qmulos

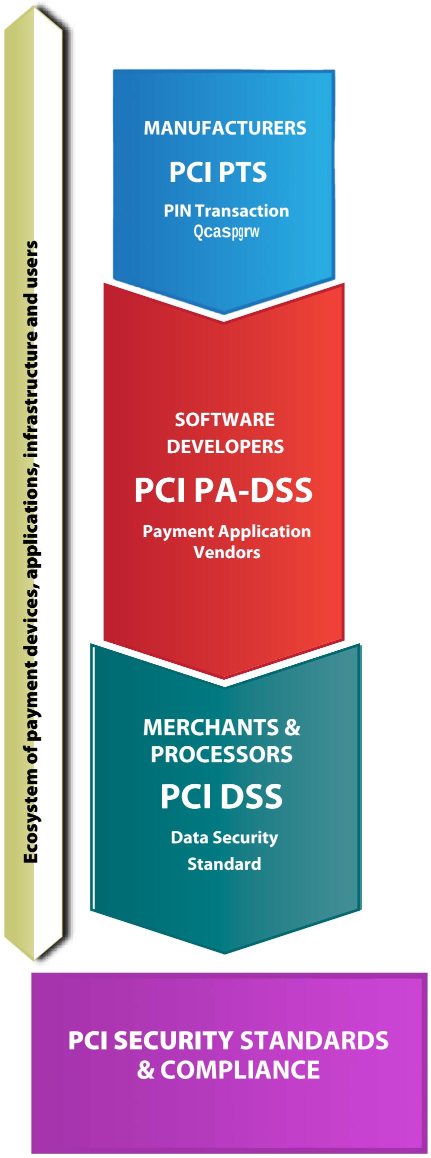
Q-GUIDE: PCI DSS

PCI DSS: Q-Compliance

REAL-TIME RISK MANAGEMENT & CON-MON COMPLIANCE FOR THE PAYMENT CARD INDUSTRY

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

MANUFACTURERS

PCI PTS

PIN Transaction Qcaspgrw

SOFTWARE DEVELOPERS

PCI PA-DSS

Payment Application Vendors

MERCHANTS & PROCESSORS

PCI DSS

Data Security Standard

PCI SECURITY STANDARDS & COMPLIANCE

Level 1: Merchants processing over 6 million card transactions per year.

Level 2: Merchants processing 1 to 6 million transactions per year.

Level 3: Merchants handling 20,000 to 1 million transactions per year.

Level 4: Merchants handling fewer than 20,000 transactions per year.

According to the FBI, there have been 72,295 violent bank robberies since 2005. However, in the same time period, there have been over 234 million sensitive record data breaches. Banks have been, and will continue to be the main target for financial crimes... because that's where the money is.

The **Payment Card Industry Data Security Standard (PCI DSS)** was put in place to protect cardholder data. The PCI Council was established by American Express, Discover, JCB International, MasterCard and Visa. As merchants for payment card transactions, banks need to use standard security procedures and technologies to protect cardholder data.

According to the PCI Security Standards Council, "PCI DSS is a set of universally accepted standards that help protect the safety of customer data." PCI DSS sets the operational and technical requirements for organizations accepting or processing payment transactions, as well as for software developers and manufacturers of the applications and devices used in those transactions.

Put simply, any business entity that is involved in accepting, processing, and storing payment card information is required to comply with PCI DSS. In the 21st Century, this is basically any and all businesses.

Furthermore, compliance can be broken into 3 parts. As seen in the graphic to the left, PCI requirements are separated into PIN Transaction (PTS) Security Requirements, Payment Application Data Security Standard (PA-DSS), and PCI Data Security Standard (DSS).

The PTS requirements cater to the design, manufacturing, and delivering of the device to the facility that implements the transaction; ie the device you swipe your card on in the grocery store. However, the PA-DSS covers virtual transactions on applications and different softwares that store cardholder data; think PayPal, ApplePay, or any given website. Finally, DSS is required for all entities that store, process or handle cardholder data in anyway.

What are the consequences?

Noncompliance may result in a fine of $5,000 to $500,000 for the acquiring bank. The bank then passes the fines along to the offending merchant.

Who will validate my compliance?

Proving compliance with PCI DSS can be achieved through two ways. You can either answer a self assessment questionnaire or have an external 3rd party annually audit your organization. Note: some banks and card brands may impose additional stipulations before they can declare your organization a level 1, 2, 3, or 4.

These rules are a lot to digest. PCI DSS compliance is a critical operational requirement for any covered organization. Amid all of the day to day business hustle and bustle, meeting these requirements frequently becomes a check-box exercise, leaving your organization, customer data, and company reputation vulnerable. The bottom line: making PCI DSS compliance a priority is essential. Compliance can be challenging and painful, but it doesn't have to be.

Your job as information security personnel should and can be easier!

