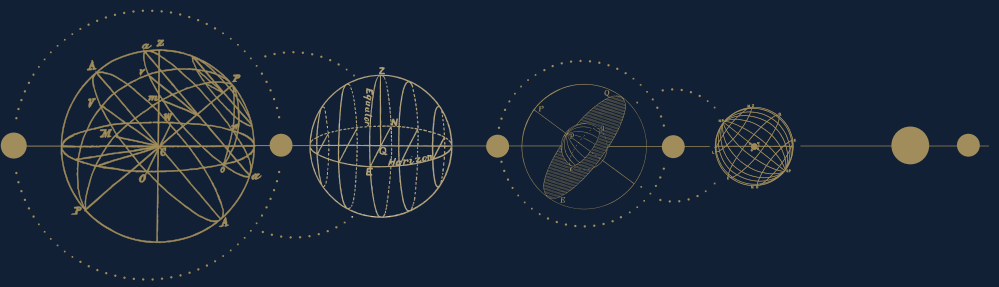
A Journey to PCI Compliance Success



For organizations that process, store or transmit credit card data



DRUMMOND

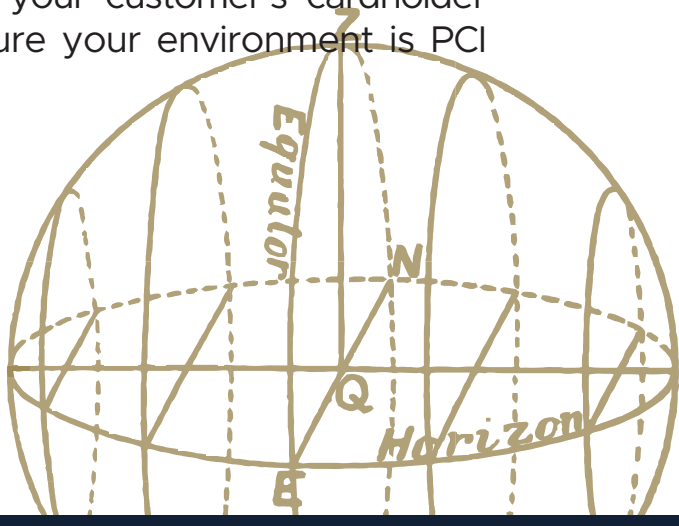
Introduction

PCI (Payment Card Industry) Compliance ensures that you can protect your business and your customers against payment card data theft and misuse. With the rise in eCommerce and email and phishing schemes, new opportunities arose for cyber criminals to infiltrate merchant and service provider networks and steal credit card data.

According to **Verizon's 2019 Payment Security Report**, only 36.7% of organizations examined for its annual global study were found to be fully compliant with PCI in 2018 - down nearly 16 % from 2017 findings.

Compliance with PCI Data Security Standard (DSS) is not required by federal law in the United States. However, the laws of some U.S. states, including Nevada, Minnesota, and Washington, have incorporated PCI DSS into their state laws, while other states have made equivalent provisions. When you sign your payment card contract—and confirm your desire to accept credit and debit cards at your business—you agree to follow card brand rules. To safely accept Visa, MasterCard, JCB, American Express, and Discover transactions, you must comply.

If you are a merchant or service provider and offer the option to use a credit card with your customers, clients, and patients where you process, store and transmit credit card data, or if you are a service provider that could impact the security of your customer's cardholder data environment, you are required to ensure your environment is PCI compliant.

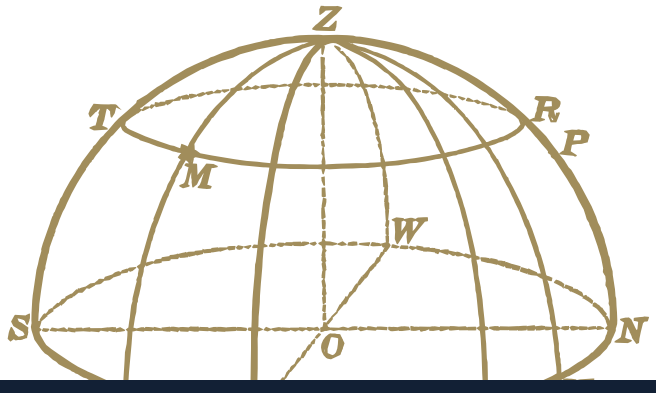


PCI Data Security Standard:
High Level Overview

The following table provides a high-level overview of the PCI DSS.

