PCI Compliance Validation Checklist

A PCI compliance validation involves an evaluation and confirmation that all security controls and procedures have been implemented properly and align with the requirements set by PCI DSS. A PCI assessment could include any of the following requirements:

Qualified Security Assessor (QSA)
A QSA refers to any individual who has acquired a PCI Security Standards Council certificate. This person can audit merchants for PCI DSS compliance. They are third-party entities that have been certified by the PCI DSS governing body.

Internal Security Assessor (ISA)
An ISA refers to any individual who has acquired a PCI Security Standards Council certificate for their specific organization. These individuals are allowed to perform PCI self-audits for their organization. The benefit of having an ISA on your team is that you are not required to hire a third-party entity to review your compliance program. They are, however, required to cooperate and collaborate with QSA's should the situation call for it.

Report on Compliance (ROC Form)
A Report on Compliance is a form required to be completed by all Level 1 merchants and service providers undergoing a PCI DSS audit. The ROC form is used to verify that all policies, strategies, and workflows are being implemented in compliance with PCI DSS standards.

Self-Assessment Questionnaire (SAQ)
SAQ's are a validation tool meant to assist merchants and service providers in their self-reporting efforts. If your company uses an ISA to self-audit, you'll need to complete a SAQ. It's comprised of several questionnaire documents that vendors are required to complete annually.

Attestation of Compliance (AOC)
An AOC is completed if your company has completed a self-audit and finalized a SAQ. It serves as a declaration of a merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS).