The Payment Card Industry Data Security Standard

PCI DSS v3.0

March 2015

Compliance Guide

Contents

RAPID7

01

WHAT IS 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 Data Security Standard (PCI DSS) was created to protect credit cardholder data, and it is now on version 3.0, released in November 2013. The PCI DSS version 3.0 encompasses twelve requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. These requirements are grouped into six major categories, shown to the right.

In total, the PCI DSS has six domains, twelve requirements, and 200 detailed sub-requirements. Page 9 of this compliance guide provides a breakdown of PCI requirements in detail.

The PCI Security Standards Council (SSC) owns, develops, maintains, and distributes the PCI DSS. The SSC also provides oversight of external on-site Qualified Security Assessors (QSA) and Internal Security Assessors (ISA) to validate compliance, the qualification of PCI Forensic Investigators (PFI) that act on compromised cases, and the certification of Approved Security Vendors (ASV) to perform external vulnerability scans and deliver an Attestation of Compliance.

In order to safeguard credit cardholder personal information, the five major payment card brands have endorsed PCI DSS: Visa, MasterCard, Discover Financial Services, American Express, and JCB International.

THE PCI DSS REQUIREMENTS ARE GROUPED INTO SIX MAJOR CATEGORIES:

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: Protect all systems against malware and regularly update anti-virus software or programs

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: Identify and authenticate access to system components

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 for all personnel

02

WHO NEEDS TO BE PCI COMPLIANT AND WHY?

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. (*See page 4 for a breakdown of the payment card brand requirements for merchants and service providers.*)

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.

03
COMPLIANCE VALIDATION TOOLS AND REQUIREMENTS

Any organization that needs to be PCI compliant must definitively prove their compliance with standards and practices in place. Thankfully, PCI has a number of available tools to help validate compliance. In this next section, we'll review some of these compliance validation tools and what PCI requirements they help fulfill.

Approved Scanning Vendor (ASV) network vulnerability scans

This tool has been specifically designed to help organizations meeting one particular requirement of PCI DSS (11.2.2):

> *Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).*

PCI requires external vulnerability scans to be performed on a quarterly basis by security companies qualified by the PCI Council (PCICo)—Approved Scanning Vendors.

The scope of the external vulnerability scan must include all externally accessible system components that are part of the cardholder data environment (CDE). It should also include any externally facing component that provides a path to the CDE.

The scan customer is responsible for defining the scope of the external vulnerability scan. If an account data compromise occurs via an externally facing system component not included in the scan, the scan customer is responsible.

ASVs validate any IP addresses found during the scan with the customer to determine whether or not they should be included within the scope of the assessment.

ASV scan reports consist of three parts:

1. An Attestation of Compliance—a declaration of global compliance
2. An executive summary—provides component compliance summary information
3. A detailed vulnerability report—detailed list of vulnerabilities found

Organizations can obtain a passing result on their network vulnerability scan when the scan report does not contain:

- High- or medium-severity vulnerabilities
- Automatic failures (as defined by the PCICo)

To be considered compliant, an organization must conduct four consecutive passing ASV scans within twelve months.

Notes:

- A passing scan report may require multiple iterative scans.
- Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed.
- Additional documentation may be required to verify that non-remediated vulnerabilities are in the process of being addressed.

Self-assessment questionnaire

The self-assessment questionnaire (SAQ) allows organizations to evaluate their compliance with PCI DSS. This is a useful tool to determine, document, and modify alignment with the standard.

There are as many SAQ versions as there are merchant types. There are five kinds of merchant types for PCI: A, B, C-VT, C, and D. Each SAQ covers only the PCI sections and requirements relevant to the specific merchant type.

