

## **Using Skybox® Solutions to Achieve Efficient and Effective PCI Compliance**

*Skybox solutions help retailers, banks, service providers and others to achieve efficient and effective PCI Compliance by automating many of required controls and processes.*

### ***White Paper***

## Executive Summary

The Payment Card Industry (PCI) established a security standard called the Data Security Standard (DSS) in order to reduce the risk organizations face as related to credit card fraud, hacking and various other security issues.

A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or it risks losing the ability to process credit card payments. The penalties and sanctions for non-compliance are severe.

The requirements cover all aspects of information security: network security, data security, vulnerability management, access control, security monitoring, and information security policy best practices.

While the requirements demanded by PCI are useful and compatible with many other security best practices, they put organizations in an impossible situation. The penalties associated with the failure to comply with PCI are enormous, potentially leading to financial disaster. Conversely, the costs necessary to assure compliance are excessive due to the amount of labor required to maintain compliance.

The only solution for this unbearable trade-off is the automation of the many labor intensive tasks that are burdened by PCI DSS.

## The Skybox PCI Value Proposition

With Skybox solutions, organizations can realize savings of 75% or more in the resources required for the implementation of the PCI requirements!

Skybox is helping the largest organizations in the world protect their critical assets, customers' data, and brand by increasing the efficiency and effectiveness of their existing security layers while reducing resource requirements.

Skybox markets two product lines; **Skybox Secure** automates the lifecycle of risk management, while **Skybox Assure** streamlines network security compliance.

The common **Skybox View** platform shared across the product lines is comprehensive, modular and scalable, provides a complete security risk and compliance software package that grows with the business. It was designed from the ground up to automate inefficient and labor-intensive security and compliance processes.

Skybox solutions do not add another layer of security requiring more people or inefficient processes that produce vague results. Skybox solutions proactively reduce risk, ensure compliance and reduce cost.

## Payment Card Industry Data Security Standard (PCI DSS) Overview

PCI DSS stands for Payment Card Industry (PCI) Data Security Standard (DSS). It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues.

A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or risk fines of up to \$500,000, increased auditing requirements or even losing the ability to process credit card transactions.

These requirements apply to organizations and corporations in many industries, such as retail, banking, travel and entertainment services, telecommunication services, and many others.

The Data Security Standard requirements apply to all “**system components**” in the IT stack, which is defined as any **network component, server, or application** included in, or connected to, the cardholder data environment.

- **Network components** include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- **Servers** include, but are not limited to, Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP).
- **Applications** include all purchased and custom applications, including internal and external applications.

Each affected organization needs to be either audited or self-assessed on an annual basis, depending on the number of credit card transactions processed in a given year.

Merchants that process 6 million transactions or more per year must have an annual on-site audit by a certified third party auditor. Merchants with less than 6 million transactions are required to perform an annual self-assessment process.

In either case, in order to become compliant organizations need to perform the required security tasks on an on-going basis.

*What are the specific requirements of PCI DSS and their challenges?*



## PCI DSS Requirements & Their Challenges

The PCI Data Security Standard outlines **12 Requirements** which must be followed by each and every organization that stores, processes or transmits cardholder data.

The requirements cover all aspects of information security: network security, data security, vulnerability management, access control, security monitoring, and information security policy best practices.

While the requirements demanded by PCI are useful and compatible with many other security best practices like those published by ISO and NIST, they put the organizations in an impossible situation where penalties of non-compliance with PCI are enormous yet require significant labor resources and heavy investments to implement compliance requirements.

For example **Requirement #1 – Maintain proper firewall configurations** – is very challenging. Large organizations typically have over a hundred firewalls, which may change a few times per month. The manual process of ensuring that these firewalls are always configured according to the required policy may cost millions of dollars and can directly affect the bottom line of the business.

Another example is **Requirement #6 - All system components and software must have the latest vendor-supplied security patches installed within one month of release.**

Though this requirement appears reasonable on paper, it forces organizations into a trade-off position in which patch implementation is costly, yet the process itself may lead to system outages and downtime due to software dependencies.

The examples listed are only a few of a long list of challenges routinely faced by organizations.

### The 12 Requirements of PCI DSS

#### Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

#### Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

#### Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

#### Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

#### Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

#### Maintain an Information Security Policy

12. Maintain a policy that addresses information security

*Is there a solution for this unbearable trade-off between non-compliance penalties and excessive cost of compliance?*

## Skybox Solutions – Automated Security Risk & Compliance Management

Skybox is helping the largest organizations in the world protect their critical assets, customers' data, and brand by increasing the efficiency and effectiveness of their existing security layers while reducing resource requirements.

