COMPLIANCE BRIEF

Meeting PCI DSS 3.2 Compliance with RiskSense Solutions

What’s Changing with PCI DSS?

Summary of RiskSense PCI Business Value

RiskSense provides support for PCI DSS compliance:

- *Automated vulnerability assessment of scan data with coverage for network, database, application, endpoints, and Internet of Things (IoT) devices.*
- *Threat-centric prioritization with continuous threat intelligence data feeds and analysis against assets in the environment.*
- *Industry-leading, AI-assisted penetration testing with real-time access to findings with remediation actions.*
- *Standardized business-based risk scoring, establishing a baseline and guide to measure continuous improvement.*

The Payment Card Industry (PCI) Council continues to make changes to ensure that their standards are up to date with emerging threats and changes in the market. However, as the PCI Data Security Standard (DSS) requirements continue to be clarified to help merchants and service providers, publicly known breaches continue to occur. This dilemma is driving a renewed focus on identifying high-risk vulnerabilities, priorities, remediation, and verification. Threat and vulnerability management touches many of the PCI DSS requirements, and it is an opportunity for organizations to navigate a path toward achieving continuous compliance and validation.

One of the changes to the PCI DSS is the new requirement for service providers to perform penetration testing on segment controls at least every six months. This increased frequency for validation of security controls and vulnerabilities is acknowledging the increased cyber risk these organizations face today. Annual penetration testing still remains for merchants, but how long before this might require more frequent testing?

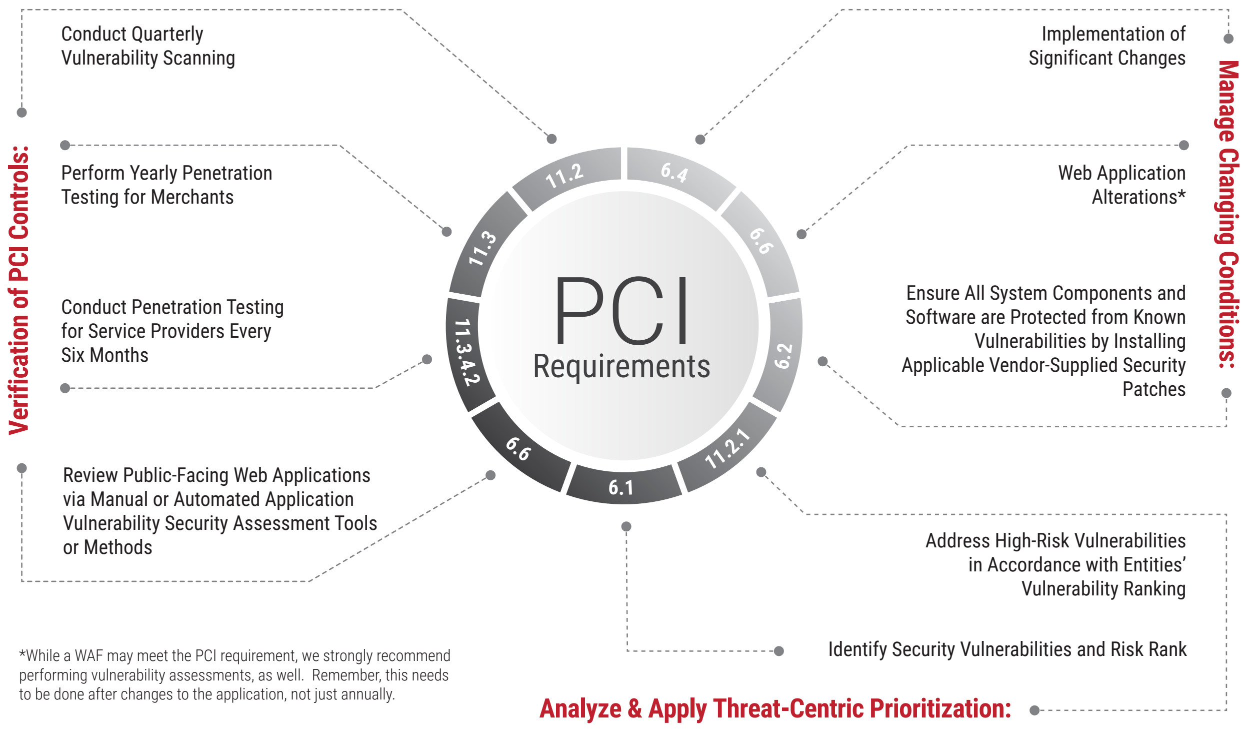
Challenges for Achieving Continuous Compliance and Validation

While each control for PCI DSS is individually called out, collectively they create a flow. The full set of controls follows a cycle. The requirements focus on protection, lifecycle management, and close-loop analysis that results in the validation of the controls. Developing effective, continuous compliance requires more than tracking and reporting progress, enumerating the mitigation efforts of identified vulnerabilities, and identifying and managing high-risk assets. The current actions of threat and vulnerability management do not necessarily lead to the validation of exposure, nor do they provide a way to measure remediation effectiveness.

