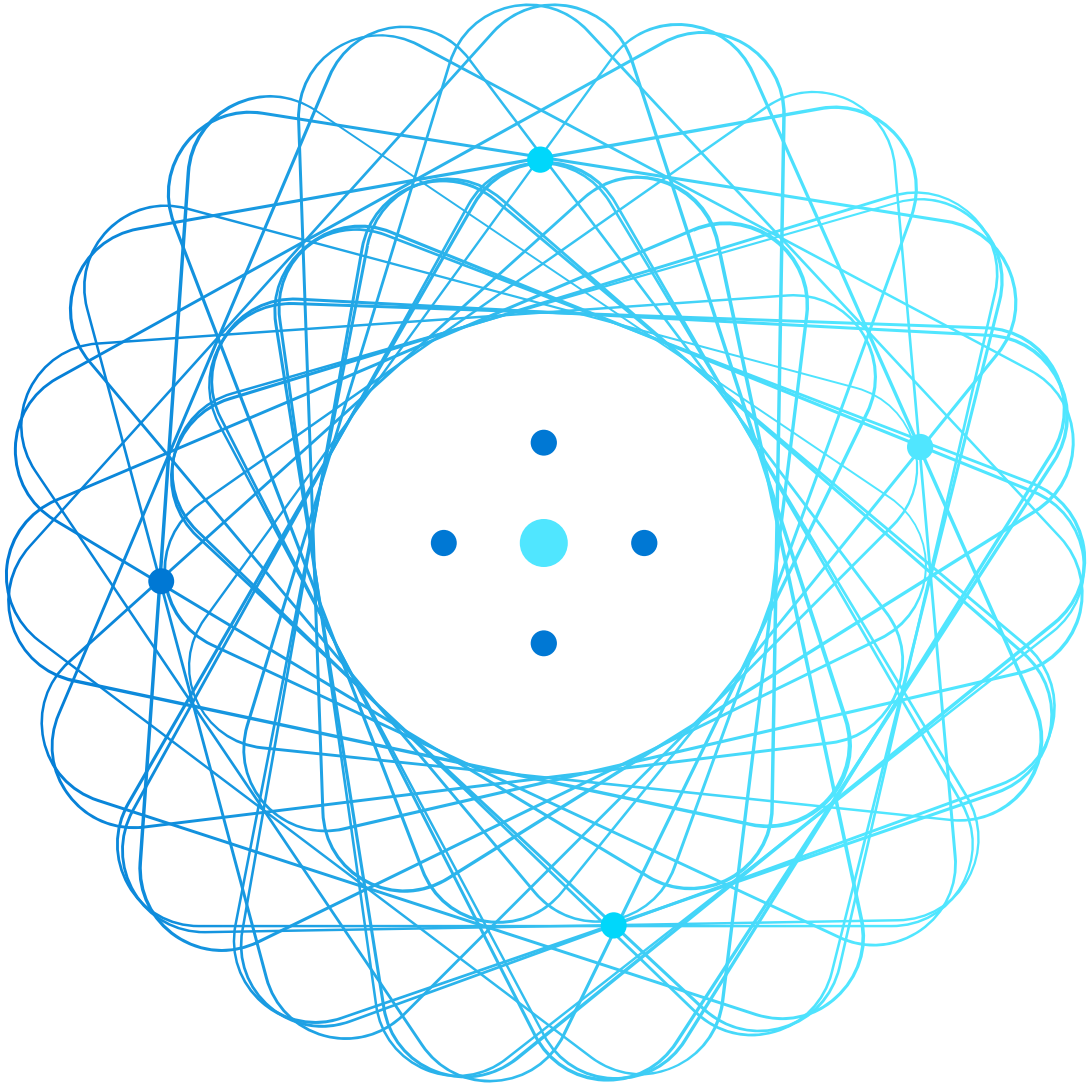
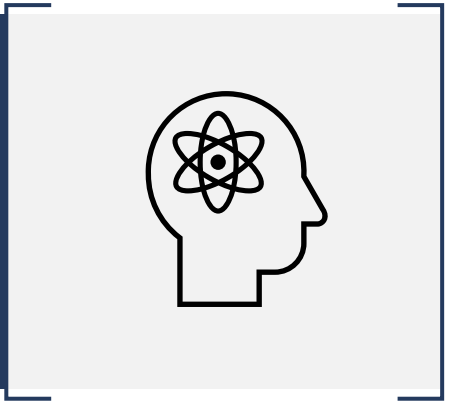
Microsoft Azure

