National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) United States

Microsoft cloud services meet the NIST Cybersecurity Framework standards.

Microsoft and the NIST CSF

The US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft cloud services have undergone independent, third-party FedRAMP Moderate and High Baseline audits and are certified according to the FedRAMP standards. Additionally, through a validated assessment performed by HITRUST, a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

Microsoft in-scope cloud services

- Azure Government
  Learn more
- Dynamics 365 for Government
  Learn more
- 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 support these standards, and other cloud services that are accessible through Office 365 ProPlus and that Microsoft may offer in the future also may not.

Audit cycle and certification

The NIST CSF certification is valid for two years.

- Attestation of Azure Alignment to the NIST CSF
- Office 365 NIST CSF Letter of Certification
- Microsoft Cloud Services Authorizations

How to implement

- **Azure NIST CSF Blueprint**
  Get tools and guidance to help you more quickly build Microsoft Azure solutions that comply with the NIST CSF.
  Learn more
- **Map Microsoft services to NIST CSF**
  Microsoft cloud services information to help you meet many of the Framework's security functions.
  Learn more

About the NIST CSF

The National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidance to help organizations assess risk. In response to Executive Order 13636 on strengthening the cybersecurity of federal networks and critical infrastructure, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (FICIC) in February 2014.

The main priorities of the FICIC were to establish a set of standards and practices to help organizations manage cybersecurity risk, while enabling business efficiency. The NIST Framework addresses cybersecurity risk without imposing additional regulatory requirements for both government and private sector organizations.

The FICIC references globally recognized standards including NIST SP 800-53 found in Appendix A. Each control within the FICIC framework is mapped to corresponding NIST 800-53 controls within the FedRAMP Moderate Baseline.

Frequently asked questions

Has an independent assessor validated that in-scope Microsoft cloud services support NIST CSF requirements?

Yes, a third-party assessment organization has attested that the Microsoft Azure Government cloud service offering conforms to the NIST Cybersecurity Framework (CSF) risk management practices, as defined in the FICIC Version 1.0, dated February 12, 2014. The NIST CSF is mapped to the FedRAMP Moderate controls framework and an independent assessor has assessed Microsoft Dynamics 365 against the FedRAMP Moderate Baseline.

How do in-scope Microsoft cloud services demonstrate compliance with the framework?

Using the formal audit reports prepared by third parties for the FedRAMP accreditation, Microsoft can show how relevant controls noted within these reports demonstrate compliance with the NIST Framework for Improving Critical Infrastructure Cybersecurity. Audited controls implemented by Microsoft serve to ensure the confidentiality, integrity, and availability of data stored, processed, and transmitted by in-scope cloud services that have been identified as the responsibility of Microsoft.

What are Microsoft responsibilities for maintaining compliance with this initiative?

Participation in the FICIC is voluntary. However, Microsoft ensures that its in-scope cloud services meet the terms defined within the governing Online Services Terms and applicable service level agreements. These define Microsoft responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

Can I leverage Microsoft compliance for my organization?

Yes. The independent third-party compliance reports on the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of in-scope Microsoft cloud services. Microsoft customers may leverage the audited controls described in these related reports as part of their own FedRAMP and NIST risk analysis and qualification efforts.

Which organizations are deemed by the US Government to be critical infrastructure?

According to the US Department of Homeland Security, these include organizations in the following sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear (Reactors Materials and Waste), Transportation Systems, and Water (and Wastewater).

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 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.

Additional resources

- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Microsoft and FedRAMP
- Microsoft Government Cloud