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regulatory 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 for all personnel

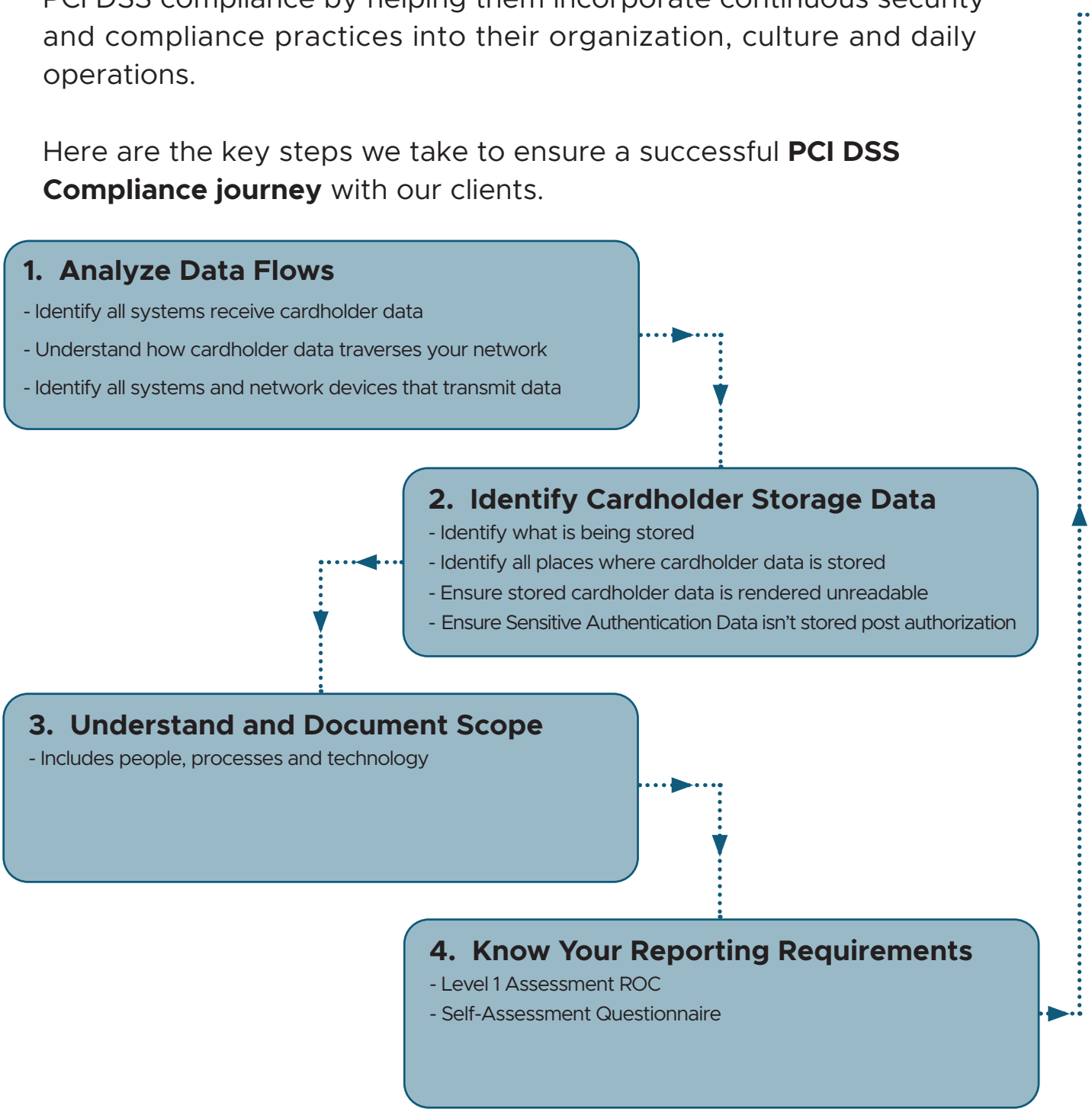
As payment methods and technologies have evolved, so has the PCI DSS. While the PCI DSS v3.2.1 is the last version, PCI-DSS v4.0 is coming with the expected final publication in 2021.



The PCI DSS Journey

At Drummond, we enable our clients take a security first approach to PCI DSS compliance by helping them incorporate continuous security and compliance practices into their organization, culture and daily operations.

Here are the key steps we take to ensure a successful **PCI DSS Compliance journey** with our clients.