Implementation of a continuous compliance program must incorporate vulnerability and threat validation as a foundational element. Its focus is to verify the key answers for PCI DSS: what’s susceptible to threats, what’s actually exposed, have the threats been remediated, and what change factors put compliance at risk. Organizations will gain the ability to quantify and measure the safety of their environments, PCI segments and others, only when this flow of continuous validation is implemented.

RiskSense Solutions Mapping to PCI Requirements

Compliance requires a combination of penetration testing and at least quarterly scanning and analysis. To address the constantly changing threat and vulnerability landscape, and identify changes in the environment that may introduce risk, a continuous approach is desired. The ultimate goal is to be able to validate risk exposure and remediation success. PCI DSS requirements produces a continuous lifecycle of threat and vulnerability validation.


Verification of PCI Controls:
Conduct Quarterly Vulnerability Scanning
Perform Yearly Penetration Testing for Merchants
Conduct Penetration Testing for Service Providers Every Six Months
Review Public-Facing Web Applications via Manual or Automated Application Vulnerability Security Assessment Tools or Methods
PCI
Requirements
11.2
6.4
6.6
6.2
11.2.1
6.1
6.6
11.3.4.2
11.3
Manage Changing Conditions:
Implementation of Significant Changes
Web Application Alterations*
Ensure All System Components and Software are Protected from Known Vulnerabilities by Installing Applicable Vendor-Supplied Security Patches
Address High-Risk Vulnerabilities in Accordance with Entities' Vulnerability Ranking
Identify Security Vulnerabilities and Risk Rank
Analyze & Apply Threat-Centric Prioritization:

*While a WAF may meet the PCI requirement, we strongly recommend performing vulnerability assessments, as well. Remember, this needs to be done after changes to the application, not just annually.

What the above brings to light is the need for an ongoing partner relationship to support and perform verification assessments and make this process as effective as possible. Doing a one-time or one-off penetration test or vulnerability scan will not get you to compliance.

Go Beyond Compliance with RiskSense Solutions

RiskSense has multiple offerings to help organizations with PCI DSS compliance and is an Approved Scanning Vendor (ASV) and listed provider. The RiskSense Platform provides visibility, prioritization, and actionable remediation recommendations to shrink attack surfaces and overall cyber risk exposure.

- Detailed attribution of all the critical vulnerabilities mapped to known exploits, malware, and exploit pulse is presented with detailed remediation action plans.
- Identify the vulnerabilities that are mostly likely to be used by adversaries to carry out infiltration and utilize post exploitation techniques to launch a successful lateral attack across the enterprise
- Provide visibility, prioritization, and actionable remediation recommendations to shrink attack surface

RiskSense Vulnerability Discovery helps merchants and service providers identify, prioritize, and provide remediation guidance to critical vulnerabilities.

- Our service provides a fully managed vulnerability assessment at monthly, quarterly, or annual intervals to swiftly and accurately identify misconfigurations and vulnerabilities on your network.
- You're provided with a detailed analysis of the assessment results, offering recommendations to remediate identified security gaps.

RiskSense Attack Surface Validation increases the organization's ability to identify and correlate for susceptible attack surface, identify indicators of attack, as well as improve the actionable intelligence of current threat feeds and extend the analysis beyond Internet exposed assets to Intranets (internal assets).

Our solution provides a fully managed validation of the vulnerabilities and bypass existing controls that are most likely to be used by cyber adversaries to carry out infiltration and utilize post-exploitation techniques to launch a successful lateral attack.

Why RiskSense?

RiskSense®, Inc. is the pioneer and market leader in threat and vulnerability management. The company provides enterprises and governments with clear visibility into their entire attack surface, including attack susceptibility and validation, as well as quantification of risks based on operational data.

The RiskSense Software-as-a-Service (SaaS) platform and related services unifies and contextualizes internal security intelligence, external threat data and business criticality to reduce cyber risk and move to a more pro-active, collaborative, and real-time discipline. It embodies hands-on expertise gained from defending critical government and commercial networks from the world's most dangerous cyber adversaries.

RiskSense Solution Summary Offerings:

RiskSense Platform

The RiskSense Platform provides visibility, prioritization, and actionable remediation recommendations to shrink your attack surface and overall cyber risk exposure.

Detailed attribution of all the critical vulnerabilities mapped to known exploits, malware, and exploit pulse is presented with detailed remediation action plans.