Each SAQ version has two parts:

1. Questions correlating to the PCI DSS requirements
2. Attestation of Compliance (AOC) or self-certification that a company is eligible to complete that specific SAQ

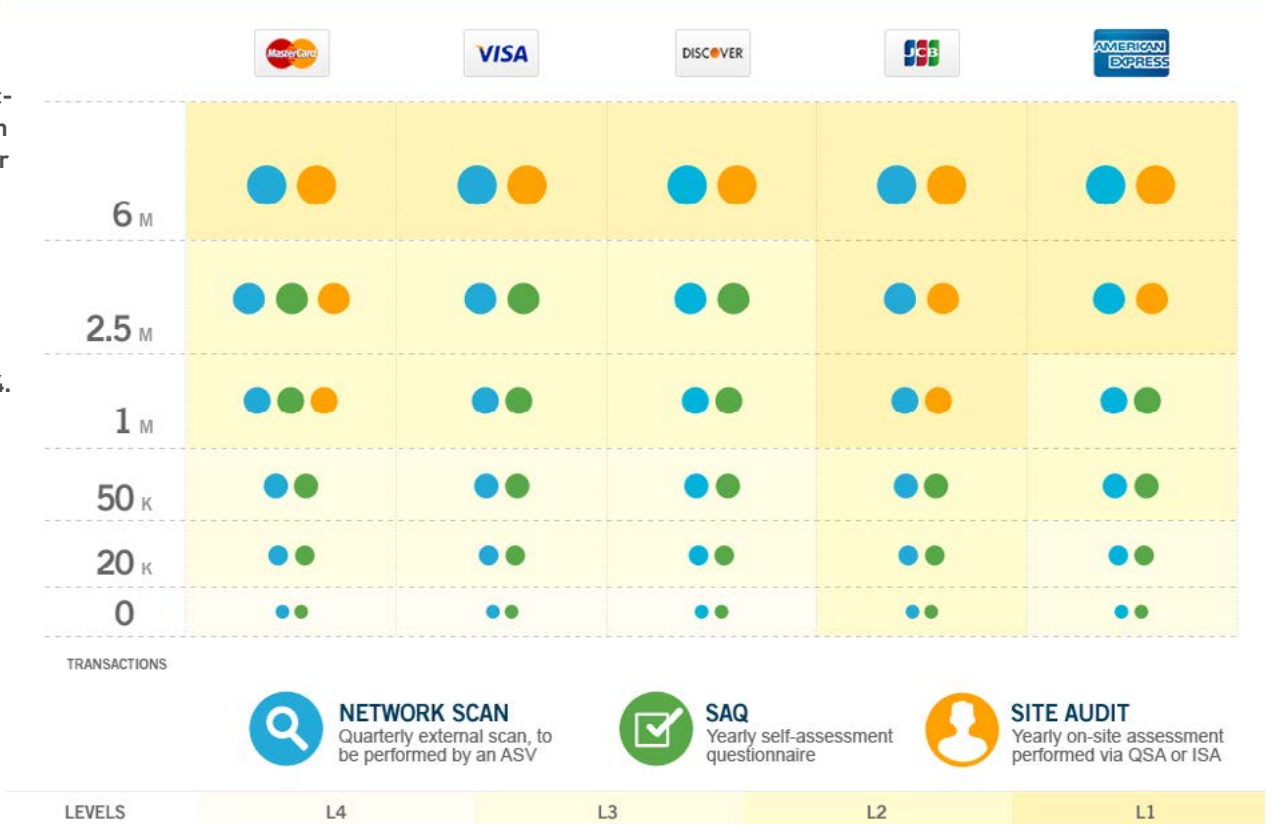
*Not sure what your type is? Find out by reading: **PCI 30-Second Newsletter #5: What's your type?** on the Rapid7 Community site.*

Rapid7 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council, authorizing us to help you achieve compliance with PCI DSS.

04

VALIDATION REQUIREMENTS FOR MERCHANTS

This chart gives a global perspective on validation requirements for merchants from each payment card brand. The requirements here are organized by level, from 1 through 4.



On-site audit

Organizations perform this thorough assessment internally in order to validate their adherence to the PCI standard.

Such assessments must be conducted by qualified external (QSAs) or internal security auditors (ISAs) trained and approved by PCIco.

If internal individuals are used, the key thing is that they must belong to an internal audit organization. For obvious conflicts of interest reasons, IT staff or information security staff must not perform the assessment.

To complete the on-site audit, organizations must:

- Validate the scope of the cardholder data environment
- Verify of all technical and procedural documentation
- Confirm that each PCI DSS requirement has been met
- Evaluate, accept, or reject compensating controls
- Produce a Report on Compliance (ROC)

Payment card brand-specific notes and recommendations:

MasterCard

Level 1 merchants: Annual on-site assessment can be executed by Internal Qualified Staff (ISA) if they

have attended PCI SSC ISA Training and passed the accreditation program every year.

