SmartSuite

Framework / Cybersecurity / PCI Security Standards

PCI DSS v4.0.1 – SAQ A-EP

SAQ A-EP specifies PCI DSS requirements for securing e-commerce payment pages that store, process, or transmit cardholder data.

What it is

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ A-EP) is a compliance assessment tool that helps merchants validate their implementation of required cardholder data security controls for e-commerce payment pages. It is part of the Payment Card Industry Data Security Standard (PCI DSS), which establishes baseline security requirements for organizations that store, process, or transmit payment card information.

Published by the PCI Security Standards Council (PCI SSC), SAQ A-EP is used primarily by e-commerce merchants whose websites direct consumers to third-party payment processors but can impact the security of payment card data through their web environment. The questionnaire covers areas such as cybersecurity controls, website security, data protection, and risk management specific to e-commerce channels.

At a glance

PUBLISHER
Payment Card Industry Security Standards Council (PCI SSC)

TYPE
Standard

VERSION
v4.0.1

EFFECTIVE
January 1, 2025

DOMAIN
Cybersecurity

FAMILY
PCI Security Standards

REGION
PCI DSS is developed, maintained, and administered by the **Payment Card Industry Security Standards Council (PCI SSC)**. The PCI SSC is an international standards body formed by major payment card brands, and it does **not** represent any single country or specific jurisdiction ([en.wikipedia.org](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard?utm_source=openai)). Therefore, the applicable **Region Detail** for the PCI DSS v4.0.1 Self-Assessment Questionnaire is: Payment Card Industry Security Standards Council

INDUSTRY
Payment & FinTech

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: https://www.pcisecuritystandards.org/document_library

Why it matters

How SmartSuite supports PCI DSS 4.0.1 SAQ A-EP

SAQ A-EP Requirement Library

Structure SAQ A-EP requirements with mapped controls, implementation tasks, and accountable owners.

Payment Page Security Governance

Document payment page architecture, scripts, integrations, and systems involved in transaction processing.

Web Application Security Monitoring

Track vulnerability scans, code reviews, and remediation activities for internet-facing payment systems.

Authentication and Access Control Management

Manage authentication policies, system configurations, and access reviews for payment infrastructure.

Security Monitoring and Incident Handling

Coordinate logging, monitoring alerts, and response workflows for payment-related security events.

Compliance and Self-Assessment Reporting

Provide dashboards showing SAQ completion status, control coverage, and remediation progress.

Common framework mappings

Official resources

PCI DSS v4.0.1 Standard

Defines the requirements for payment card security standards and related assessment procedures.

pcisecuritystandards.org/document_library

PCI DSS SAQ A-EP Guidance

Provides self-assessment questionnaire guidance for e-commerce payment page security controls.

pcisecuritystandards.org/document_library

PCI DSS Quick Reference Guide

Describes key concepts and security requirements of PCI DSS v4.0.

pcisecuritystandards.org/document_library?document=pci_dss_qrg

Frequently asked questions

What is PCI DSS v4.0.1 SAQ A-EP used for?

PCI DSS v4.0.1 SAQ A-EP is designed for e-commerce merchants who outsource all cardholder data functions to PCI DSS compliant service providers but still manage payment page elements. It ensures that payment pages controlling the redirection or capture of cardholder data are properly secured according to PCI DSS requirements.

Is PCI DSS SAQ A-EP mandatory or certifiable?

PCI DSS compliance is mandatory for any organization that stores, processes, or transmits cardholder data. While SAQ A-EP completion demonstrates compliance, the requirement itself is imposed by the payment brands and acquirers, not as an official “certification” but as an attestable validation.

Who should use PCI DSS SAQ A-EP?

SAQ A-EP applies to e-commerce merchants who outsource all payment processing but maintain control over the web pages that direct customers to third-party payment services. It specifically excludes merchants who do not handle any payment page elements or redirect processes themselves.

What controls does PCI DSS SAQ A-EP require?

SAQ A-EP requires controls such as maintaining secure systems, protecting payment page scripts, implementing vulnerability management, and restricting unauthorized changes to payment pages. Merchants must also ensure security monitoring and ongoing testing for components within their control.

 © 2026 SmartSuite Inc. All rights reserved.

What is the key difference between SAQ A and SAQ A-EP in PCI DSS?

SAQ A covers merchants with entirely outsourced cardholder data environments and no control over payment pages, whereas SAQ A-EP is for merchants who manage payment page elements but outsource the actual card data handling. SAQ A-EP thus involves additional security and monitoring controls for the merchant-managed components.

How does PCI DSS SAQ A-EP relate to other PCI SAQs?

SAQ A-EP addresses a distinct scenario among PCI DSS Self-Assessment Questionnaires, focusing on e-commerce environments with partial control over payment pages. It has stricter requirements than SAQ A but fewer than SAQ D, reflecting the shared compliance responsibilities.

What are the ongoing compliance requirements for SAQ A-EP?

Ongoing compliance with SAQ A-EP includes regular quarterly vulnerability scans, continuous monitoring of payment page scripts, periodic risk assessments, and maintaining documentation of controls and incident response procedures. Merchants must also keep evidence of compliance for review during audits.

How would SmartSuite support PCI DSS v4.0.1 SAQ A-EP?

SmartSuite can help organizations manage PCI DSS SAQ A-EP by enabling risk tracking for payment page vulnerabilities, control management of compliance requirements, and structured evidence collection for audits. It supports audit readiness through workflow automation and provides reporting tools that simplify oversight and compliance documentation.

License included / downloadable: Yes The PCI DSS v4.0.1 SAQ A-EP is published by the PCI Security Standards Council and is publicly available for download from the Council's website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/pci-dss-v4-0-1-saq-a-ep-ecommerce-payment-pages