Identify the vulnerabilities that are mostly likely to be used by adversaries to carry out infiltration and utilize post exploitation techniques to launch a successful lateral attack across the enterprise

RiskSense Discovery

One of the primary goals is identify, prioritize, and provide remediation guidance to critical vulnerabilities before your cyber adversary can exploit them.

Our service provides a fully managed vulnerability assessment at monthly, quarterly, or annual intervals to swiftly and accurately identify misconfigurations and vulnerabilities on your network.

You're provided with a detailed analysis of the assessment results, offering recommendations to remediate identified security gaps.

RiskSense Attack Validation

Organizations require a solution that increases the organization's ability to identify and correlate for susceptible attack surface, identify indicators of attack, as well as improve the actionable intelligence of current threat feeds and extend the analysis beyond Internet exposed assets to Intranets (Internal Assets).

Our solution provides a fully managed validation of the vulnerabilities and bypass existing controls that are most likely to be used cyber adversaries to carry out infiltration and utilize post exploitation techniques to launch a successful lateral attack across your organization.

Appendix A

RiskSense Platform Offerings Mapped to PCI-DSS:

PCI Requirement	Brief Description	How Can RiskSense Assist	RiskSense Product		
			RiskSense Product	RiskSense Discovery	RiskSense Attack Validation
2.0	Do not use default passwords or security parameters	RiskSense provides visibility into system components, vulnerable services, default and misconfigurations, default user accounts, and insecure vendor default settings.	✓	✓	✓
5.1.2	Identify and evaluate evolving malware threats	RiskSense attack validation evaluates the efficacy of Antivirus systems and other controls in place to protect and defend against polymorphic and malware mutants.			✓
6.1	Establish a process to identify security vulnerabilities and assign a risk ranking	Threat Intelligence is aggregated from the Dark Web and over 60 different sources. All the identified vulnerabilities are aggregated and correlated for attack susceptibility. RiskSense prioritizes vulnerabilities based on risk, exploitability, and the ability to launch a lateral attack.	✓	✓	✓
6.2	Ensure that all components and software are protected from known vulnerabilities	RiskSense continuous assessment and validation will allow organizations to prioritize critical vulnerabilities and provide guidance on applicable patches. RiskSense validates if critical systems are being patched within 30 days.	✓	✓	✓
6.5	Address common coding vulnerabilities in software-development processes OWASP Top 10 and Top 25 Programming Errors	The vulnerabilities identified in 6.5.1 through 6.5.10 provide a minimum baseline. It is up to the organization to remain up to date with vulnerability trends and incorporate appropriate measures into their secure coding practices. RiskSense solution provides full context of vulnerabilities including common coding errors that are introduced during the development process or by using existing libraries and frameworks.		✓	✓
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. Implement a methodology for penetration testing to review public-facing web applications via manual or automated application vulnerability security assessment tools or methods.	This is an evaluation of web applications in a distinct and customized approach based on the target web application's features. We provide an in-depth understanding of how an input changes data inside the application. We use a proprietary framework to discover multiple attack vectors by passing or inputting data to user interfaces, application programming interfaces (APIs), and other places where inputs are processed.			✓
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).	RiskSense is an approved scanning vendor (ASV). Our service provides a fully managed vulnerability assessment at monthly, quarterly, or annual intervals to swiftly and accurately identify misconfigurations and vulnerabilities on your network. You're provided with a detailed analysis of the assessment results, offering recommendations to remediate identified security gaps. This includes identifying "high risk" vulnerabilities must be addressed in accordance with the entity's vulnerability ranking (as defined in Requirement 6.1), and verified by rescans.		✓	

PCI Requirement	Brief Description	How Can RiskSense Assist	RiskSense Product		
			RiskSense Product	RiskSense Discovery	RiskSense Attack Validation
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	RiskSense attack validation empowers organizations to identify and correlate for susceptible attack surface, identify indicators of attack, as well as improve the actionable intelligence of current threat feeds and extend the analysis beyond Internet exposed assets to Intranets (Internal Assets). As a part of the penetration testing and attack surface validation custom exploits and well know common hacker techniques will be used to identify indicators of attack (IOAs) against your existing environment (platforms, applications, devices, and computing elements). Our solution provides a fully managed validation of the vulnerabilities and bypass existing controls that are most likely to be used cyber adversaries to carry out infiltration and utilize post exploitation techniques to launch a successful lateral attack across your organization. The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. 11.3.4.1 New requirement for service providers to perform penetration testing on segmentation controls at least every six months. Effective February 1, 2018			✓

RiskSense Platform – the industry's most comprehensive, intelligent platform for managing cyber risk.

Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

CONTACT US

SCHEDULE A DEMO

READ OUR BLOG