Level 2 merchants:

- Effective June 30, 2012, level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training and pass the associated 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 on-site assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA), rather than complete an annual self-assessment questionnaire.

Level 4 merchants: Consult acquirer for more information on completing the network scan and SAQ.

Visa

Network scans and SAQs for level 4 merchants are recommended. Compliance validation requirements are set by acquirers.

American Express and **Discover**

Network scans and SAQs for level 3 merchants (American Express) or level 4 (Discover) are not mandatory but strongly recommended.

JCB

Network scans for level 1 or level 2 merchants are not required if your organization does not handle cardholder data and transaction data via the internet or an internet-accessible network.

05

VALIDATION REQUIREMENTS FOR SERVICE PROVIDERS

This chart gives a global perspective on validation requirements for service providers from each payment card brand. The requirements here are organized by level, from 1 through 4.

Payment card brand-specific notes and recommendations:

MasterCard

- Level 1 service providers definition: All Third Party Processors (TPPs) and all Data Storage Entities (DSEs) with more than 300,000 total combined MasterCard and Maestro transactions annually.
- Level 2 service providers definition: All Data Storage Entities (DSE) with less than 300,000 total combined MasterCard and Maestro transactions annually.
- A DSE or Data Storage Entity is an entity other than a member, merchant, Independent Sales Organization (ISO), or Third Party Processor (TPP) that stores, transmits, and/or processes MasterCard account data for or on behalf of a merchant, ISO, or TPP.

Visa

- Level 1 service provider definition: VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 Visa transactions annually.
- Level 2 service provider definition: Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions annually.

JCB

- For all service providers: Network scans and site audits are not required if your organization does not handle cardholder data and transaction data via the internet or an internet-accessible network.

American Express

- For level 3 service providers: Network scans and SAQs are not mandatory but strongly recommended.

Discover

- For all service providers: Discover authorizes use of either an annual on-site review by QSA or an annual SAQ.

06
HOW RAPID7 CAN HELP

Rapid7 has extensive experience partnering with financial institutions, merchants, and service providers globally such as Stein Mart, Trader Joe's, Olympia Sports, The Blackstone Group, LendingTree, and E*TRADE FINANCIAL. Rapid7's PCI Compliance Solutions meet data security standards required for merchants and service providers to achieve PCI compliance by addressing PCI DSS v3.0 requirements.

Rapid7 Nexpose is a threat exposure management solution that proactively supports the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting, and mitigation.

In the context of the PCI version 3.0, Nexpose helps organizations subjected to compliance to:

- Perform quarterly internal and external vulnerability scans. Rapid7 is a certified 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 scan 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)
- Get top-down visibility of risk to their assets and business operations enabling them to organize and prioritize thousands of assets and quickly focus on the items that pose the greatest risk.
- Get a clear map of the RealRisk™ posed by the identified vulnerabilities across the organization's IT landscape.
- Make the inventory of their systems, services, and installed applications using the latest fingerprinting technologies.
- Provide an automated mechanism to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials through automated alerts.
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications.
- Generate easy-to-use detailed reports combined with role-based access controls to allow organizations to share information easily.
- Provide an automated mechanism to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.
- Audit users and groups on their systems.
- Discover accounts that were terminated and review results either in the UI or in a report format, and then use the data to feed your information access and management policies.
- Set up automated monitoring access controls (including adherence to policies for role-based access) to validate enforcement of access restrictions.
- Test the efficiency of their access control systems and policies.
- Test their external and internal boundaries defenses.
- Detect and report malicious software.
- Set up automated monitoring access controls, including number of login attempts, password length, allowable special characters, and other login ID access control policies.
- Get a detailed, sequenced remediation roadmap with time estimates for each task.
- Ensure continuous logging of historical scan data showing a device's previous state.
- Use automated utility to save duplicates of data to a backup server.
- Deliver auditable and reportable events on vulnerabilities throughout the infrastructure.
- Provide records to what occurred, sources of events and outcomes of events related to vulnerabilities.