AZ-900

Identity, governance, privacy, and compliance, Security



Module outline

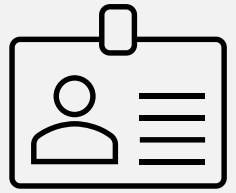


Module – Outline

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 Security features**
  - Security Center and resource hygiene
  - Key Vault, Sentinel, and Dedicated Hosts

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)

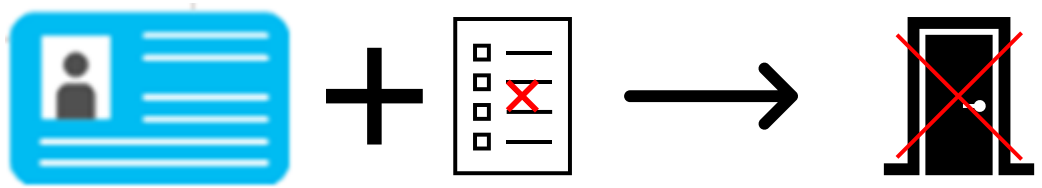
Compare Authentication and Authorization

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

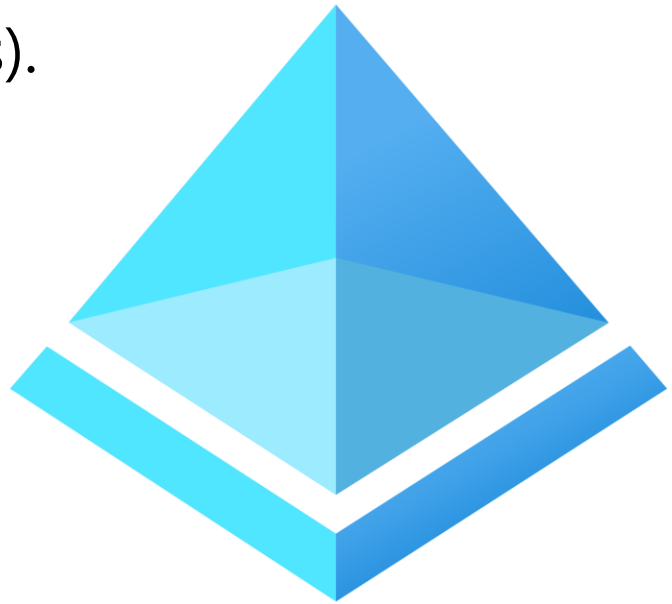
Provides additional security for your identities by requiring two or more elements for full authentication.

- 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.

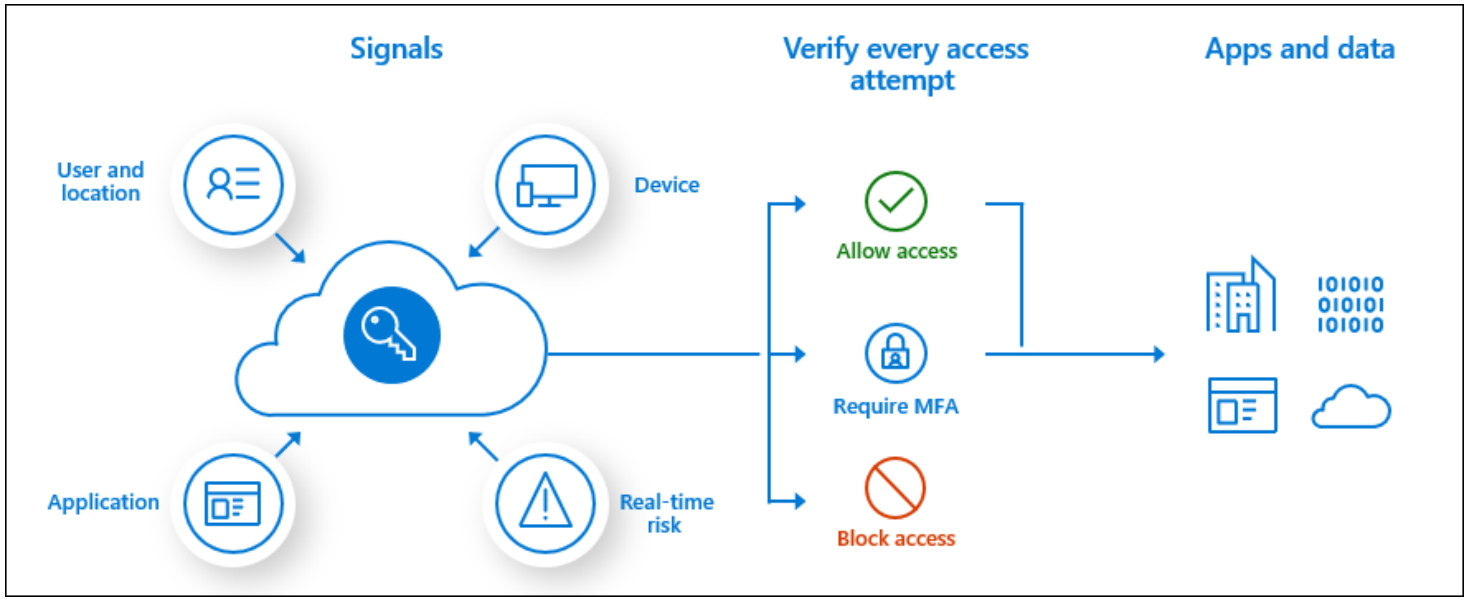
- Authentication (employees sign-in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.



