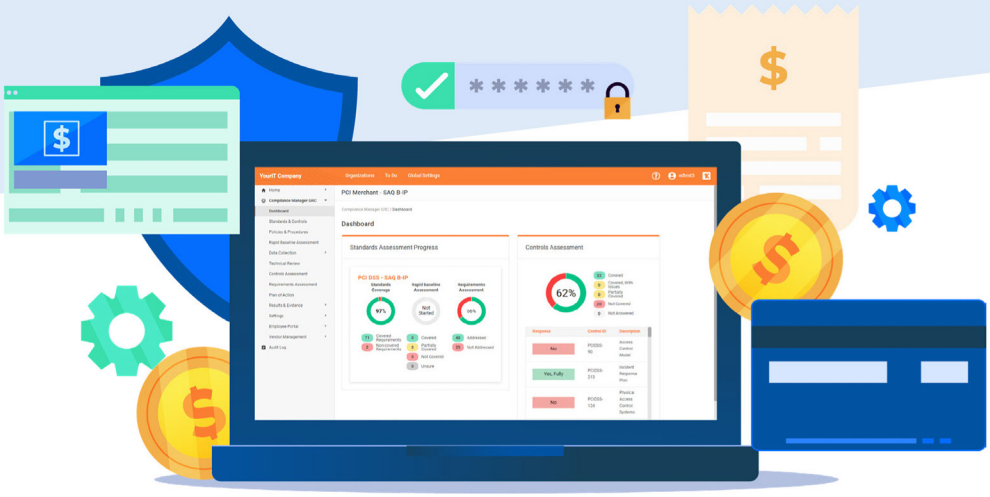
Texas Cyber Security
Your Digital Security Guard

PCI **DSS** Standard

Meet the requirements of the PCI DSS standard while managing compliance with ALL your IT security requirements, regardless of source.



History of PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) is a global standard that establishes the technical and operational criteria for protecting credit card payment data in motion.

The PCI Security Standards Council (PCI SSC) is responsible for establishing the criteria. PCI DSS 4.0.1 was released on June 11, 2024, and was made effective immediately.

Who is subject to PCI DSS?

PCI DSS requirements apply to all system components, including people, processes and technologies included in the cardholder data or cardholder data environment, and to the storage, processing or transmission of card data linked to that environment that accept credit cards.

All organizations that accepts credit cards are required to meet a total of 12 PCI DSS requirements. Compliance requirements vary depending on the type and volume of transactions carried out by the company and are determined by the acquiring bank.

PCI DSS v 4.0 has been upgraded to v4.0.1

The PCI DSS standard continues to evolve as the PCI SSC works to address emerging threats to data and leverage new technologies to defend payment card transactions.

PCI DSS v4.01 replaces PCI DSS v4.0 immediately. There is a short transition window in effect that allows merchants time to familiarize themselves with the changes in PCI DSS and work to meet the new standard. However, the grace period ends on December 31, 2024.

Regulators will expect all organizations that process payment card data to implement the new requirements identified as best practices in PCI DSS v4.01 by March 31, 2025.

CM-PCI-DSS-Standard-1.jpg

Featured Product Highlights For

PCI DSS Standard

Compliance Manager GRC allows you to use all of your current IT security tools, software and systems to meet the requirements of PCI DSS while you maintain compliance with all your other IT requirements, regardless of source. The built-in Standard Management Templates allow you to quickly determine if you can "check the boxes" for every control, identifies the gaps and automatically prepares all of the documents you need to comply with the regulation based on the evidence you compile in the process from various sources.

The 6 Control Objectives

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives."

While each version of PCI DSS (Payment Card Industry Data Security Standard) has divided these six requirements into a number of different sub-requirements, the twelve high-level requirements have not changed since the inception of the standard.

The 3 PCI DSS Sections

Requirement Declaration: It defines the main description of the requirement. The endorsement of PCI DSS is done on the proper implementation of the requirements.

Testing Processes: The processes and methodologies carried out by the assessor for the confirmation of proper implementation.

Guidance: It explains the core purpose of the requirement and the corresponding content, which can assist in the proper definition of the requirement.

The 12 Requirements for Compliance

The twelve requirements for building and maintaining a secure network and systems can be summarized as follows:

- Installing and maintaining a firewall configuration to protect cardholder data.
- Changing vendor-supplied defaults for system passwords and other security parameters.
- Protecting stored cardholder data.
- Encrypting transmission of cardholder data over open, public networks.
- Protecting all systems against malware and performing regular updates of antivirus software.
- Developing and maintaining secure systems and applications.
- Restricting access to cardholder data to only authorized personnel.
- Identifying and authenticating access to system components.
- Restricting physical access to cardholder data.
- Tracking and monitoring all access to cardholder data and network resources.
- Testing security systems and processes regularly
- Maintaining an information security policy for all personnel.

