Security Standards Council®

Payment Card Industry
Data Security Standard

Frequently Asked Questions

PCI DSS v4.0 Designated Entities Supplemental Validation

June 2022

FAQs for Designated Entities Supplemental Validation

Q1: What is a Designated Entity?

A: *A Designated Entity is determined by an Acquirer or Payment Brand as an organization that requires additional validation to existing PCI DSS requirements.*

Q2: How will I know if my organization has been deemed a Designated Entity?

A: *Your Acquirer and/or Payment Brand(s) will manage communications about which organizations are a Designated Entity as part of their compliance programs.*

Q3: What are some examples of Designated Entities?

A: *Examples of Designated Entities could include organizations that store, process, or transmit large volumes of account data; organizations that provide aggregation points for account data; or organizations that may have suffered a security breach of account data. Whether a particular entity is deemed a Designated Entity is determined by Payment Brand compliance programs.*

Q4: Why was the Designated Entities Supplemental Validation (DESV) created?

A: *Analysis of recent account data breaches and PCI DSS compliance trends has revealed that many organizations view PCI DSS compliance as a periodic exercise and do not have processes in place to ensure that PCI DSS security controls are continuously enforced. This can result in lapses in security controls between validation assessments. PCI DSS compliance is an ongoing process that must be incorporated into an entity's overall security strategy, and the DESV was created to provide a means for entities to assess and document how they are maintaining PCI DSS controls on a continual basis.*

Q5: What are the requirements within the Designated Entities Supplemental Validation (DESV)?

A: *The DESV is a series of additional validation procedures to provide greater insight into and assurance that an organization's PCI DSS controls are being effectively maintained through validation of Business-as-Usual (BAU) processes, and increased validation and scoping consideration.*

Q6: Can I use the DESV even if I'm not a Designated Entity?

A: *Yes. The DESV can be used to complement any entity's PCI DSS compliance efforts, and all entities are encouraged to follow the DESV as a best practice, even if not required to validate.*

Q7: If my organization has been defined as a Designated Entity, is that designation permanent?

A: *The duration for which an entity is deemed a Designated Entity is defined by each Payment Brand as part of their compliance programs.*

Q8: Is it possible to be deemed a Designated Entity by one payment brand but not the others? If so, how would my organization report PCI DSS compliance?

A: *Yes. As each Payment Brand manages their own compliance program, it is possible that one Brand may deem an organization a Designated Entity while the others may not. It is important that a Designated Entity work with each of their compliance-accepting entities (that is, their Acquirers and/or Payment Brands) to determine specific compliance reporting requirements.*

Q9: As a Designated Entity, am I expected to comply with all requirements in the DESV?

A: *Yes, it is the intent that a Designated Entity comply with all requirements in the DESV. However, entities should check with their Acquirer and/or the Payment Brands directly as they may have different compliance validation expectations as part of their individual compliance programs.*

Q10: How does the DESV impact my PCI DSS assessment?

A: *Typically, the supplemental validation would be performed in conjunction with a full PCI DSS assessment. Designated Entities should contact their Acquirer and/or Payment Brand(s) with any questions about completing and submitting reports on compliance.*

Q11: How do I report my DESV assessment?

A: *As mentioned previously, a supplemental validation would typically be performed in conjunction with a full PCI DSS assessment. The PCI DSS ROC Reporting Template and AOC cover aspects of the supplemental validation (for example, in the Scope of Work and Details of Reviewed Environment sections). However, there is also a supplemental ROC Template (S-ROC) and a supplemental Attestation of Compliance (S-AOC) that are specific to supplemental validations, and these need to be completed in addition to the PCI DSS ROC and AOC respectively. Designated Entities should contact their Acquirer and/or the Payment Brand(s) directly with any questions about how to complete and submit these documents.*