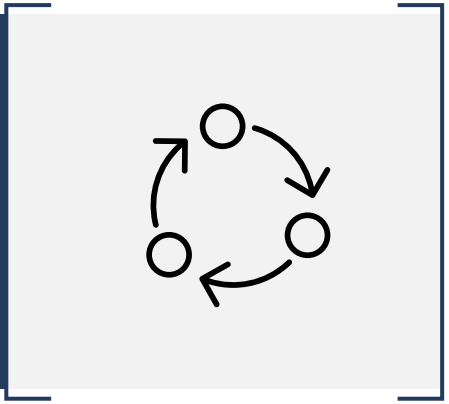
Conditional Access

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



Azure Governance Methodologies

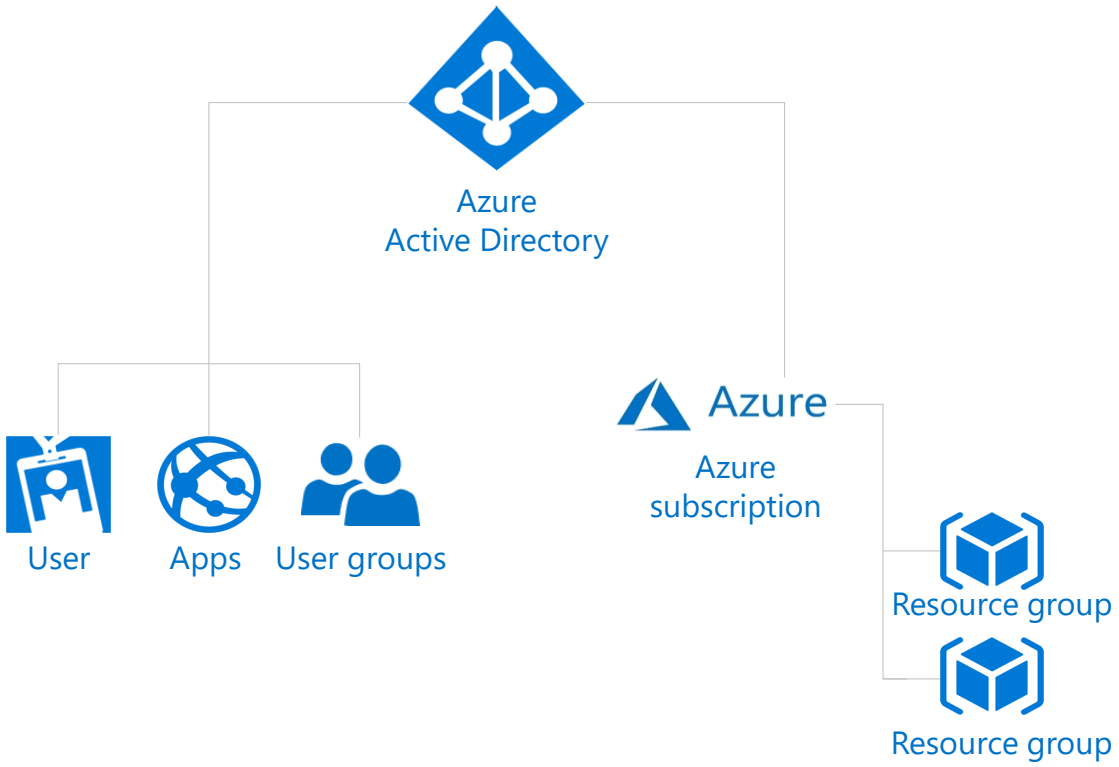


Azure Governance Methodologies - Objective Domain

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