Rapid7 Managed PCI Services provides the added value of automated quarterly scans including external vulnerability scanning to review scan results and discuss remediation recommendations as well as any requested scan & report configuration changes. (Requirement 11.2,11.2.2,11.2.3)

Rapid7 Metasploit is a penetration testing solution helping the enterprise's vulnerability management program and testing how well their defenses hold up against real world attacks.

In the context of the PCI DSS version 3.0, Metasploit Pro helps covered entities to:

- Perform internal and external penetration tests on the Cardholder infrastructure.
- Validate efficiency of their network segregation.
- Test the efficiency of their access control systems and policies.
- Survey hosts for use of approved authentication measures.
- Audit password length and complexity and authentication methods.
- Test their external and internal boundaries defenses.
- Support their incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits.

Rapid7 UserInsight is an intruder analytics solution helping organizations to detect and respond to incidents. In the context of PCI DSS version 3.0, UserInsight helps covered entities to:

- Audit the separation between development/test and production environments.
- Monitor access to cardholder data to ensure user's job requires access.
- Alert if individuals are sharing User IDs.
- Track if users are elevated to administrator status across on-premise and cloud systems.
- Monitor users across on-premise and cloud systems and alert if a suspended user is trying to access a system.
- Audit database access.
- Track authentications to all systems and store information in a secure, central location.
- Notify security team if a user deleted log files.
- Identify exceptions and anomalies in the log files.
- Retain audit history indefinitely and available for immediate analysis.
- Collect and alert on logs from IDS/IPS systems as well as firewalls.

Rapid7 Consulting service helps organizations subjected to PCI compliance to:

- Provide assistance in completing the appropriate PCI Self-Assessment Questionnaire (SAQ).
- Perform formal risk assessments.
- Conduct a vulnerability analysis on information systems.
- Perform penetration testing on information systems based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.
- Build the Penetration testing methodology.
- Perform a full gap analysis, including penetration testing and social engineering to evaluate their daily security controls, determine if security policies and procedures are being followed in actual day-to-day operations, identify gaps in their security program against PCI DSS, and provide guidance on developing missing control policies and procedures required to secure information systems and data from external threats.
- Provide customizable security awareness training to users of their organizational information systems.
- Provide vulnerability management security training and certification to managers and users of organizational information systems requiring knowledge and technical abilities to detect and validate vulnerabilities on the IT infrastructure, determine the associated risk severity, write IT risks reports, apply mitigations through remediation and control.

The Rapid7 community site helps organizations subjected to PCI compliance to:

- Stay up-to-date with the latest development in the vulnerability management and information security areas.

07

RAPID7 SOLUTIONS FOR PCI DSS VERSION 3.0 COMPLIANCE

This section details the PCI DSS version 3.0 security requirements and how Rapid7 Nexpose, Metasploit Pro, UserInsight and Consulting Services help organizations become and remain compliant.

PCI DSS V3.0	Nexpose	Metasploit	UserInsight	Consulting Services
Install and maintain a firewall configuration to protect cardholder data	X	-	-	X
Do not use vendor supplied defaults for systems	X	X	-	X
Protect stored cardholder data	-	-	X	X
Encrypt transmission of cardholder data across open, public networks	X	-	-	X
Use and regularly update anti-virus software	X	-	-	X
Develop and maintain secure systems and applications	X	X	X	X
Restrict access to cardholder data by business need-to-know	-	-	X	X
Identify and authenticate access to system components	X	X	X	X
Restrict physical access to cardholder data	-	-	-	X
Track and monitor all access to network resources and cardholder data	X	-	X	X
Regularly test security systems and processes	X	X	-	X
Maintain a policy that addresses information security	-	-	X	X

Requirement 1 - Install and maintain a firewall configuration to protect cardholder data

1.1	Establish firewall and router configuration standards that include: network connectivity and dataflow 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
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

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. (1.2)
- Detect configuration violations that allow unauthorized connections between cardholder data environments and untrusted networks. (Requirement 1.2)
- Verify that Windows firewall is enabled and configured to actively run on all workstations. (Requirement 1.4)

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, 1.4 and 1.5)

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 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	Maintain an inventory of system components that are in scope for PCI DSS.
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
2.6	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.

