

Do ASV scans in SAQ A apply to merchants with webpages that redirect to TPSPs or include TPSPs' embedded iframes?

PCI SSC FAQ | Article 1604 | June 2026

Yes. SAQ A for PCI DSS v4.x includes requirements for external vulnerability scanning by a PCI SSC Approved Scanning Vendor (ASV) for merchant e-commerce webpages, even where payment processing is fully outsourced to a third party. Requirements 11.3.2 and 11.3.2.1 were added to SAQ A to address risks where a merchant's webpage could be compromised and thereby result in compromise of the payment process.

Merchants with e-commerce webpages that complete SAQ A, even where payment processing is outsourced to TPSPs, still have responsibility for the PCI DSS requirements included in SAQ A, including the requirements for ASV scanning. This includes merchants with webpages that:

- Redirect transactions to a TPSP (or to another third-party redirection server which then redirects to a TPSP).
- Include a TPSP's embedded iframe (or an iframe that includes another TPSP's iframe).

PCI ASV scans for purposes of satisfying PCI DSS Requirement 11.3.2 must be performed by a PCI Approved Scan Vendor (ASV) listed as an Approved Scanning Vendor

(https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors/) on the PCI SSC website, using the ASV scan solution from that vendor.

The two-page ASV Resource Guide (<https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI%20SSC%20ASV%20Resource%20Guide.pdf>), created in 2024, provides information to help understand this requirement and how it applies to merchants, including those completing SAQ A.

Source: <https://www.pcisecuritystandards.org/faqs/1604/>