5. Document Everything

- Practice what you document
- Policies and procedures need to be enforced
- Avoid repeating the PCI Requirement in a policy without practice
- Maintain System and Software Inventories

6. Use PA-DSS Validated Applications

- Always use PCI compliant Service Providers
- Provides confidence that use will not jeopardize your compliance
- May help reduce your scope

7. Correct Deficiencies

- Vulnerabilities
- Issues identified in self-reviews

8. Think About Compensating Controls

- Only use if there is a legitimate business or technical constraint
- Must meet the intent of the original control
- Must go above and beyond all other required controls

9. Get Management Support - This Can Not Be Done Alone

10. Review and Maintain Your Compliance Program Regularly

Work With A Proven Partner

With one of the longest running PCI compliance practices in the industry, we are ready to help you protect payment card data and ensure compliance. Our PCI Compliance services include the following:

PCI Assessment Service: Drummond Qualified Security Assessors (QSAs) engage to understand your business requirements, cardholder data storage, processing, and transmission processes, and optimize your assessment scope and reporting. We bring practical compliance project experience to help you achieve your immediate compliance goals, with a view to easing future recertification efforts.

PCI DSS Gap Analysis: Drummond high-skilled experts will evaluate your readiness for an assessment, working with your team we develop a customized report of prioritized remediation needs required for compliance. Our gap analysis provides actionable findings with an easily understandable summary and supporting detail mapped to each affected PCI DSS requirement, to simplify your remediation efforts.

PCI SAQ Advisory Services: Once you complete the PCI Self-Assessment Questionnaire (SAQ), our PCI experts help you define your scope for testing, give advice on SAQ responses, and review your completed SAQ prior to submission, to help ensure successful self-submission.

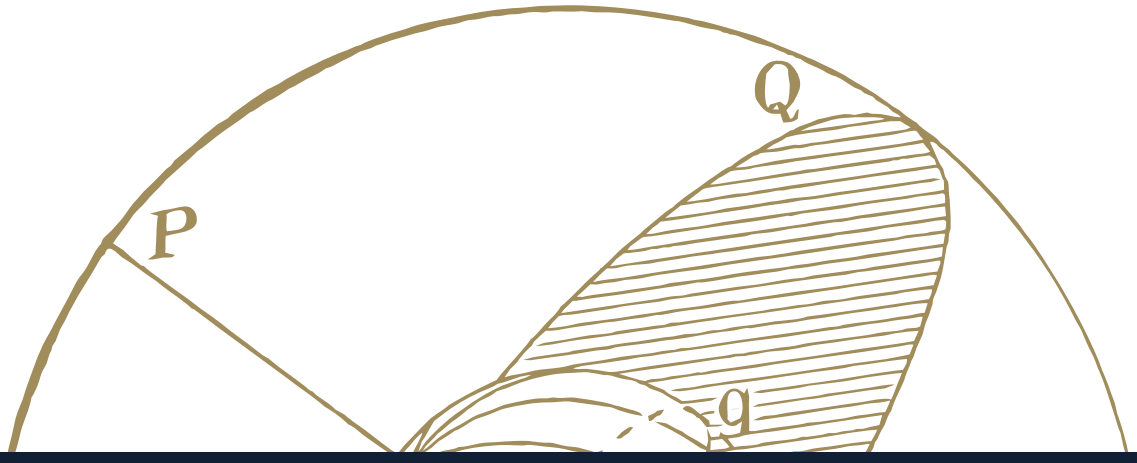
PCI QSA General Consulting Services: Need to assess the impact of upgrades to your cardholder data environment? Looking to reduce scope of assessment? Drummond general advisory services include security policy review, PCI compliance planning, risk assessment advisory, review, and advice with respect to the implementation of PCI environments and applications.



PCI Continuous Compliance Services: Drummond's team of PCI experts help you maintain compliance throughout the year to avoid unexpected issues and complexities when it's time to re-certify. Our QSAs work with you to plan, develop, manage and maintain your PCI compliance program; ensuring completion of daily, weekly, monthly, quarterly, semi-annual and annual tasks, as well as monthly, quarterly and annual validation touch points to maintain compliance through the year. This service includes the Annual PCI Assessment and Report on Compliance, as well as any remediation validation required.

PCI Payment Application (PA) DSS Assessment Service: Drummond team of experts provide assessment, gap analysis, remediation, and change impact analysis services, as well as general consultation services for developers of payment applications that handle cardholder data, we. For change impact analysis, our QSAs consult PA-DSS Program Guide requirements to ease Security Standards Council (SSC) review and listing updates.

Penetration Testing Services: Together with Lares, our strategic cybersecurity partner, we offer best-in-class Penetration Testing services that meet the full scope of recommendations put forth by the Penetration Test Guidance Special Interested Group per the PCI SSC Information Supplement Penetration Testing Guidance report (September 2017).