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. (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). Verify that each server only has a single critical role installed, default credentials have been changed, and unnecessary services and functionality are disabled. (Requirement 2.2)

Use Rapid7 Metasploit Pro to:

- Scan ports to determine if there are multiple primary functions with differing security levels coexisting on the same server that should instead be implemented on separate servers. (Requirement 2.2)
- Determine if any non-console administrative access tools, including browser-based management tools, are not encrypted. (Requirement 2.3)

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)
- Build and maintain system inventory. (Requirement 2.4)
- Create or validate security policies and operational procedures (Requirement 2.5)
- Evaluate and recommend if shared hosting providers meet requirements defined in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers. (Requirement 2.6)

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 tokens and pads (pads must be securely stored); Strong cryptography with associated key-management processes and procedures
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

Use Rapid7 UserInsight to:

- Monitor which users access critical systems or restricted network zones that may hold cryptographic keys, providing you with an access audit trail. (Requirement 3.5.1)

Use Rapid7 PCI Consulting Services to:

- Evaluate cardholder data policy and operational procedures associated with these requirements (Requirements 3.7)
- Identify gaps in your security program, determines if security policies and operational procedures are being followed in actual day-to-day operations (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)

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).
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

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 card-holder data. (Requirement 4.1)

Use Rapid7 PCI Consulting Services to:

- Evaluate your policies and operational procedures associated to these requirements (Requirement 4.3)
- 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 5 - Use and regularly update anti-virus 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.
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

Use Rapid7 Nexpose to:

- Provide customizable scan settings for continuous, automatically generated, comprehensive mapping of all assets, including applications such as anti-virus software, and verify that anti-virus software has been deployed to all workstations. (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, and verify that anti-virus software and definitions are up-to-date on all workstations. (Requirement 5.2)
- Verify that anti-virus software is actively running on all workstations. (Requirement 5.3)

Use Rapid7 PCI Consulting Services to:

- Evaluate your policies and operational procedures associated with these requirements. (Requirement 4.3)

Requirement 6 - Develop and maintain secure systems and applications

6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
6.2	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
6.3	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	Address common coding vulnerabilities in software-development processes as follows: Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Develop applications based on secure coding guidelines.
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.

6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

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 6.2)
- 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. (Requirements 6.2, 6.3, 6.4, 6.5 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. (Requirements 6.2, 6.3, 6.4, 6.5 and 6.6)

Use Rapid7 Metasploit Pro to:

- Find hosts with exploitable vulnerabilities. (Requirements 6.1 to 6.6)

Use Rapid7 UserInsight to:

- Monitor multiple separated environments, define network zones and alert you if access policies are violated. As an example, an organization could prevent all users that are "developers" to access the network zone "PCI Production," ensuring UserInsight alerts them on any such violations. (Requirements 6.4.1 and 6.4.2)

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.
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

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. (Requirements 7.1 to 7.3)

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)

Use Rapid7 UserInsight to:

- Flag systems in the cardholder data environment (CDE) as critical systems and alerts you when unusual and suspicious authentications are detected, e.g. a user authenticating to the CDE that has never authenticated to it before, helping

you enforce your policy. (Requirement 7.1)

- Flag systems in the cardholder data environment (CDE) as critical systems and alert whenever it sees any unusual authentications. You can set up different alerts for each system in the CDE to alert on who is allowed to access what system. Should an account allowed to access a CDE system escalate privileges to a different account, this would trigger additional alerts unless the behavior had been seen previously and deemed legitimate. (Requirement 7.1.1)
- Alert if any user violates the authentication policies you have defined, monitoring that the policies are enforced. (Requirement 7.3)

Requirement 8 - Identify and authenticate access to system components

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all systems.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.
8.3	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, including vendor access for support or maintenance.
8.4	Document and communicate authentication procedures and policies to all users.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods.
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

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 8.2)
- Verify that administrative credentials are not shared across multiple workstations or servers. (Requirement 8.5)

Use Rapid7 Metasploit Pro to:

- Survey hosts for use of approved authentication measures. (Requirement 8.2)
- Audit password length and complexity and authentication methods. (Requirement 8.4, 8.5)

