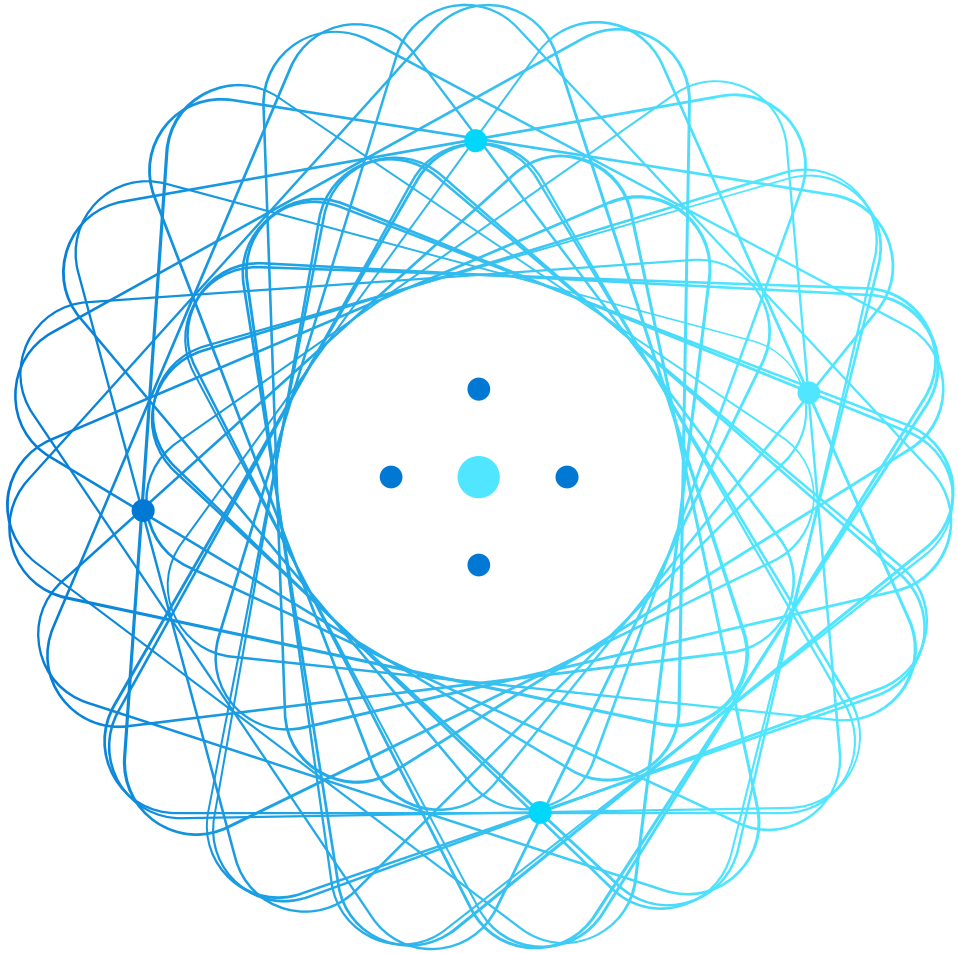
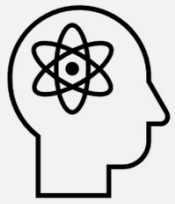
Microsoft Azure

AZ-900T0x Module 05: Identity, governance, privacy, and compliance



Module outline

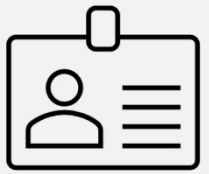


Module 05 – Outline

You will learn the following concepts:

- **Azure identity services**
  - Authentication versus Authorization
  - Azure AD, MFA, SSO and Conditional Access
- **Azure governance features**
  - RBAC
  - Resource locks and tags
  - Policy, Blueprints, and CAF
- **Azure privacy and compliance**
  - Privacy statement and Online Services Terms
  - Trust Center and compliance documentation
  - Azure Sovereign Regions

Core Azure identity services



Azure Identity Services - Objective Domain

- Explain the difference between authentication and authorization
- Define Azure Active Directory
- Describe the functionality and usage of Azure Active Directory
- Describe the functionality and usage of Conditional Access, Multi-Factor Authentication (MFA), and Single Sign-On (SSO)

Compare Authentication and Authorization

Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

Authorization

- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.