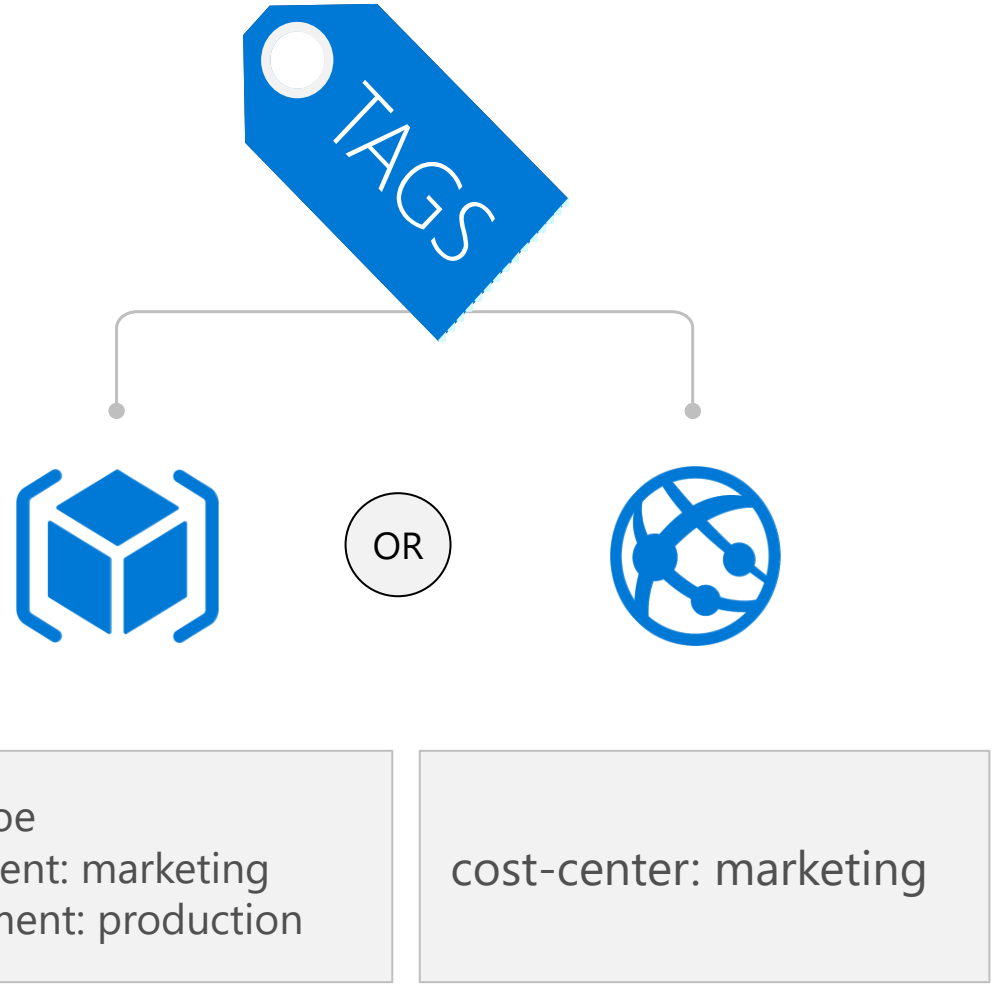
Walkthrough - Manage Resource Locks

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

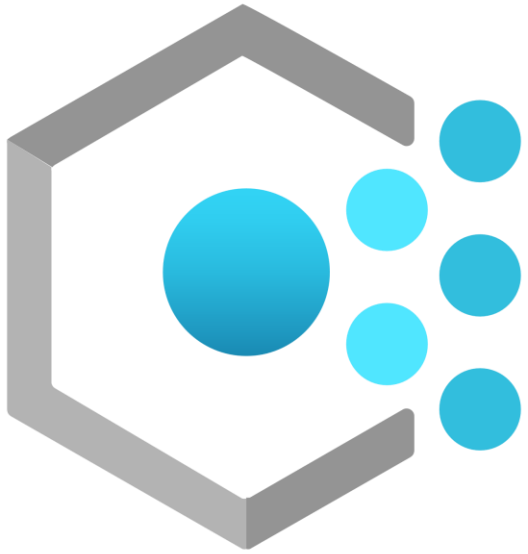
Create a policy assignment that requires tagging, then create a storage account and test the tagging.