Use Rapid7 UserInsight to:

- Alert if users are sharing accounts, providing you real-time visibility into policy violations. (Requirement 8.1.1 and 8.5)
- Alert if a user is elevated to administrator status, in Directory Services and Amazon Web Services. All account modifications can be viewed in a single Administrator Activity view. (Requirement 8.1.2)
- Alert if any users that are disabled in the Directory Services attempts to access any other associated account, including ActiveSync and cloud accounts such as Salesforce.com, Box.com, and Amazon Web Services. (Requirement 8.1.3)
- Define a network zone that a vendor should have access to and alert you if the credential is used outside of this zone, for example UserInsight can alert if an account in the HVAC user group is used outside of the HVAC network zone. UserInsight also monitors VPN activity and detects unusual behavior, such as a vendor connecting from a different country. UserInsight will alert you on attempts to use disabled accounts, allowing you to detect potential vendors being compromised or attempting to connect when their services are not required. (Requirement 8.1.5)

- Alert on brute forcing attempts, through failed authentications in logs, authentications to honeypots, and logins to honey user accounts. (Requirement 8.1.6)
- Get instant visibility into accounts that have their password set to never expire and the date of the last password change. Rapid7 UserInsight alerts when a credential that does not expire authenticates from the Internet through VPN, ActiveSync, or any other inbound service. (Requirement 8.2.4)

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. (Requirements 8.2, 8.3, 8.6, 8.7)
- 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 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 easily distinguish between on-site personnel and visitors.
9.3	Control physical access for on-site personnel to the sensitive areas.
9.4	Implement procedures to identify and authorize visitors.
9.5	Physically secure all media.
9.6	Maintain strict control over the internal or external distribution of any kind of media.
9.7	Maintain strict control over the storage and accessibility of media.
9.8	Destroy media when it is no longer needed for business or legal reasons.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

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. (Requirements 9.2, 9.4, 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 if 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. (Requirements 9.1, 9.3, 9.5, 9.6, 9.7, 9.8, 9.9)

Requirement 10 - Track and monitor all access to network resources and cardholder data

10.1	Implement audit trails to link all access to system components to each individual user.
10.2	Implement automated audit trails for all system components to reconstruct events.
10.3	Record at least the following audit trail entries for all system components.
10.4	Using time-synchronization technology, synchronize all critical system clocks and times.
10.5	Secure audit trails so they cannot be altered.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.
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 backup).

10.8	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

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)
- 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 UserInsight to:

- Collect all authentication logs, correlate them by user, and track all authentications, giving you full visibility to authentications to all systems. (Requirement 10.1)
- Collect a wide variety of system logs and store copies of them off-site where they can no longer be altered by the organization or an attacker, providing a secure and reliable audit trail. (Requirements 10.2 and 10.3)
- Record a full audit trail for all authentications to all systems, viewable by user and by asset. (Requirement 10.2.1)
- Get a list of all administrators, a history of all administrative activity across the network and Amazon Web Services environments and correlate all administrator account authentications to all systems. (Requirement 10.2.2)
- Track all authentication attempts, both successful and invalid ones. (Requirement 10.2.4)
- Get instant visibility into which users have administrative privileges in your organization, for both on-premise and cloud systems. UserInsight also alerts you of any changes to administrators, e.g. users added to the administrative group. (Requirement 10.2.5)
- Scan systems on the network and alerts if any logs have been deleted. (Requirement 10.2.6)
- Log user accounts and correlates them to a physical user. (Requirement 10.3.1)
- Log the type of event, alerting if an event type is a cause for concern. (Requirement 10.3.2)
- Log the date and time of events and provide a timeline of events per user and system across the network. Incident responders can also search this data and create an interactive timeline in the case of a security incident. (Requirement 10.3.3)
- Log the success or failure of each authentication event. (Requirement 10.3.4)
- Log where authentications came from, enabling incident responders to follow the trail through the network. (Requirement 10.3.5)
- Record which asset a user authenticated to. (Requirement 10.3.6)
- Continually collect logs either directly where they are generated or from a SIEM. They are uploaded to the UserInsight platform where they can no longer be altered. This platform is only accessible using unique credentials provided to each member of the security team, and it is separate from the organization's security systems. (Requirements 10.5, 10.5.1, 10.5.2, 10.5.3 and 10.5.4)
- Consume all logs, create user behavior baselines, and alert on any anomalies or suspicious activities. (Requirement 10.6)
- Alert security teams about any critical log entries and help them see the signal in the noise. For example, UserInsight can display firewall, proxy, and IDS/IPS data by user, showing users with the most alerts on the top. This provides valu-

able insight into which users exhibit suspicious activities and may have been compromised. (Requirement 10.6.1)