Azure Multi-Factor Authentication

Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

Azure Active Directory (AAD)

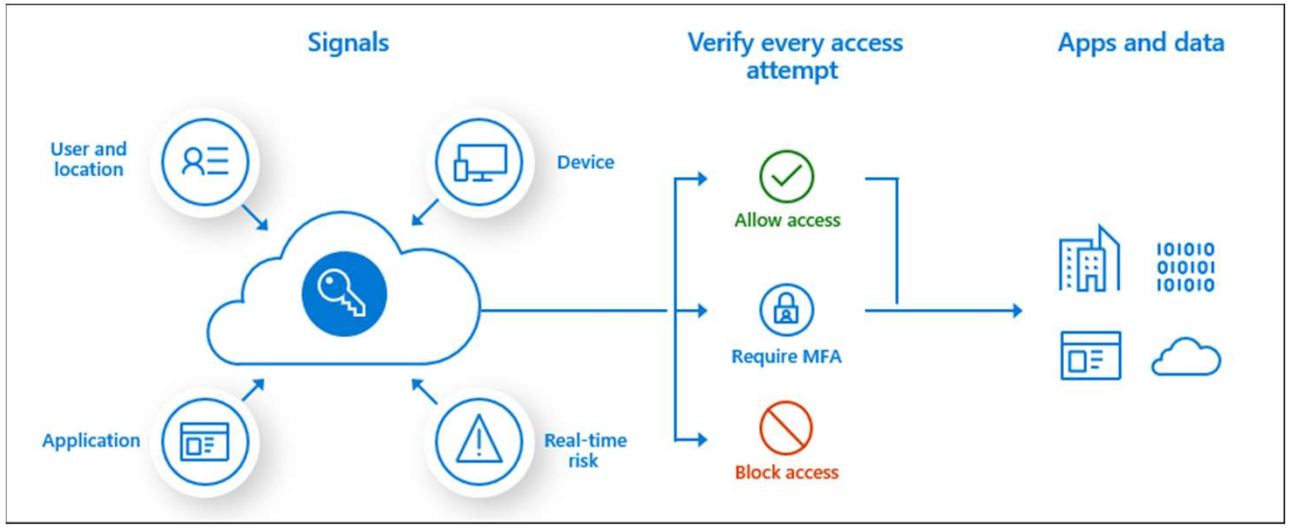
Azure Active Directory (AAD) is Microsoft Azure's cloud-based identity and access management service.

- Authentication (employees sign-in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.

Conditional Access

Conditional Access is used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies.

- User or Group Membership
- IP Location
- Device
- Application
- Risk Detection

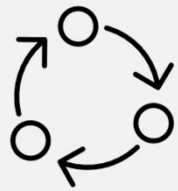


Walkthrough - Manage access with RBAC

Assign roles and view activity logs.

