PCI DSS Compliance Without the Headache
Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide standard established by five major credit card companies—Visa, MasterCard, Discover, American Express, and JCB—to enhance and enforce security in processing credit cards. By mandating controls around the storage, transmission and processing of cardholder data, PCI DSS aims to help vendors and retailers protect sensitive customer data and reduce card fraud during and after online transactions. Annual validation of compliance is required by the major payment brands and is determined by either a qualified security assessor or through a self-assessment questionnaire, depending on the organization’s volume of transactions.
Any organization that processes credit or debit card data will require some level of PCI DSS adherence. Specifics will vary depending on organization type (e.g., retailer, service provider, bank) and transactional volumes. For detailed PCI DSS requirements as they pertain to your organization, please see the PCI DSS 3.1 Requirements and Security Assessment Procedures. Version 3.2 of PCI DSS is slated for release in March/April 2016.

PCI DSS is not a federally mandated compliance measure. That said, payment brands will levy significant fines on organizations that fail to meet PCI DSS requirements. Furthermore, some US states have adopted part of PCI DSS into their legal frameworks or have even instituted the entire standard into state law. For example, both Nevada and Washington State have incorporated PCI DSS requirements into their laws and mandate that in-state merchants comply with PCI DSS. Specific state and local requirements may vary, but adherence usually shields compliant entities from liability (at least in part) in the event of a data breach. Above all else, PCI DSS enforces strong IT security controls around sensitive data—standards that organizations should strive for even in the absence of legislation and/or potential fines.
PCI DSS consists of 12 main requirements designed to satisfy a myriad of security objectives, including building and maintaining a secure network, protecting stored cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining information security policies. These requirements essentially satisfy what payment brands feel are basic controls for effective assessment, remediation, and reporting as related to securing sensitive customer information. Depending on an organization’s unique infrastructure and specific environment for cardholder data, certain controls may or may not apply.

Please note that though the 12 primary requirements for PCI DSS have not changed since the standard’s inception, more than 400 controls and sub-controls have been added since. The complete PCI DSS 3.1 Requirements and Security Assessment Procedures contains up-to-date specifications and controls/sub-controls that may apply to your organization.

Again—the 12 requirements stipulated by PCI DSS have not changed since their creation, but a plethora of controls and sub-controls have been added to address new innovations and the evolving threat landscape. For example, more granular requirements have been created for merchants or vendors handling larger transactional loads, and revisions and additions have been made to account for newer technologies such as wifi, mobile devices, virtualization, and cloud computing.
<table>
<thead>
<tr>
<th><strong>Goal</strong></th>
<th><strong>Requirement</strong></th>
</tr>
</thead>
</table>
| **Build and Maintain a Secure Network** | Install and maintain a firewall configuration to protect cardholder data.  
Do not use vendor-supplied defaults for system passwords and other security parameters. |
| **Protect Cardholder Data** | Protect stored cardholder data.  
Encrypt transmission of cardholder data across open, public networks. |
| **Maintain a Vulnerability Management Program** | Use and regularly update anti-virus software or programs. |
| **Implement Strong Access Control Measures** | Develop and maintain secure systems and applications.  
Restrict access to cardholder data by business need to know.  
Assign unique ID to each person with computer access.  
Restrict physical access to cardholder data. |
| **Regularly Monitor and Test Networks** | Track and monitor all access to network resources and cardholder data.  
Regularly test security systems and processes. |
| **Maintain an Information Security Policy** | Maintain a policy that addresses information security for all personnel. |
The 12 major requirements specified in PCI DSS are structured under six key areas/goals to ensure that the most comprehensive measures are taken to secure cardholder transaction and personal data.

**Build and Maintain a Secure Network**

**Requirement 1:**
Install and maintain a firewall and router configuration to protect cardholder data. Properly functioning firewalls and correctly configured routers comprise the critical first layers of network defense of an organization’s IT infrastructure. Compliance with this item will require a demonstration of the above, with appropriate testing and validation measures in place to ensure expected operations are indeed functioning. UpGuard can scan and validate that firewalls are routers are configured correctly through comprehensive change monitoring and policy-driven testing.

**Requirement 2:**
Do not use vendor-supplied defaults for system passwords and other security parameters. Many intrusions and data breaches are the result of unchanged default passwords or system software settings in payment card systems or architectures. Since most default administrator passwords, application service passwords, and system monitoring passwords for leading products are widely known and accessible, changing or removing factory-set credentials is an integral preliminary step when deploying applications or devices. Furthermore, controls should be instituted to verify that default logins do not exist in the environment. Using UpGuard to automatically scan and monitor for the existence of vendor-supplied defaults can satisfy this requirement.

**Protect Cardholder Data**

**Requirement 3:**
Protect stored cardholder data. Any cardholder data stored in the systems must be encrypted. In this case, the shortest path to compliance is determining where credit card data is stored and encrypting it before saving. PCI DSS stipulates that cardholder data must be rendered unreadable before saving to disk, so these encryption requirements apply to any type of storage media: portable media storage, backup media and the like. As Requirement 3 only applies to organizations that store cardholder data on their systems, many merchants have circumvented this by opting to not saving credit card data at all. PCI DSS actually prefers this, since not storing cardholder data by default translates to stronger protection.