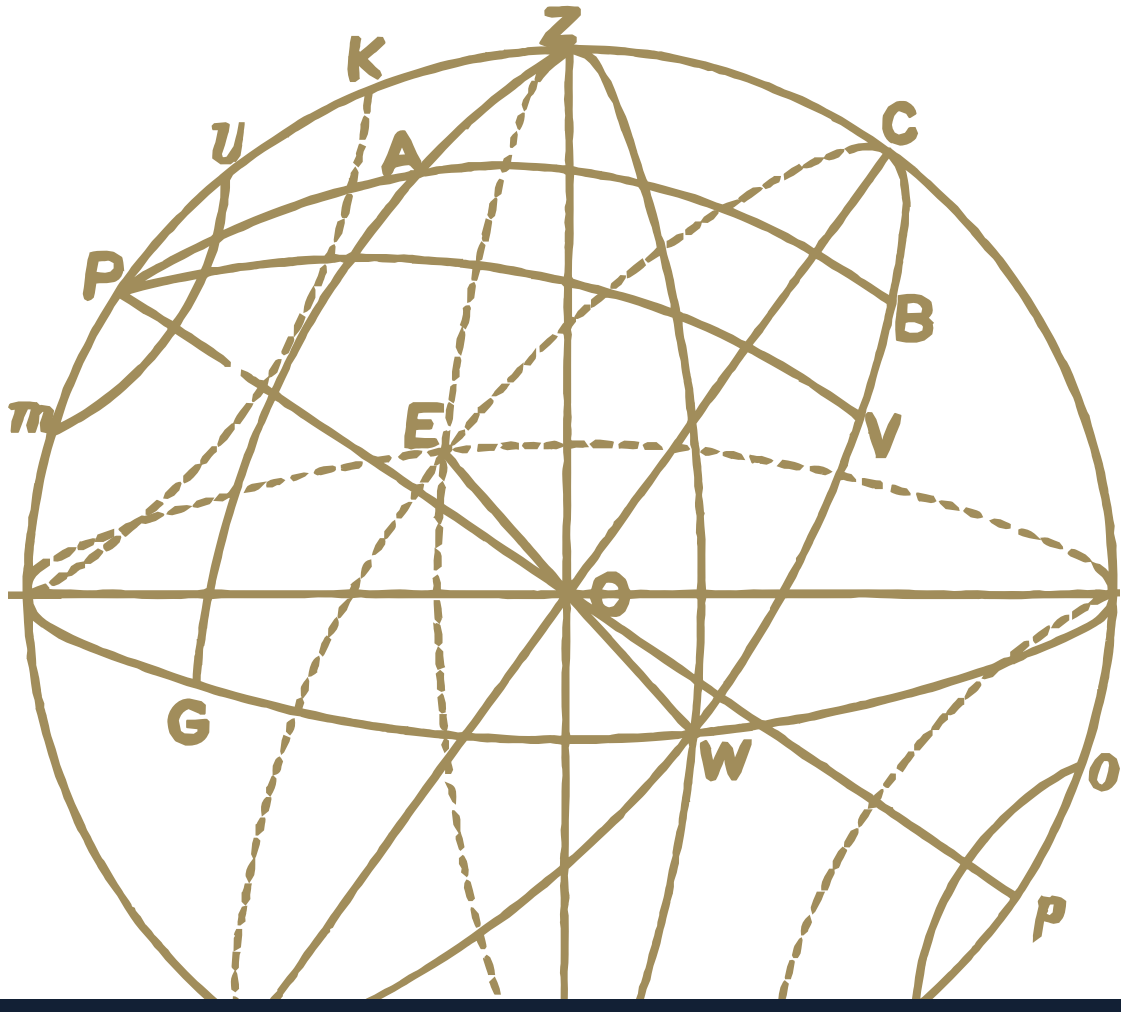


Ensure PCI Success Today

Ready to ensure PCI compliance with a trusted partner?

We are ready to help you achieve PCI DSS compliance and be prepared for regulatory information security mandates. Experience our team of highly skilled experts – having completed over 280 assessments -- ready to collaborate with you and your team on your PCI compliance needs. Increase trust, gain expertise and experience our unique approach and attention to detail with the following services. The people of Drummond are here to help you ensure compliance and protect what matters most. Let's start a conversation to see how we can help drive your business forward.

Contact us at **sales@drummondgroup.com**



DRUMMOND



Copyright © 2020, Drummond Group