1. View and assign roles.
2. View the activity log and remove a role assignment.

Azure Governance Methodologies

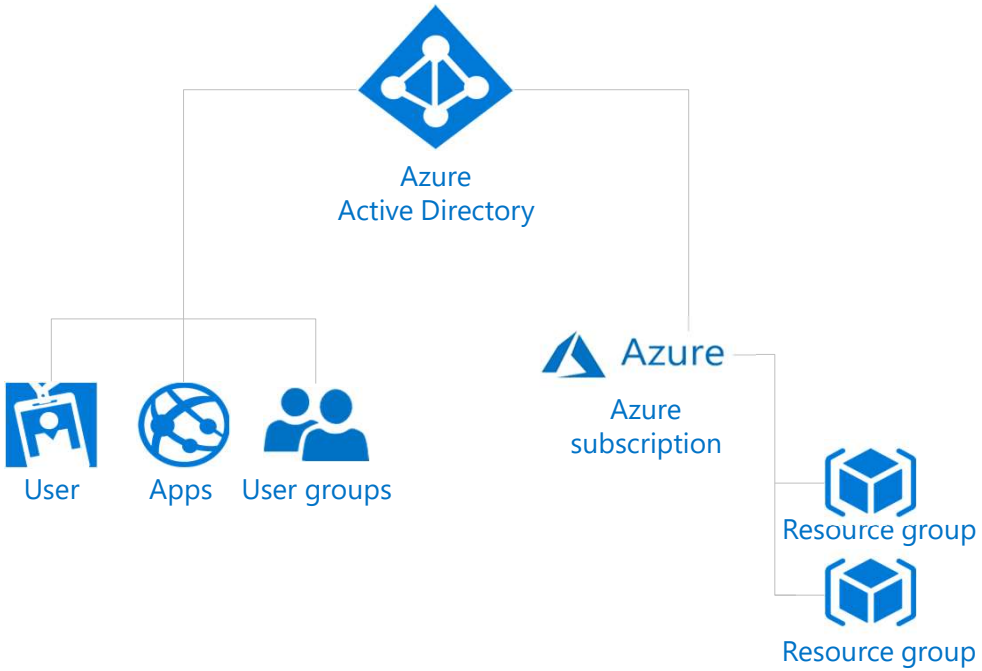


Azure Governance Methodologies - Objective Domain

Describe the functionality and the usage of:

- Role-Based Access Control (RBAC)
- Resource locks
- Tags
- Azure Policy
- Azure Blueprints
- Cloud Adoption Framework for Azure

Explore Role-based access control (RBAC)



- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

Resource locks

- Protect your Azure resources from accidental deletion or modification.
- Manage locks at subscription, resource group, or individual resource levels within Azure Portal.

