Payment Card Industry (PCI) Data Security Standards (DSS)

Azure complies with Payment Card Industry Data Security Standards Level 1 version 3.2.

Microsoft and PCI DSS

Microsoft Azure completes an annual PCI DSS assessment using an approved Qualified Security Assessor (QSA). The auditor reviews the Azure environment, which includes validating the infrastructure, development, operations, management, support, and in-scope services. The PCI DSS designates four levels of compliance based on transaction volume. Azure is certified as compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions—more than 6 million a year).

The assessment results in an Attestation of Compliance (AoC) and Report on Compliance (RoC) issued by the QSA. The effective period for compliance begins upon passing the audit and receiving the AoC from the assessor, and ends one year from the date the AoC is signed. The AoC is available to customers to show that the QSA has determined that Azure is in compliance with PCI DSS v3.2.

Customers who want to develop a cardholder environment or card processing service can leverage the Azure validation in many of the underlying portions, thereby reducing the associated effort and costs of getting their own PCI DSS certification.

It is, however, important to understand that Azure PCI DSS compliance status does not automatically translate to PCI DSS certification for the services that customers build or host on the Azure platform. Customers are responsible for ensuring that they achieve compliance with PCI DSS requirements. The Azure Customer PCI Guide specifies areas of responsibility for each PCI DSS requirement, and whether it is assigned to Azure or the customer, or if the responsibility is shared.

Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Cloud App Security
- Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Graph
- Intune
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

Audits, reports, and certificates

- Azure PCI DSS Attestation of Compliance Package

How to implement

- **Azure PCI DSS solution**
  Get reference architectures, deployment guidance, control implementation mappings, and automated scripts.
  Learn more

About PCI DSS

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. Organizations of all sizes must follow PCI DSS standards if they accept payment cards from the five major credit card brands—Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (JCB). Compliance with PCI DSS is required for any organization that stores, processes, or transmits payment and cardholder data.

Frequently asked questions

Why does the Attestation of Compliance (AoC) cover page say June 2018?

The June 2018 date on the cover page is when the AoC template was published. Refer to Section 2 for the date of the assessment.

Why are there multiple Azure Attestations of Compliance?

Azure is continuously releasing new services that PCI customers want to leverage. To keep up with customer demand, Azure undergoes two PCI assessments annually. The "Core" AoC covers the Azure platform, infrastructure, and the bulk of Azure services. The "Add-on" AoC covers new Azure services that were not included in the Core assessment. These should be used together, as the Add-on AoCs rely on the Core AoC. The Core AoC is issued in March, and the Add-on AoC follows each year in June.

What is the relationship between the PA DSS and PCI DSS?

The Payment Application Data Security Standard (PA DSS) is a set of requirements that comply with the PCI DSS, and replaces Visa's Payment Application Best Practices, as well as consolidates the compliance requirements of the other primary card issuers. The PA DSS helps software vendors develop third-party applications that store, process, or transmit cardholder payment data as part of a card authorization or settlement process. Retailers must use PA DSS certified applications to efficiently achieve their PCI DSS compliance. Note that the PA DSS does not apply to Azure.

What is an acquirer and does Azure use one?

An "acquirer" is a bank or other entity that processes payment card transactions. Azure does not offer payment card processing as a service and thus does not use an acquirer.

To what organizations and merchants does the PCI DSS apply?

It applies to any company, no matter the size or number of transactions, that accepts, transmits, or stores cardholder data. That is, if any customer ever pays a company using a credit or debit card, then the PCI DSS requirements apply. Companies are validated at one of four levels based on the total transaction volume over a 12-month period. Level 1 is for companies that process over 6 million transactions a year; Level 2 for 1 million to 6 million transactions; Level 3 is for 20,000 to 1 million transactions; and Level 4 is for fewer than 20,000 transactions.

Where do I begin my organization's PCI DSS compliance efforts for a solution deployed on Azure?

The information that the PCI Security Standards Council makes available is a good place to learn about specific compliance requirements. The council publishes the PCI DSS Quick Reference Guide for merchants and others involved in payment card processing. It explains how the PCI DSS can help protect a payment card transaction environment and how to apply it.

Compliance involves several factors, including assessing the systems and processes not hosted on Azure. Individual requirements will vary based on which Azure services are used and how they are employed within the solution.

Additional resources

- PCI Security Standards Council
- Azure PCI DSS 3.2 Responsibility Matrix