Skybox solutions do not add another layer of security requiring more people or new processes. Skybox solutions proactively reduce risk, ensure compliance and reduce cost.

Skybox offers two product lines: **Skybox Secure** automates the lifecycle of risk management, while **Skybox Assure** streamlines network security compliance.

The Skybox Secure product line provides a comprehensive, business-centric view of exposures to critical and regulated assets. This product line offers three core applications:

- **Risk Exposure Analyzer** - Automates risk assessment and remediation prioritization for risk reduction and resource optimization.
- **Threat Alert Manager** - Enhances productivity and reduces time in managing daily threat alerts workflow and remediation tracking.
- **Security Profile Advisor** - Measures the effectiveness of vulnerability and remediation programs with KPI generation and trends derived from multiple sources.

The Skybox Assure product line provides a comprehensive, scalable solution that drives the cost of network security compliance down, while improving the availability and security of the network. This product line offers three core applications:

- **Firewall Compliance Auditor** – Automates the on-demand firewall compliance and rule usage analysis process.
- **Network Compliance Auditor** – An automated and holistic network policy compliance and visualization solution.
- **Change Assurance Manager** – Change assurance workflow beginning at the receipt of the change request, through the impact analysis, and to the post-deployment validation.

All of the above applications play a critical role in effective and efficient PCI Compliance as explained in the next section.

More information about Skybox's solutions can be found at: [www.skyboxsecurity.com](http://www.skyboxsecurity.com).



## Efficient and Effective PCI DSS Compliance with Skybox Solutions

This section is intended for the audience who seeks solutions for specific PCI challenges.

The following table provides the high level mapping between the PCI DSS requirements, and the challenges solved by Skybox. Each of the challenges and solutions is further explained in a dedicated sub-section.

PCI DSS Requirement	Challenges Solved by Skybox's Solutions
<a href="#"><u>1: Install and maintain a firewall to protect cardholder data</u></a>	<ul style="list-style-type: none"> <li>- Costly, non-scalable, and error-prone firewall audits</li> <li>- Tough to maintain current network diagrams</li> <li>- Need to demonstrate on-going firewall change assurance</li> <li>- Need to demonstrate network access policy consistent with PCI guidelines</li> </ul>
<a href="#"><u>6: Develop and maintain secure systems and applications</u></a>	<ul style="list-style-type: none"> <li>- Costly and sometimes dangerous patch deployment process</li> <li>- Need to provide proof that compensating controls achieve acceptable risk mitigation</li> <li>- Non-scalable threat &amp; vulnerability alert management process</li> <li>- Non-scalable change management requirements for impact analysis and documentation</li> </ul>
<a href="#"><u>11: Regularly test security systems and processes</u></a>	<ul style="list-style-type: none"> <li>- Costly, non-scalable testing of network security controls for attack mitigation</li> <li>- Costly and limited penetration testing process</li> <li>- Need to provide proof that vulnerability management for all layers of the IT stack is performed per requirements (quarterly and after every major change)</li> </ul>
<a href="#"><u>12: Maintain a policy that addresses information security</u></a>	<ul style="list-style-type: none"> <li>- Formal risk assessment is required annually</li> <li>- Formal policy is required for network security configurations and vulnerability &amp; threat management</li> <li>- For service providers – effective and efficient way to ensure PCI compliance for connected entities</li> </ul>



### **Requirement 1: Install and Maintain a Firewall to Protect Cardholder Data**

Challenge	Skybox Solution
<i>Costly, non-scalable, and error-prone audit of the access rule sets of firewalls</i>	<b>Skybox Firewall Compliance Auditor (FCA)</b> performs fully automated firewall configuration audits and rule usage analysis, according to the PCI access requirements and corporate policies. Skybox's solutions can save 75% or more of required resources.
<i>Tough to maintain updated network diagrams</i>	<b>Skybox Network Compliance Auditor (NCA)</b> performs full network modeling and visualization. Provides information on all possible access routes in the network given routing tables, firewall rules, NAT tables, for heterogeneous network environments.
<i>Need to demonstrate on-going firewall change assurance</i>	<b>Skybox Change Assurance Manager (CAM)</b> automates and documents the change assurance workflow from the receipt of change request to post-deployment validation. This process automation can save 75% or more of the required resources. (Scheduled release: 2008)
<i>Need to demonstrate network access policy consistent with PCI guidelines</i>	Skybox solutions ( <b>FCA &amp; NCA</b> ) are delivered with out-of-the-box network access policy per PCI requirements. In addition, the solutions allow organizations to document their own policies for network availability (i.e. permitted traffic) and security.