The 12 requirements of PCI DSS

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
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

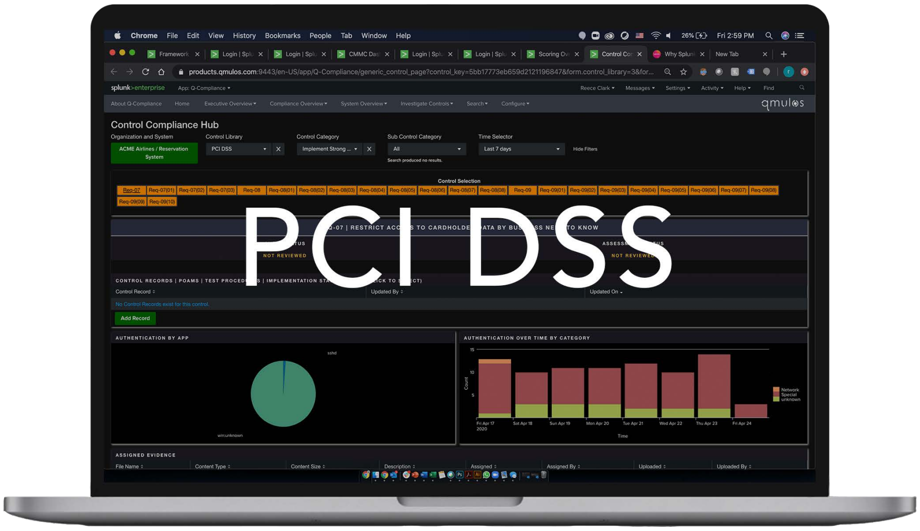
At Qmulos, we pride ourselves on simplifying compliance.

As a native Splunk powered solution, Q-Compliance solves this problem by applying a compliance lens to near real-time data being ingested across your enterprise and assessing it against each of the PCI categories and their relevant security controls.

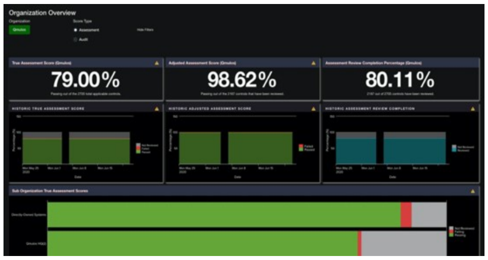
Q-Compliance contextualizes the log data ingested through Splunk into a PCI DSS compliance lens, making compliance easy for anyone to prove. No longer does a team need to manually collect technical evidence from various data sources and vend, spend fortunes on audits, or spend hours sifting through static spreadsheets.

Q-Compliance is purpose-built to help you streamline and automate complex cybersecurity auditing and compliance requirements like PCI DSS, NIST 800-53, SOX, CMMC, and many others. By selecting one of Qmulos' PCI DSS dashboards the user can track how an organization and its systems are scoring against each of the control categories, and where it needs to improve. The dashboards provide an ability to quickly drill into specific domains to view compliance against the capabilities, practices and processes set forth, and also drill into individual controls to see the specific systems, events, and assets that are non-compliant.

Q-Compliance gives the user the ability to upload policies, procedures and file evidence, as well as automatically log human activity. The software keeps evidence needed for audits all in one place, making things more organized and efficient. Q-Compliance also aligns specific security controls with the PCI DSS policies and procedures to use real- time log and event data from Splunk to help you automate the assessment and scoring of your organization's practices. Qmulos codified industry best practices into the application workflows, enabling your organization to institutionalize and optimize the processes that improve your cyber posture and protect you and your customers cardholder data.



ExecutiveView



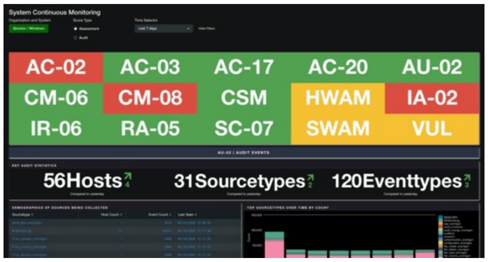
Organization Overview

True Assessment Score (Qmulos)	Adjusted Assessment Score (Qmulos)	Assessment Review Completion Percentage (Qmulos)
79.00%	98.62%	80.11%

HISTORIC TRUE ASSESSMENT SCORE
HISTORIC ADJUSTED ASSESSMENT SCORE
HISTORIC ASSESSMENT REVIEW COMPLETION
Sub Organization True Assessment Scores

- Compliance and risk postures
- Organization & system views
- View status across different compliance frameworks

Control Monitoring



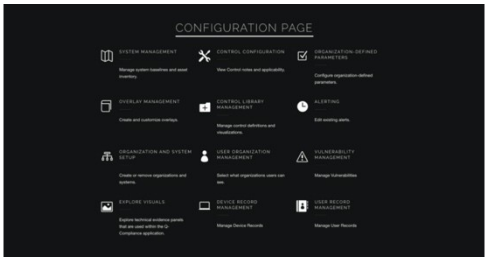
System Continuous Monitoring

AC-02	AC-03	AC-17	AC-20	AU-02
CM-06	CM-08	CSM	HWAM	IA-02
IR-06	RA-05	SC-07	SWAM	VUL

56 Hosts 31 Sourcetypes 120 Eventtypes

- Real-time risk and compliance visibility
- Single pane of glass for all evidence and artifacts
- Workflows for time and event-based assessments

Native RMF Features



CONFIGURATION PAGE

SYSTEM MANAGEMENT
Manage system baselines and asset inventory.

CONTROL CONFIGURATION
View Control notes and applicability.

ORGANIZATION-DEFINED PARAMETERS
Configure organization-defined parameters.

OVERLAY MANAGEMENT
Create and customize overlays.

CONTROL LIBRARY MANAGEMENT
Manage control definitions and visualizations.

ALERTING
Edit existing alerts.

ORGANIZATION AND SYSTEM SETUP
Create or remove organizations and systems.

USER ORGANIZATION MANAGEMENT
Select what organizations users can see.

VULNERABILITY MANAGEMENT
Manage Vulnerabilities

EXPLORE VISUALS
Explore technical evidence panels that are used within the Q-Compliance application.

DEVICE RECORD MANAGEMENT
Manage Device Records

USER RECORD MANAGEMENT
Manage User Records

- Support for all RMF steps
- Overlay management
- Organization, system, and asset management
- Control tailoring
- Assessment automation