Lock Types	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No

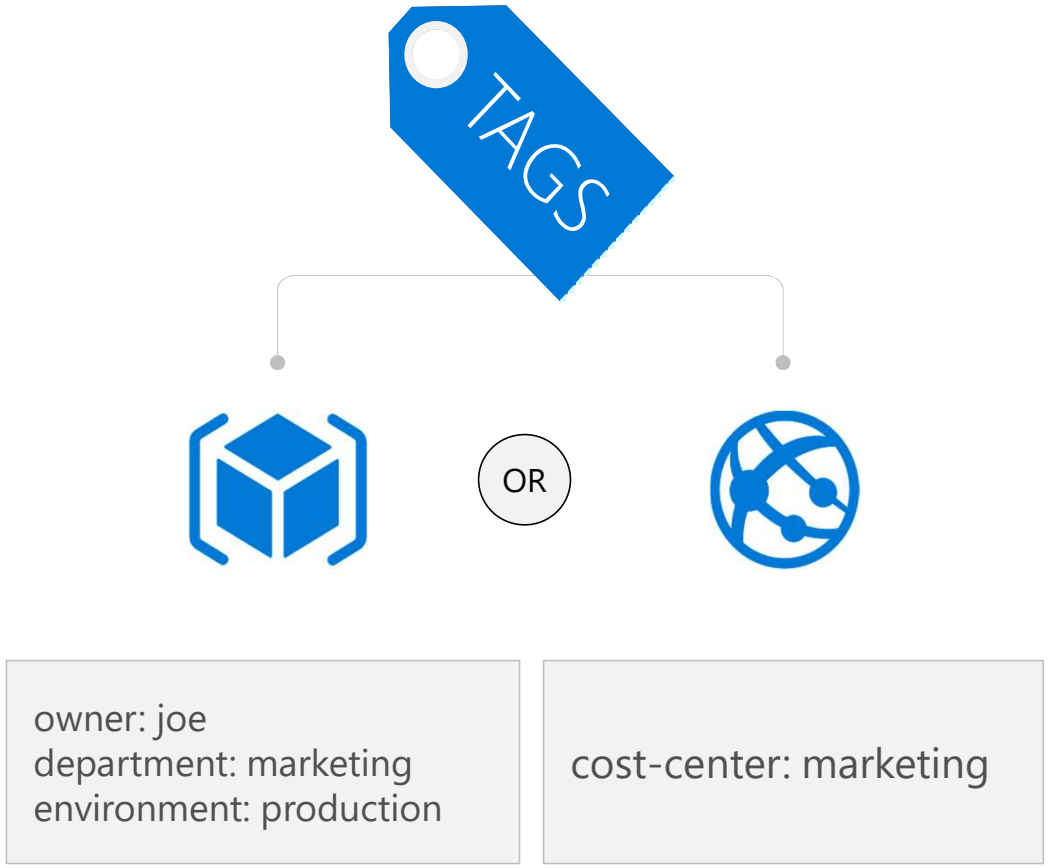
Walkthrough - Manage Resource Locks

Create a resource group add a lock and test deletion, test deleting a resource in the resource group.

1. Create a resource group.
2. Add a resource lock to prevent deletion of a resource group.
3. Test deleting a member of the resource group.
4. Remove the resource lock.

Tags

- Provides metadata for your Azure resources.
- Logically organizes resources into a taxonomy.
- Consists of a name-value pair.
- Very useful for rolling up billing information.



Walkthrough – Implement resource tagging

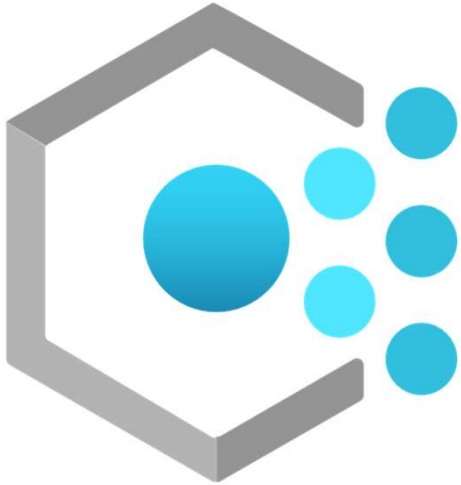
Create a policy assignment that requires tagging, then create a storage account and test the tagging.

1. Create a policy assignment to require tagging.
2. Create a storage account to test required tagging.
3. View all resources with a specific tag.
4. Delete the policy assignment.

Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Provides governance and resource consistency with regulatory compliance, security, cost, and management.

- Evaluates and identifies Azure resources that do not comply with your policies.
- Provides built-in policy and initiative definitions, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.



Walkthrough - Create an Azure Policy

Create an Azure Policy to restrict deployment of Azure resources to a specific location.

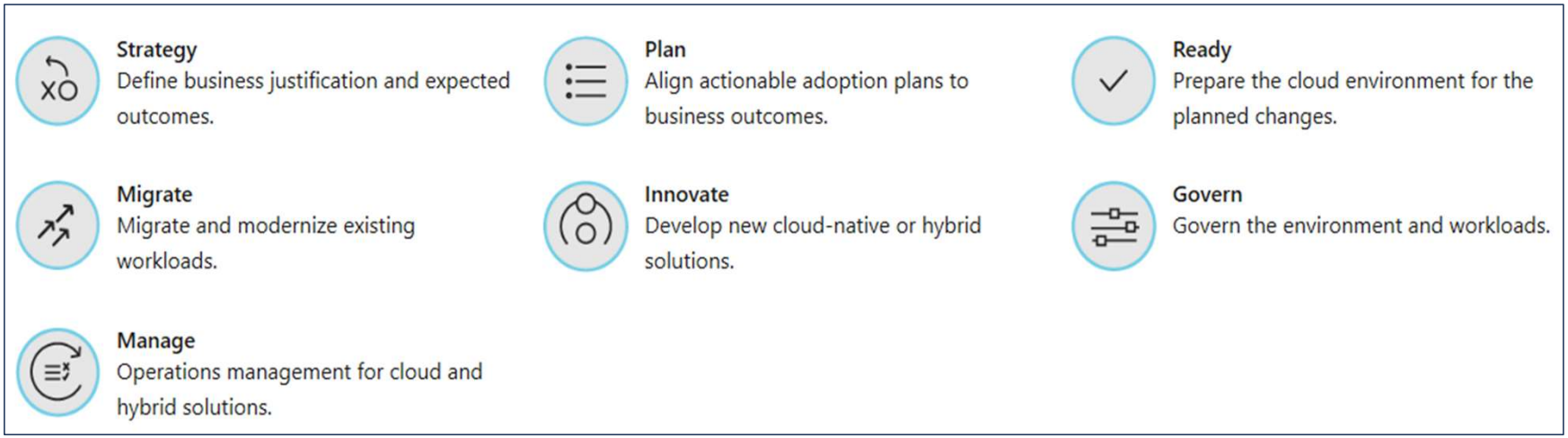
1. Create a policy assignment.
2. Test the allowed location policy.
3. Delete the policy assignment.

