Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0 Framework United States

Microsoft complies with the US Minimum Acceptable Risk Standards for Exchanges (MARS-E)

Microsoft and the MARS-E 2.0 Framework

Currently, there is no formal authorization and accreditation process for MARS-E. However, Microsoft Azure platform services have undergone independent FedRAMP audits at the Moderate Impact Level and Azure Government at the High Impact Level, and are authorized according to FedRAMP standards. Although these standards do not specifically focus on MARS-E, the MARS-E control requirements and objectives are very closely aligned and serve to protect the confidentiality, integrity, and availability of data on Azure. Furthermore, Microsoft business cloud services are monitored and assessed each year for the FedRAMP authorization process.

Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Intune

About the MARS-E 2.0 Framework

In 2012, the Center for Medicare and Medicaid Services (CMS) published the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with CMS information security and privacy programs. The suite of documents, including guidance, requirements, and templates, was designed to address mandates of the Patient Protection and Affordable Care Act (ACA) and regulations of the Department of Health and Human Services that apply to the ACA. The National Institute of Standards and Technology (NIST) Special Publication 800-53 serves as the parent framework that establishes the security and compliance requirements for all systems, interfaces, and connections between ACA-mandated health exchanges and marketplaces.

Following the release of MARS-E, NIST released an update, Special Publication 800-53r4, to address growing challenges to online security, including application security; insider and advanced persistent threats; supply chain risks; and the trustworthiness, assurance, and resilience of systems of mobile and cloud computing. CMS then revised the MARS-E framework to align with the updated controls and parameters in NIST 800.53r4, publishing MARS-E 2.0 in 2015.

These updates address the confidentiality, integrity, and availability in health exchanges of protected data, which includes personally identifiable information, protected health information, and federal tax information. The MARS-E 2.0 framework aims to secure this protected data and applies to all ACA administering entities, including exchanges or marketplaces—federal, state, state Medicaid, or Children's Health Insurance Program (CHIP) agencies—and supporting contractors.

Frequently asked questions

To whom does the standard apply?

MARS-E applies to all Affordable Care Act administering entities, including exchanges or marketplaces—federal, state, Medicaid, and CHIP agencies administering the Basic Health Program—as well as all their contractors and subcontractors.

How does Microsoft demonstrate Azure and Azure Government compliance with this standard?

Using the formal audit reports prepared by third parties for FedRAMP authorizations, Microsoft is able to show how relevant controls noted within these reports demonstrate Azure capabilities in meeting MARS-E security and privacy control requirements. Audited controls implemented by Microsoft serve to protect the confidentiality, integrity, and availability of data stored on the Azure platform, and correspond to the applicable regulatory requirements defined in MARS-E that have been identified as the responsibility of Microsoft.

What are Microsoft responsibilities for maintaining compliance with this standard?

Microsoft ensures that the Azure platform meets the terms defined within the governing Online Services Terms and applicable service level agreements (SLAs). These define our responsibility for implementing and maintaining controls adequate to secure the Azure platform and monitor the system.

Can I use Microsoft compliance in the MARS-E qualification efforts for my organization?

Yes. Third-party audit reports to the FedRAMP standards attest to the effectiveness of the controls Microsoft has implemented to maintain the security and privacy of the Azure platform. Azure and Azure Government customers may use the audited controls described in these related reports as part of their own FedRAMP and MARS-E risk analysis and qualification efforts.

Additional resources

- MARS-E regulatory guidance, MARS-E Document Suite, Version 2.0
  - Volume II: Minimum acceptable risk standards for exchanges
  - Volume III: Catalog of minimum acceptable risk security and privacy controls for exchanges
- Microsoft and FedRAMP
- Microsoft Online Services Terms
- Microsoft Government Cloud