**Requirement 4:**
Encrypt transmission of cardholder data across open, public networks. When credit card information is transmitted over public networks like the internet (e.g., submitting a web form with payment details), encryption methods such as SSL must be used to protect the data. Additionally, wireless networks using the WEP encryption standard are no longer allowed to transmit credit card data of any type. Through policy-driven testing, UpGuard can monitor and verify that encryption mechanisms are indeed working as expected.
Maintain a Vulnerability Management Program

Requirement 5:
Use and regularly update antivirus software or programs. Malicious software such as malware and viruses are standard tools in a hacker’s arsenal, often enabling advanced persistent threats (APT) and multi-pronged attacks to be orchestrated at a later date. Anti-virus software is therefore a critical component of IT security, but like all applications—must be regularly updated and patched to maintain its effectiveness. UpGuard ensures that antivirus programs are regularly accounted for in patch management initiatives through tools for collaborative change management and post-deployment patch testing.

Requirement 6:
Develop and maintain secure systems and applications. In an increasingly complex and integrated world of applications and services, maintaining a comprehensive view of security is a major challenge. Review the alerts of all the software vendors used in your systems and apply their patches methodically. If the application has been customized, patching can be very difficult as the extended code may be affected by the patch. In this situation, the application needs to be properly tested to see whether the application is vulnerable and then a plan must be put in place to address any issues. In addition, organisations with customised applications should consider conducting a vulnerability assessment. UpGuard’s policy-driven testing and OVAL-backed vulnerability scanning and monitoring can satisfy this requirement.

Implement Strong Access Control Measures

Requirement 7:
Restrict access to cardholder data by business need-to-know. All access to critical cardholder data should be restricted and recorded. For example, access should only be given to staff explicitly requiring credit/debit card details. Remember—through the use of encryption and directory access controls, it is possible to allow administrators and support staff appropriate access to the services they need without revealing sensitive data. Additionally, all access should be documented and regularly audited. UpGuard can track all access to files and applications to ensure that only authorized access is permitted.

Requirement 8:
Assign a unique ID to each person with computer access. It’s a well-known fact that the majority of data breaches originate from inside the corporate network. Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by—and can be traced to—known and authorized users. All remote users should access corporate data and applications via two factor authentication (e.g. tokens or smartcards). Devices should be logged off after a period of inactivity. Passwords should be routinely tested to prove they are unreadable during transmission and storage. UpGuard’s detailed reporting gives organizations the answers to questions such as “who accessed the application or network and when?”

Requirement 9:
Restrict physical access to cardholder data. Physical access to any building needs to be via a
reception area with all visitors and contractors signing in. All devices that store or could store credit card details must be in a secure environment. Server rooms need to be locked with CCTV installed. Access to the wireless and wired network components must be restricted. UpGuard can test and monitor physical security devices such as IP cameras to ensure that they are properly configured and working as expected.

**Regularly Monitor and Test Networks**

**Requirement 10:**
Track and monitor all access to network resources and cardholder data. The logs of all network and device activity need to be recorded and analysed for anomalies. They need to be stored in a manner that provides tracking of legitimate access, intrusions, and attempted intrusions. The logs must be available as material evidence in the event of a breach. UpGuard can integrate with leading log analysis and SIEM solutions to satisfy this requirement.

**Requirement 11:**
Regularly test security systems and processes. Organizations affected by PCI DSS should conduct regular vulnerability scans for possible exploitable weaknesses in their environments. When there are significant changes to the network, device operating systems, or applications, organizations should run internal and external vulnerability scans to check for exploitable security flaws. UpGuard satisfies this requirement by automatically scanning the entire infrastructure for vulnerabilities through comprehensive OVAL-backed testing. The platform’s continuous monitoring capabilities ensure that all systems and applications are free from security flaws on an ongoing basis.

**Requirement 11.5:**
Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert 24 personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution. UpGuard’s file integrity monitoring (FIM) feature will alert you automatically when suspicious changes are detected in critical files. This—combined with the platform’s policy-based validation system—gives organizations a fully integrated, one-stop integrity monitoring solution.

**Maintain an Information Security Policy**

**Requirement 12:**
Maintain a policy that addresses information security for all personnel. Virtually all businesses transact digitally these days. For this reason, organizations need to include IT security in their overall policies and risk management strategies. Ownership of these initiatives must be assigned to a person or group within the organisation. A strong security policy sets the tone for the entire company and informs employees of what is expected of them. Some of the areas addressed include remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and mobile devices, among others. Additionally, service providers should also be monitored and managed. With UpGuard in place as the system of record for the organization’s IT infrastructure, more accurate policies and precise documentation can be created to support policies and risk management strategies.
Conclusion

Since the inception of PCI DSS, organizations have struggled to understand, implement, and comply with its guidelines. The standard—albeit burdensome—is critical for thwarting cyber attackers in today’s evolving threat landscape. By providing more prescriptive security measures around the protection of cardholder data, PCI DSS establishes and enforces a base level of security for organizations under its guidance. It’s worth noting that PCI DSS’ guidelines represent the minimum security controls necessary for compliance, as opposed to optimal levels required for successfully repelling cyber attacks on an ongoing basis. Ultimately, the unique makeup and characteristics of an organization’s infrastructure determines the efficacy of its existing security mechanisms. In all cases, a layered approach that combines continuous monitoring and policy-based testing/validation is required for maintaining a strong security posture. To this end, UpGuard’s platform for integrity monitoring validates that your systems and applications are available, secure, and PCI DSS compliant on an ongoing basis.
Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world’s first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.