

PCI DSS v4.0.1 – SAQ C-VT

PCI DSS SAQ C-VT specifies security controls for virtual terminal merchants to protect cardholder data and assess PCI compliance.



What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ C-VT) is a compliance tool within the Payment Card Industry Data Security Standard (PCI DSS) framework that assists organizations in validating security controls for virtual terminal merchants that manually enter cardholder data. This questionnaire helps businesses confirm their adherence to industry requirements for protecting payment card information and managing payment card risks.

Published by the PCI Security Standards Council (PCI SSC), SAQ C-VT is intended for organizations that process cardholder data solely via virtual payment terminals on devices isolated from other payment processing environments. It focuses on cybersecurity controls related to data protection, secure network configuration, and the mitigation of payment card fraud in accordance with PCI DSS requirements.

At a glance

PUBLISHER Payment Card Industry Security Standards Council (PCI SSC)	TYPE Assessment / Maturity Model	VERSION v4.0.1
EFFECTIVE June 2024	DOMAIN Cybersecurity	FAMILY PCI Security Standards
REGION PCI DSS (Payment Card Industry Data Security Standard), including version 4.0.1 and its associated Self-Assessment Questionnaires such as SAQ C-VT, is developed and managed by the PCI Security Standards Council. The Council is an international consortium established by major payment card brands—but it is headquartered and incorporated in the United States ([en.wikipedia.org] (https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard?utm_source=openai)).	INDUSTRY Payment & FinTech	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High Source: https://www.pcisecuritystandards.org/document_library?category=saqs		

Why it matters

- Strengthen data protection measures** Reduce risk of unauthorized access and compromise by enforcing strict controls for handling cardholder data through virtual terminals.
- Enhance compliance support** Aid organizations in demonstrating adherence to payment card industry requirements, simplifying the process of regulatory and third-party validation.
- Increase audit readiness** Promote systematic recordkeeping and documentation that enables smoother and faster

How SmartSuite supports PCI DSS 4.0 SAQ C-VT

SAQ C-VT Requirement Library

Structure SAQ C-VT requirements with mapped controls, assigned owners, and compliance tasks.

Virtual Terminal Access Governance

Track authorized users, authentication policies, and approved devices accessing virtual payment terminals.

Endpoint Security and Configuration Management

Manage security controls for systems used to access payment terminals, including patching and malware protection.

Logging and Monitoring Evidence

Capture logs and monitoring data supporting detection of unauthorized payment system activity.

Service Provider and Processor Oversight

Track payment processors, contracts, and compliance documentation supporting PCI requirements.

SAQ Completion and Compliance Reporting

Provide dashboards showing SAQ completion status, control coverage, and outstanding compliance actions.

Common framework mappings

CIS Controls v8.1

COBIT 2019

HIPAA

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

SWIFT CSCF

Official resources

PCI DSS v4.0.1 Documentation

Official documentation detailing the PCI DSS version 4.0.1 security requirements and guidance.

pcisecuritystandards.org/document_library

PCI DSS SAQ C-VT Guidance

Provides detailed guidance on completing the Self-Assessment Questionnaire for PCI DSS compliance.

pcisecuritystandards.org/document_library

Frequently asked questions

What is PCI DSS v4.0.1 SAQ C-VT used for?

PCI DSS v4.0.1 SAQ C-VT is designed for merchants who process cardholder data solely via virtual terminals on personal computers connected to the internet. It provides a tailored set of security requirements to ensure that cardholder data is protected during payment transactions, specifically when no electronic storage of cardholder data occurs.

Is compliance with PCI DSS SAQ C-VT mandatory?

Yes, compliance with PCI DSS SAQ C-VT is mandatory for merchants who meet the eligibility criteria defined by the Payment Card Industry Security Standards Council (PCI SSC). Acquirers and payment brands may require proof of compliance through annual self-assessment and periodic vulnerability scans.

Who is eligible to use SAQ C-VT under PCI DSS v4.0.1?

SAQ C-VT applies to merchants that process card payments solely through validated virtual terminals (not storing cardholder data electronically) and do not transmit cardholder data via other channels. It is not applicable to merchants using POS systems or any systems that store, process, or transmit cardholder data outside the virtual terminal environment.

What are the most important controls required by PCI DSS SAQ C-VT?

Key controls include maintaining secure configurations for computers, strong access controls, regular system monitoring, and ensuring encrypted transmission of cardholder data. Merchants must also implement anti-virus software, restrict physical access, and ensure no cardholder data is stored electronically.

How is PCI DSS SAQ C-VT implemented in practice?

Implementation involves assessing the environment for eligibility, configuring systems to support only virtual terminal transactions, restricting access to systems processing card data, and documenting compliance using the SAQ C-VT questionnaire. Regular employee training and policy enforcement are also essential.

How does PCI DSS SAQ C-VT relate to other PCI SAQs or versions?

PCI DSS SAQ C-VT is one of several self-assessment options within PCI DSS, each tailored to a specific merchant environment. It is more limited in scope compared to SAQ D (for service providers and larger merchants) and is specifically for those using virtual terminals exclusively.

What are the ongoing compliance requirements for PCI DSS SAQ C-VT?

Ongoing requirements include annual completion of the SAQ C-VT, continued adherence to the outlined controls, regular review of system configurations, and ongoing security awareness training for staff. Merchants must also remain vigilant for any environment changes that could affect their eligibility or compliance status.

How would SmartSuite support PCI DSS v4.0.1 SAQ C-VT?

SmartSuite can help organizations manage PCI DSS SAQ C-VT by tracking compliance risks, managing security control implementation, collecting and organizing compliance evidence, and ensuring readiness for internal or external audits. The platform also provides robust reporting capabilities and supports workflow management to help teams maintain continuous compliance.

License included / downloadable: Yes PCI DSS v4.0.1 SAQ C-VT is freely available for download from the PCI SSC website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-v401-saq-c-vt-cardholder-data-security-controls-for-virtual-terminal-merch