CM-PCI-DSS-Standard-2.jpg

The Top PCI DSS Self-Assessment Questionnaires

Merchants and service providers are required to perform PCI DSS self-assessments and report the results to their merchant bank. The requirements of the self-assessments vary depending on the type of organization. PCI DSS designates the requirements by letters, and has a separate Self-Assessment Questionnaire (SAQ) for each. Compliance Manager GRC supports the following assessment types:*

SAQ A - For e-commerce or mail/telephone-order companies that fully outsource all cardholder data functions to PCI DSS-validated third-party service providers, with no electronic storage, processing or transmission of any cardholder data on the merchant's systems or premises.

SAQ A-EP - For e-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have websites that don't directly receive cardholder data but can impact the security of the payment transaction. No electronic storage, processing or transmission of any cardholder data on the merchant's systems or premises.

SAQ B-IP - For merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.

SAQ C-VT - For merchants who manually enter a single transaction at a time via a keyboard into an internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.

SAQ C - For merchants with payment application systems connected to the internet, with no electronic cardholder data storage.

SAQ D - For merchants that store, process or transmit any cardholder data. This comprehensive standard is now supported by Compliance Manager GRC, covering a broad spectrum of cardholder data environments.

SAQ P2PE - For merchants that process cardholder data only via a validated PCI-listed Point to Point Encryption (P2PE) solution.

SAQ SPoC - For merchants that use commercial off the shelf mobile device (for example, phone or tablet) with a secure card reader that is part of a PCI SSC validated SPoC Solution to process cardholder data.

**There are other highly specialized SAQ types that are not currently supported by Compliance Manager GRC. Check our web site for updates.*

PCI **DSS** Standard

TCS
Texas Cyber Security
Your Digital Security Guard

CM-PCI-DSS-Standard-3.jpg

Texas Cyber Security
Your Digital Security Guard

Here are a few of the value-added features you get:

- **Rapid Baseline Assessments –** Quickly identify gaps where you are not compliant with the PCI DSS.
- **Technical Risk Assessments –** Full risk assessment to meet the PCI DSS security requirements.
- **Auditor's Checklist –** Easy access for auditors to quickly verify compliance with every requirement.
- **Plan of Action & Milestones –** Tracking and management of things you need to do to become compliant.
- **Policies & Procedures Manual –** Required documentation of everything you need to do.
- **Automated Documentation & Storage –** Helps speed up the review process in the event of an audit or lawsuit.
- **Bullphish Integration –** Helps with end-user training.

Full-featured to manage **PCI DSS compliance** along with all your other **IT requirements**

Compliance Manager GRC is simple to use, and you don't have to be a compliance expert to manage the specific parameters of the PCI DSS Standard. Compliance Manager GRC automatically loads the specific requirements and controls you need to implement to comply. Best of all, you can also track everything that's in scope for your IT operation at the same time, and on the same dashboard, regardless of source.

Whether complying with the requirements of PCI DSS, tracking cyber insurance policy terms or managing your total IT security and privacy assurance program, Compliance Manager GRC does it all, in once place, at the same time.

COMPLETE: ALL-IN-ONE SOLUTION

Whether complying with the requirements of PCI DSS, tracking the terms of your cyber-risk insurance policy, or making sure your own IT policies and procedures are being followed, Compliance Manager GRC helps you Get IT All Done at the same time, and in the same place. No other Compliance Management software give you this kind of flexibility

AUTOMATED ASSESSMENTS & REPORTS

Assuring compliance with PCI DSS – as well as all your other IT requirements – is easy with Compliance Manager GRC. You get more work done with less labor, thanks to automated data collection, automated management plans and automated document generation – all specifically tied to the SAQ that applies to your organization.

AFFORDABLE FOR ALL

Compliance Manager GRC is affordable, yet boasts the power and functionality most often found in expensive, enterprise-class governance, risk and compliance platforms. Whether you manage compliance for your own organization, or are an MSP delivering compliance-as-a-service, there's a sensible subscription for you.

Request a demo today
and discover the advantages of Compliance Manager GRC, the purpose-built compliance management platform for IT professionals

PCI **DSS** Standard

CM-PCI-DSS-Standard-4.jpg