[Detailed list of Skybox-enabled solutions for Requirement 1 can be found in Appendix A.](#)

### **Requirement 6: Develop and Maintain Secure Systems and Applications**

Challenge	Skybox Solution
<i>Costly and sometimes dangerous patch deployment process</i>	<b>Skybox Risk Exposure Analyzer (REA)</b> can reduce patching pressure by assessing where the actual risks are (i.e. where no compensating controls exist), and therefore focus the patching work only where needed – saving up to 90% of required resources.
<i>Need to provide proof that compensating controls achieve acceptable risk mitigation</i>	<b>Skybox Risk Exposure Analyzer (REA)</b> automatically assesses the effectiveness of the technical controls, and whether they mitigate the critical risks.
<i>Non-scalable threat &amp; vulnerability alert management process</i>	<b>Skybox Threat Alert Manager (TAM)</b> automates the threat alert handling process - starting by normalizing threat alerts, guiding remediation, and tracking the effective completion of required remediation – saving 75% or more of resources required.
<i>Non-scalable change management requirements for impact analysis and documentation</i>	All Skybox solutions (for risk lifecycle management and network security compliance) support "what-if modeling." This capability enables scalable impact analysis for every change in the IT environment before the change is implemented.

[Detailed list of Skybox-enabled solutions for Requirement 6 can be found in Appendix A.](#)

**Requirement 11: Regularly Test Security Systems and Processes**

Challenge	Skybox Solution
<i>Costly, non-scalable testing of network security controls for attack mitigation</i>	<b>Skybox Risk Exposure Analyzer (REA)</b> automatically simulates all attack vectors given threats, vulnerabilities, network topology, and the compensating controls (such as firewalls, and IPS). This simulation validates that all relevant high-risk attacks can be mitigated.
<i>Costly and limited penetration testing process</i>	<b>Skybox Risk Exposure Analyzer (REA)</b> automatically simulates all attack vectors given threats, vulnerabilities, network topology, and the compensating controls (such as firewalls, and IPS). The results of the simulation provide a very wide and deep "virtual penetration testing" without touching or affecting the actual network.
<i>Need to provide proof that vulnerability management for all layers of the IT stack is performed per requirements (quarterly and after every major change)</i>	<b>Skybox Security Profile Advisor (SPA)</b> normalizes all vulnerability and patch data, and provides KPI and trends for the vulnerability and remediation program within the organization. SPA also provides complete documentation for all current and historical vulnerabilities and remediation. SPA receives its input from any vulnerability scanner and patch management applications.

[Detailed list of Skybox-enabled solutions for Requirement 11 can be found in Appendix A.](#)

**Requirement 12: Maintain a Policy that Addresses Information Security**

Challenge	Skybox Solution
<i>Formal risk assessment is required annually</i>	<b>Skybox Risk Exposure Analyzer (REA)</b> performs automated risk assessment based on industry standard methodologies such as NIST SP 800-30, and others.
<i>Formal policy is required for network security configurations and vulnerability &amp; threat management</i>	<p><b>Skybox Firewall Compliance Auditor (FCA)</b> and <b>Network Compliance Auditor (NCA)</b> provide documentation for the network access policies in the organization.</p> <p><b>Skybox Security Profile Advisor (SPA)</b> captures the vulnerability level and remediation latency policy of the organization.</p>
<i>For Processors and Service Providers – effective and efficient way to ensure PCI compliance for connected entities</i>	All Skybox solutions are available also in an ad-hoc Project Mode, which allows service providers to audit the connected entities for the compliance with the PCI DSS requirements.

[Detailed list of Skybox-enabled solutions for Requirement 12 can be found in Appendix A.](#)

## Summary

Companies that process, store, or transmit credit card numbers face real day-to-day challenges in implementing the requirements as specified by the PCI DSS.

Today's manual techniques introduce an unbearable trade-off to these organizations – severe penalties for non-compliance or heavy cost in becoming compliant.

The only cost effective solution for PCI DSS compliance is the introduction of automation for the day-to-day security management processes.

Skybox Security is the only vendor that provides an automated, comprehensive suite of solutions that address many of the challenges in PCI DSS, turning them from a heavy burden into useful proactive security management best practices.

