



Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) United States

Azure and Office 365 are certified to the Health Information Trust Alliance Common Security Framework.

Microsoft and the HITRUST CSF

HITRUST offers three degrees of assurance, or levels of assessment: self-assessment, CSF validation, and CSF certification. Each level builds with increasing rigor on the one below it. An organization with the highest level, CSF-certified, meets all the certification requirements of the CSF. Microsoft Azure and Microsoft Office 365 were the first hyperscale cloud services to receive CSF certification for HITRUST. Coalfire, a HITRUST assessor firm, performed the assessments based on how Azure and Office 365 implement security, privacy, and regulatory requirements to protect sensitive information.

Microsoft in-scope cloud services

Covered services for HITRUST CSF:

- Azure and Azure Government
[Learn more](#)
- Intune
- Office 365 and Office 365 U.S. Government
[Learn more](#)

Note Office 365 ProPlus enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards for HITRUST. OneDrive consumer cloud storage does not and other cloud services that are accessible through Office 365 ProPlus and that Microsoft may offer in the future also may not support these standards.

Audits, reports, and certificates

The HITRUST CSF certification of Azure and Office 365 is valid for two years.

- [Azure HITRUST Letter of Certification](#)
- [Office 365 HITRUST Letter of Certification](#)

How to implement

- **Cloud risk assessment tool**
Promote your HITRUST compliance and expedite risk assessments relating to the use of Azure.
[Learn more](#)
- **Azure HIPAA/HITRUST blueprint**
Get tools and guidance to get started building HIPAA/HITRUST-compliant workloads in Azure.
[Learn more](#)
- **Map Microsoft services to HITRUST CSF**
Information on Microsoft cloud services to help customers meet many of the Framework's security functions.
[Learn more](#)

About the HITRUST CSF

The [Health Information Trust \(HITRUST\) Alliance](#) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner.

The CSF builds on HIPAA and the HITECH Act, which are US healthcare laws that have established requirements for the use, disclosure, and safeguarding of individually identifiable health information, and that enforce noncompliance. HITRUST provides a benchmark—a standardized compliance framework, assessment, and certification process—against which cloud service providers

and covered health entities can measure compliance. The CSF also incorporates healthcare-specific security, privacy, and other regulatory requirements from such existing frameworks as the Payment Card Industry Data Security Standard ([PCI-DSS](#)), [ISO/IEC 27001](#) information security management standards, and Minimum Acceptable Risk Standards for Exchanges ([MARS-E](#)).

The CSF is divided into 19 different domains, including endpoint protection, mobile device security, and access control. HITRUST certifies IT offerings against these controls. HITRUST also adapts requirements for certification to the risks of an organization based on organizational, system, and regulatory factors.

Frequently asked questions

Can I use the Azure and Office 365 HITRUST compliance to build on my organization's certification process?

Yes. If your business requires a HITRUST certification for implementations deployed on Microsoft services, you can build on their HITRUST compliance when you conduct your compliance assessment. However, you are responsible for evaluating the HITRUST requirements and controls within your own organization.

Why are some services not in the scope of this certification?

Microsoft provides the most comprehensive offerings compared to other cloud service providers. To keep up with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process the data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

Does Microsoft certification mean that if my organization uses Azure or Office 365, it is compliant with HITRUST CSF?

When you store your data in a cloud service like Azure or Office 365, Microsoft and your organization share the responsibility for achieving compliance. Microsoft manages the majority of the infrastructure controls including physical security, network controls, and application level controls, and your organization has the responsibility to manage access controls and protect your sensitive data. The Office 365 HITRUST certification demonstrates the compliance of the Microsoft control framework. Building on that, your organization needs to implement and maintain your own data protection controls to meet HITRUST CSF requirements.

Does Microsoft provide guidance for my organization to implement appropriate controls when using Azure and Office 365?

Yes, you can find recommended customer actions in Compliance Manager, cross-Microsoft Cloud solutions that help your organization meet complex compliance obligations when using cloud services. Specifically, for HITRUST CSF, we recommend you perform risk assessments using the NIST 800-53 and NIST CSF assessments in Compliance Manager. In the assessments, we provide you with step-by-step guidance and the Microsoft solutions you can leverage to implement your data protection controls. [Learn more](#).

Additional resources

- [HITRUST CSF 8.1](#)
- [Understanding and Leveraging the CSF](#)
- [Microsoft and the NIST Cybersecurity Framework \(CSF\)](#)