Azure Blueprints

Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments. Development teams can quickly build trust through organizational compliance with a set of built-in components (such as networking) in order to speed up development and delivery.

- Role Assignments
- Policy Assignments
- Azure Resource Manager Templates
- Resource Groups

Cloud Adoption Framework



- The One Microsoft approach to cloud adoption in Azure.
- Best practices from Microsoft employees, partners, and customers.
- Tools, guidance, and narratives for strategies and outcomes.

Privacy, compliance, and data protection standards

Privacy, Compliance, and Data Protection - Objective Domain

Describe the purpose of the:

- Microsoft core tenants of Security, Privacy, and Compliance
- Microsoft Privacy Statement, Online Services Terms (OST) and Data Protection Amendment (DPA)
- Trust Center
- Azure compliance documentation
- Azure Sovereign Regions (Azure Government cloud services and Azure China cloud services)

Security, Privacy, and Compliance

Security: Secure by design. With built in intelligent security, Microsoft helps to protect against known and unknown cyberthreats, using automation and artificial intelligence.

Privacy: We are committed to ensuring the privacy of organizations through our contractual agreements, and by providing user control and transparency.

Compliance: We respect local laws and regulations and provide comprehensive coverage of compliance offerings.

Compliance Terms and Requirements

Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider. Some compliance offerings include.

CJIS Criminal Justice Information Services	**HIPAA** Health Insurance Portability and Accountability Act
CSA STAR Certification	**ISO/IEC 27018**
EU Model Clauses	**NIST** National Institute of Standards and Technology

Microsoft privacy statement

The Microsoft privacy statement provides openness and honesty about how Microsoft handles the user data collected from its products and services.

The Microsoft privacy statement explains:

- What data Microsoft processes.
- How Microsoft processes it.
- What purposes the data is used for.

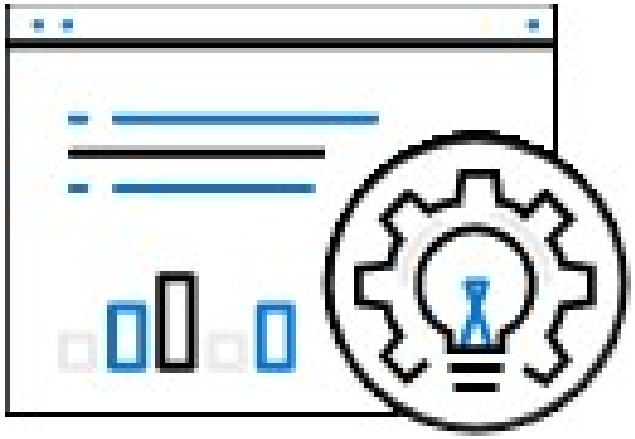
Online Services Terms and Data Protection Addendum

Online Services Terms: The licensing terms define the terms and conditions for the products and Online Services you purchase through Microsoft Volume Licensing programs.

Data Protection Addendum: The DPA sets forth the obligations, with respect to the processing and security of Customer Data and Personal Data, in connection with the Online Services.

Trust Center

Learn about security, privacy, compliance, policies, features, and practices across Microsoft's cloud products.