## References

- Payment Card Industry (PCI) Data Security Standard - Version 1.1 (Release: September 2006)
- Payment Card Industry (PCI) Data Security Standard - Security Audit Procedures (Release: September 2006)
- PCI Security Standards Council site: <https://www.pcisecuritystandards.org/index.htm>
- VISA Security guidelines:  
[http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html](http://usa.visa.com/merchants/risk_management/cisp_overview.html)
- Skybox Security website: <http://www.skyboxsecurity.com/>



## Appendix A – Detailed List for Skybox-Enabled PCI DSS Tasks

Skybox solutions solve many of the challenges outlined by PCI DSS. These solutions assist in automation, verification, and/or documentation for the requirements checked in the table below:

<b>Requirement 1: Install and Maintain a Firewall to Protect Cardholder Data</b>	<b>Skybox-Enabled</b>
1.1 Establish firewall configuration standards that include the following:	√
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	√
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	√
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	√
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	
1.1.5 Documented list of services and ports necessary for business	√
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	√
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	√
1.1.8 Quarterly review of firewall and router rule sets	√
1.1.9 Configuration standards for routers.	
1.2 Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.	√
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:	√
1.3.1 Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)	√
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ	√
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only “established” connections are allowed into the network)	
1.3.4 Placing the database in an internal network zone, segregated from the DMZ	√
1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	√
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	√
1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic	√
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.	
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	√
1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic	√
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	√



<b>Requirement 1: Install and Maintain a Firewall to Protect Cardholder Data</b>	<b>Skybox-Enabled</b>
<b>1.5</b> Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	√

<b>Requirement 6: Develop and maintain secure systems and applications</b>	<b>Skybox-Enabled</b>
<b>6.1</b> Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	√ Skybox can validate that the right patches are installed on time
<b>6.2</b> Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	√
<b>6.3</b> Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle. <i>[List omitted as irrelevant for Skybox]</i>	
<b>6.4</b> Follow change control procedures for all system and software configuration changes. The procedures must include the following:	√
<b>6.4.1</b> Documentation of impact	√
<b>6.4.2</b> Management sign-off by appropriate parties	√ For network changes
<b>6.4.3</b> Testing of operational functionality	√ For network changes
<b>6.4.4</b> Back-out procedures	
<b>6.5</b> Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following: <i>[List omitted as irrelevant for Skybox]</i>	
<b>6.6</b> Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: <ul style="list-style-type: none"> <li>• Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security</li> <li>• Installing an application layer firewall in front of web-facing applications.</li> </ul>	

<b>Requirement 11: Regularly Test Security Systems and Processes</b>	<b>Skybox-Enabled</b>
<b>11.1</b> Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	√ Wireless analysis is not supported at this point
<b>11.2</b> 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).	√ Skybox isn't a scanner, but a consolidator of vulnerability data from many sources
<b>11.3</b> Perform 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:	√ Skybox performs highly scalable "virtual penetration testing" without affecting/touching the actual IT environment.
<b>11.3.1</b> Network-layer penetration tests	√
<b>11.3.2</b> Application-layer penetration tests.	



<b>Requirement 11: Regularly Test Security Systems and Processes</b>	<b>Skybox-Enabled</b>
<b>11.4</b> Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	
<b>11.5</b> Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.	

<b>12: Maintain a Policy that Addresses Information Security</b>	<b>Skybox-Enabled</b>
<b>12.1</b> Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	√ For network access policy
<b>12.1.1</b> Addresses all requirements in this specification	√ According to the checks in this appendix
<b>12.1.2</b> Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment	√
<b>12.1.3</b> Includes a review at least once a year and updates when the environment changes.	√
<b>12.2</b> Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	
<b>12.3</b> Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following: <i>[List omitted as irrelevant for Skybox]</i>	
<b>12.4</b> Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	
<b>12.5</b> Assign to an individual or team the following information security management responsibilities: <i>[List omitted as irrelevant for Skybox]</i>	
<b>12.6</b> Implement a formal security awareness program to make all employees aware of the importance of cardholder data security. <i>[List omitted as irrelevant for Skybox]</i>	
<b>12.7</b> Screen potential employees to minimize the risk of attacks from internal sources. <i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	
<b>12.8</b> If cardholder data is shared with service providers, then contractually the following is required: <i>[List omitted as irrelevant for Skybox]</i>	
<b>12.9</b> Implement an incident response plan. Be prepared to respond immediately to a system breach. <i>[List omitted as irrelevant for Skybox]</i>	
<b>12.10</b> All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:	√
<b>12.10.1.</b> Maintain a list of connected entities	
<b>12.10.2.</b> Ensure proper due diligence is conducted prior to connecting an entity	√
<b>12.10.3.</b> Ensure the entity is PCI DSS compliant	√
<b>12.10.4.</b> Connect and disconnect entities by following an established process.	