- Get real-time visibility into all logs and alerts about suspicious access to critical systems that deviate from baseline behavior. Accounts, assets and network zones that are defined as critical in the risk management strategy can be configured in UserInsight, to detect violations of the policy. (Requirement 10.6.2)
- Get an incident alert for each suspicious activity on the network. The security team is notified about each alert by email. UserInsight enables quick and easy investigations by searching existing logs and mapping findings on an interactive incident timeline that speeds up investigation, communication, and containment. The result of an investigation can then be exported by PDF, as well as kept within UserInsight. (Requirement 10.6.3)
- Augment the functionality of a log management tool. UserInsight can be used to investigate security incidences back to the day the solution was installed without having to pull logs from storage. (Requirement 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 (Requirements 10.3-10.4, 10.6,10.8)

Requirement 11 - Regularly test security systems and processes

11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
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).
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
11.3	Implement a methodology for penetration testing.
11.3.1/2	Perform external internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification.
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) 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.
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

Use Rapid7 Nexpose to:

- Enable internal security staff to conduct ad-hoc internal vulnerability scans. (Requirements 11.2, 11.2.3)

Use Rapid7 Metasploit to:

- Perform penetration tests either in preparation for the official security assessment or for the audit itself. (Requirements 11.3.1, 11.3.2, 11.3.3 and 11.4)

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 11.2)

- 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, 11.2.3)
- 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)
- Develop your penetration testing methodology. (Requirement 11.3)
- Develop your security policies and operational procedures. (Requirement 11.6)

Requirement 12 - Maintain a policy that addresses information security

12.1	Establish, publish, maintain, and disseminate a security policy.
12.2	Implement a risk-assessment process.
12.3	Develop usage policies for critical technologies and define proper use of these technologies.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
12.5	Assign to an individual or team the information security management responsibilities.
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)
12.8	Maintain and implement policies and procedures to manage service providers.
12.9	Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.

Use Rapid7 UserInsight to:

- Track each device and associated users, determining which users is an asset's primary user. Each user is associated with a department, location, email address and a supervisor, making it easy to contact an asset owner. (Requirement 12.3.4)
- Get full visibility about when external vendor credentials were used to connect through VPN and to which assets they connected at what time. UserInsight also detects attempts to use accounts that are currently disabled, and alerts you when the behavior is suspicious. (Requirement 12.3.9)
- Search logs for anomalies in real-time and sends out alerts to the security team by email. UserInsight enables security professionals to search and map suspicious activity on an interactive incident timeline, simplifying communication and accelerating containment and response. (Requirement 12.5.2)
- Alert if any users that are disabled in the Directory Services accesses any other associated account, including ActiveSync and cloud accounts such as Salesforce.com, Box.com, and Amazon Web Services. (Requirement 12.5.4)
- Collect and alert on logs from intrusion detection and intrusion prevention systems as well as firewalls. (Requirement 12.10.5)

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.
- 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)

08
ABOUT RAPID7

Rapid7's IT security data and analytics software and services help organizations reduce the risk of a breach, detect and respond to attacks, and build effective IT security programs. With comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques, Rapid7 strengthens an enterprise's ability to defend against everything from opportunistic drive-by attacks to advanced threats. Unlike traditional vulnerability management and incident detection technologies, Rapid7 provides visibility, monitoring, and insight across assets and users from the endpoint to the cloud. Dedicated to solving the toughest security challenges, we offer unmatched capabilities to spot intruders leveraging today's #1 attack vector: compromised credentials. Rapid7 is trusted by more than 3,500 organizations across 78 countries, including 30% of the Fortune 1000. For more information about Rapid7, please visit http://www.rapid7.com.