	APPLIES TO	REQUIREMENTS
LEVEL 1	1. Organizations that process more than 6 million transactions annually; or 2. Have experienced a data breach; or 3. Are deemed "Level 1" by any card association (Visa, Mastercard, etc)	1. Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)—also commonly known as a Level 1 onsite assessment—or internal auditor if signed by an officer of the company 2. Quarterly network scan by Approved Scan Vendor (ASV) 3. Attestation of Compliance (AOC) for Onsite Assessments–there are specific forms for merchants and service providers
LEVEL 2	Organizations that process between 1-6 million transactions annually	1. Annual PCI DSS Self-Assessment Questionnaire (SAQ)—there are 9 SAQ types shown briefly in the table below 2. Quarterly network scan by Approved Scan Vendor (ASV) 3. Attestation of Compliance (AOC)—each of the 9 SAQs has a respective AOC form
LEVEL 3	1. Organizations that process between 20,000-1 million **online** transactions annually 2. Organizations that process less than 1 million **total**transactions annually	
LEVEL 4	1. Organizations that process fewer than 20,000 **online**transactions annually; or 2. Organizations that process up to 1 million **total** transactions annually	

For Level 2-4, there are different SAQ types depending on your payment integration method. Here's a brief table:

SAQ	DESCRIPTION
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage, and/or • Standalone, dial-out terminals with no electronic cardholder data storage.

	Not applicable to e-commerce channels.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed Point-to-Point Encryption (P2PE) solution, with no electronic cardholder data storage. *Not applicable to e-commerce merchants.*
D	**SAQ D FOR MERCHANTS:** All merchants not included in descriptions for the above SAQ types.

SAQ D FOR SERVICE PROVIDERS: All service providers defined by a payment brand as eligible to complete an SAQ.