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.

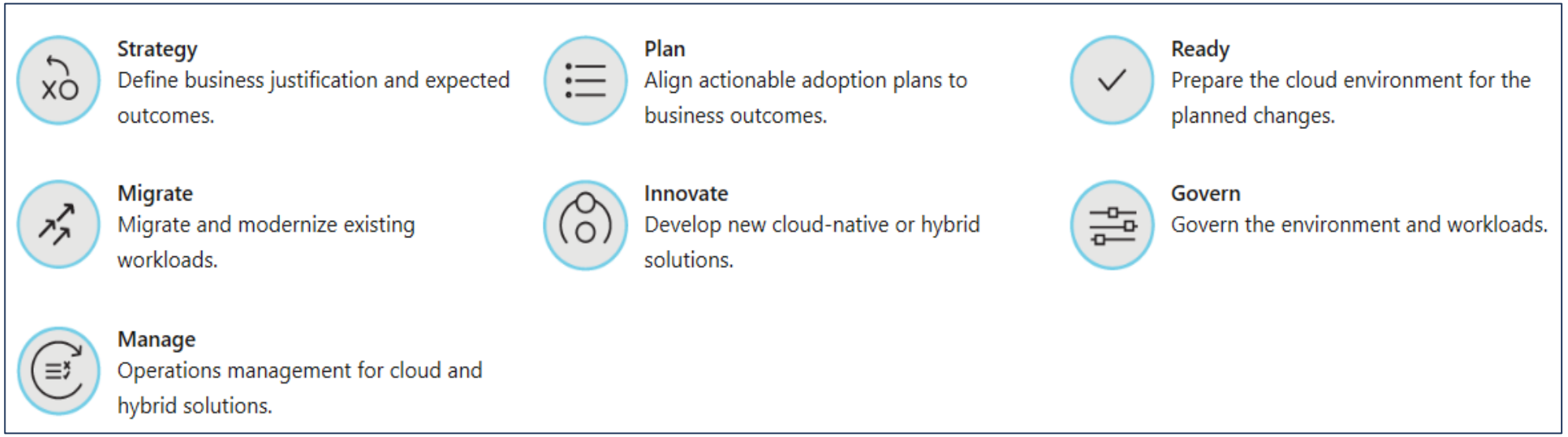
1. Create a policy assignment.
2. Test the allowed location policy.
3. Delete the policy assignment.

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

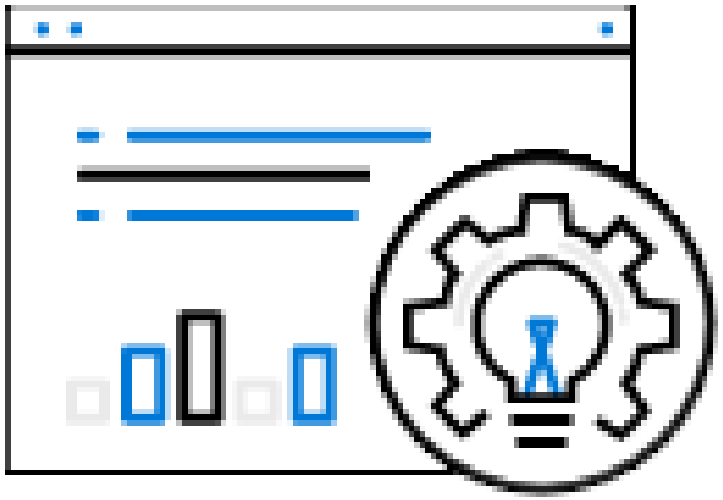
Cloud Adoption Framework



- 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.

