Compliance terms and requirements

100 XP

8 minutes

When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards. Some questions to ask about a potential provider include:

- How compliant is the cloud provider when it comes to handling sensitive data?
- How compliant are the services offered by the cloud provider?
- How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?
- What terms are part of the privacy statement for the provider?

Compliance Offerings

The following list provides details about *some* of the compliance offerings available.

- **Criminal Justice Information Services (CJIS)**. Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhering to the same requirements that law enforcement and public safety entities must meet.

- **Cloud Security Alliance (CSA) STAR Certification**. Azure, Intune, and Microsoft Power BI have obtained STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. This STAR certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). This certification demonstrates that a cloud service provider:
  - Conforms to the applicable requirements of ISO/IEC 27001.
  - Has addressed issues critical to cloud security as outlined in the CCM.
  - Has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

- **General Data Protection Regulation (GDPR)**. As of May 25, 2018, a European privacy law — GDPR — is in effect. GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.

- **EU Model Clauses**. Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud from Europe to the rest of the world.

- **Health Insurance Portability and Accountability Act (HIPAA)**. HIPAA is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the **Health Information Technology for Economic and Clinical Health (HITECH)** Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

- **International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27018**. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

- **Multi-Tier Cloud Security (MTCS) Singapore**. After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 certification across all three service classifications:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)

  Microsoft was the first global cloud solution provider (CSP) to receive this certification across all three classifications.

- **Service Organization Controls (SOC) 1, 2, and 3**. Microsoft-covered cloud services are audited at least annually against the SOC report framework by independent third-party auditors. The Microsoft cloud services audit covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)**. NIST 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 Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits, and are certified according to the FedRAMP standards. Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

- **UK Government G-Cloud**. The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received official accreditation from the UK Government Pan Government Accreditor.

Next unit: Economies of scale