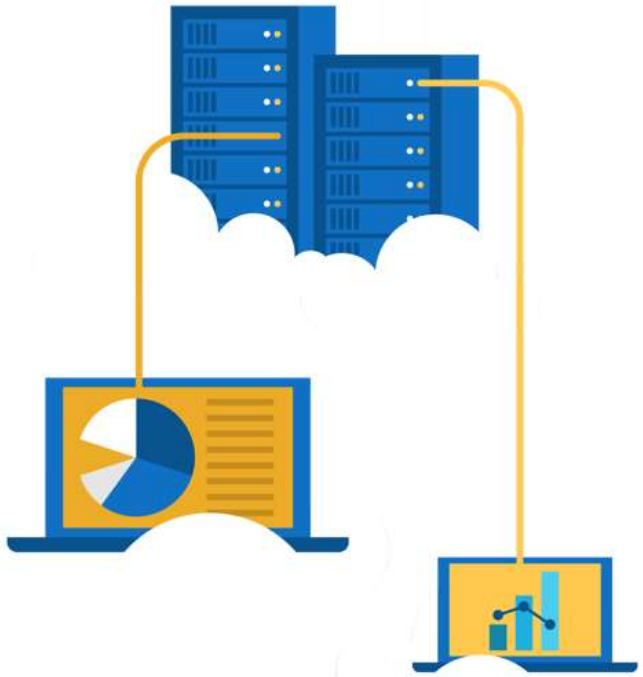
The Trust Center website provides:

- In-depth, expert information.
- Curated lists of recommended resources, arranged by topic.
- Role-specific information for business managers, administrators, engineers, risk assessors, privacy officers, and legal teams.

Walkthrough – Exploring the Trust Center

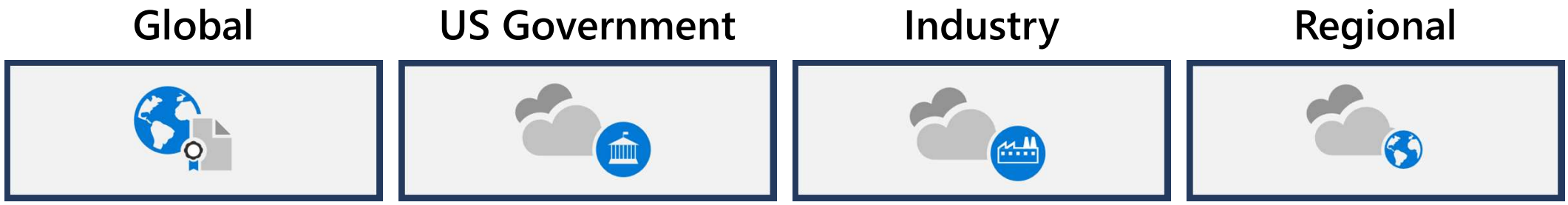
Access the Trust Center, Service Trust Portal (STP), and Compliance Manager.

1. Access the Trust Center.
2. Access the Service Trust Portal.
3. Access the Compliance Manager.



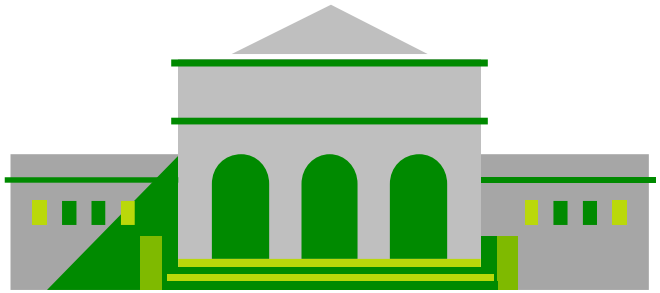
Azure Compliance Documentation

Microsoft offers a comprehensive set of compliance offerings to help your organization comply with national, regional, and industry-specific requirements that govern the collection and use of data.



Azure Sovereign Regions (US Government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.



Azure Government:

- Separate instance of Azure.
- Physically isolated from non-US government deployments.
- Accessible only to screened, authorized personnel.

Examples of compliant standards : FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L2, L4 & L5, and CJIS.

Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet
- All data stays within China to ensure compliance

Module 05 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Azure identity services
- Authentication versus authorization
- Azure AD, MFA, SSO and Conditional Access
- Azure governance features
- RBAC, Resource locks and tags
- Policy, Blueprints, and CAF
- Azure privacy and compliance
- Privacy Statement, Online Services Terms, Trust Center and compliance documentation.
- Azure Sovereign Regions