings on your LAN and WLAN for vulnerabilities and weaknesses to

PCI Requirements	Detailed Requirements	Rapid7 Solution
	scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff. 11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: Network-layer penetration tests; Application-layer penetration tests 11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date. 11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	understand your risk posture. (Requirement 11.2) ➢ Enable internal Red Team staff to perform both scheduled and ad-hoc penetration testing by use NeXpose in conjunction with Metasploit, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. (Requirement 11.3) Use Rapid7 PCI Consulting Services to: ➢ Perform Wireless Security Audits to test identify security best practices to prevent unauthorized use of your Wireless LAN (802.11). Conduct penetration testing and perform wireless reconnaissance to locate rogue unsecured access points. (Requirement 11.1) ➢ Perform your quarterly internal network vulnerability scans. As a PCI Approved Scanning Vendor (ASV), Rapid7 Professional Services is certified to complete the internal network vulnerability scans required by PCI. (Requirement 11.2) ➢ Perform your quarterly external network vulnerability scans. As a PCI Approved Scanning Vendor (ASV), Rapid7's Managed PCI Compliance Services provides both internal and **external** quarterly scans, in addition to detailed compliance reporting, a PCI remediation plan, and eight hours of consulting time with one of our professional security consultants. (Requirement 11.2) ➢ Perform your annual external and internal penetration testing to determine if a hacker could access and steal protected cardholder data. Penetration testing includes network-layer and application-layer tests. Penetration testing is conducted using NeXpose in conjunction with a variety of specialized tools including Metasploit, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. (Requirement 11.3) ➢ Perform PCI Gap Analysis to evaluate and document security controls, identify gaps in your security program, determine if security policies are being

PCI Requirements	Detailed Requirements	Rapid7 Solution
		followed in actual day-to-day operations, and recommend ways to address any deficiencies, including insufficient IDS/IPS coverage, and gaps in your file-integrity monitoring controls. (Requirement 11.4 – 11.5)
Requirement 12 Maintain a policy that addresses information security	12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following: Addresses all PCI DSS requirements; Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment; Includes a review at least once a year and updates when the environment changes. 12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures). 12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. 12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors. 12.5 Assign either an individual or team the information security management responsibilities for access control, monitoring, and incident management. 12.6 Implement a formal security	Use Rapid7 PCI Consulting Services to: ➢ Perform a full PCI Gap Analysis to identify threats, and vulnerabilities. Perform the formal risk assessment, and assist in writing the documentation to meet annual PCI requirements such as the applicable Self-Assessment Questionnaire (SAQ), and formal security policy documentation. (Requirement 12.1) ➢ Perform a full PCI Gap Analysis including Penetration Testing and Social Engineering to evaluate your daily security controls, determines if security policies are being followed in actual day-to-day operations, identifies gaps in your security program, and provides guidance on developing missing control policies and procedures required to secure information systems and data from external threats. (Requirement 12.2-12.5, 12.7, 12.8-12.9) ➢ Provide holistic vulnerability management security training, including detailed security training on using Rapid7 NeXpose within an integrated security management program. Provides recommendations and guidance on implementing a security awareness training program to make all employees and contractors aware of importance of securing cardholder data. (Requirement 12.6)

PCI Requirements	Detailed Requirements	Rapid7 Solution
	awareness program to make all employees aware of the importance of cardholder data security. 12.7 Screen potential employees prior to hire to minimize the risk of attacks from internal sources. 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	

Contact us to find out how Rapid7 can help you implement PCI for both Web and storefront transactions, and achieve PCI compliance for your business and your customers.

About Rapid7

Rapid7 is the leading provider of unified vulnerability management, compliance, and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies.

Recognized as the fastest growing vulnerability management company in the U.S. by *Inc.* Magazine, Rapid7 helps leading organizations such as Liz Claiborne, Southern Company, the United States Postal Service, the *New York Times*, Carnegie Mellon University and the National Nuclear Security Administration (NNSA) to mitigate risk and maintain compliance for regulations such as PCI, HIPAA, FISMA, SOX and NERC . Rapid7 also manages the Metasploit Project, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. For more information, visit www.rapid7.com.