Trust Center

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

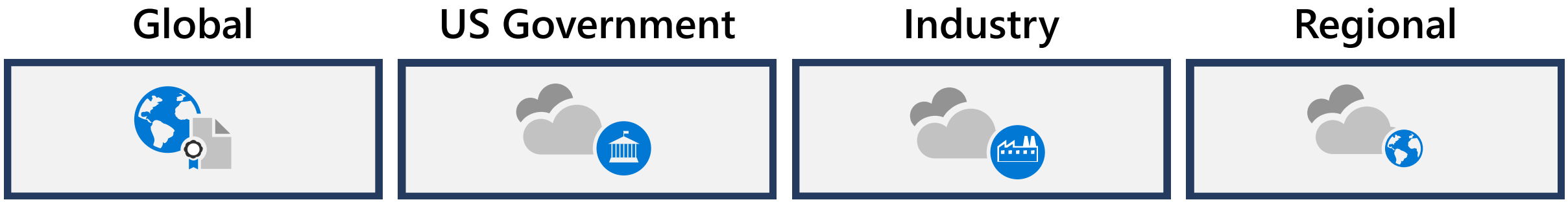


The Trust Center website provides:

- 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.

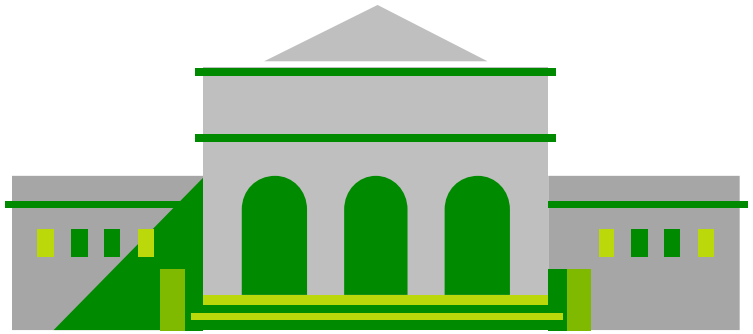
Azure Compliance Documentation

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

Security tools and features

Security tools and features - Objective Domain

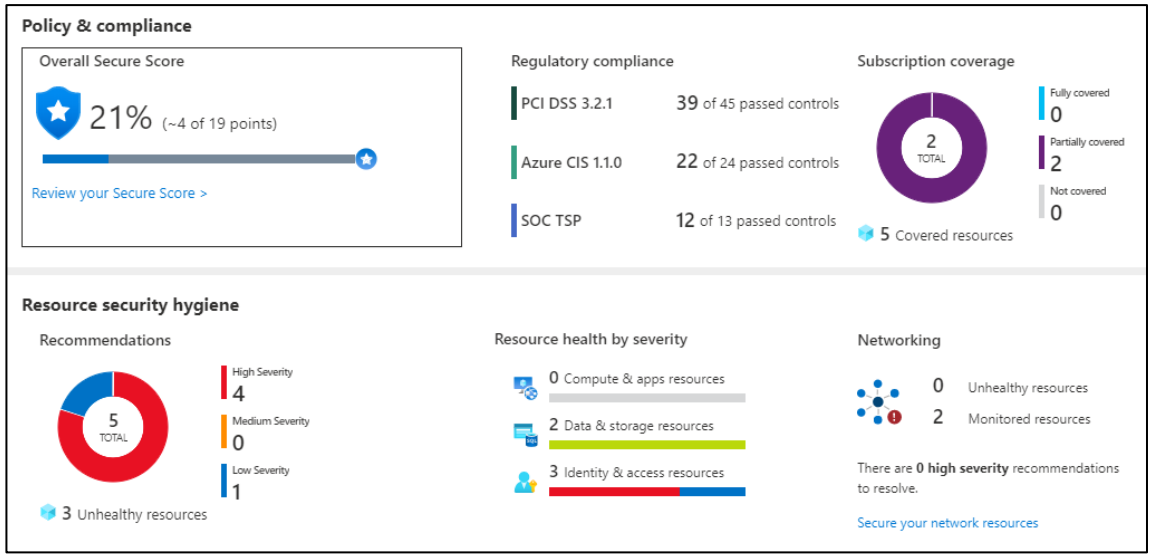
Describe the features and the functionality of:

- Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- Azure Sentinel
- Key Vault
- Azure Dedicated Hosts

Azure Security Center

Azure Security Center is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports



Azure Security Center - capabilities

Policy Compliance

Run policies across management groups, subscriptions, or tenants.

Continuous Assessments

Assess new and deployed resources to ensure that they are configure properly.

Tailored Recommendations

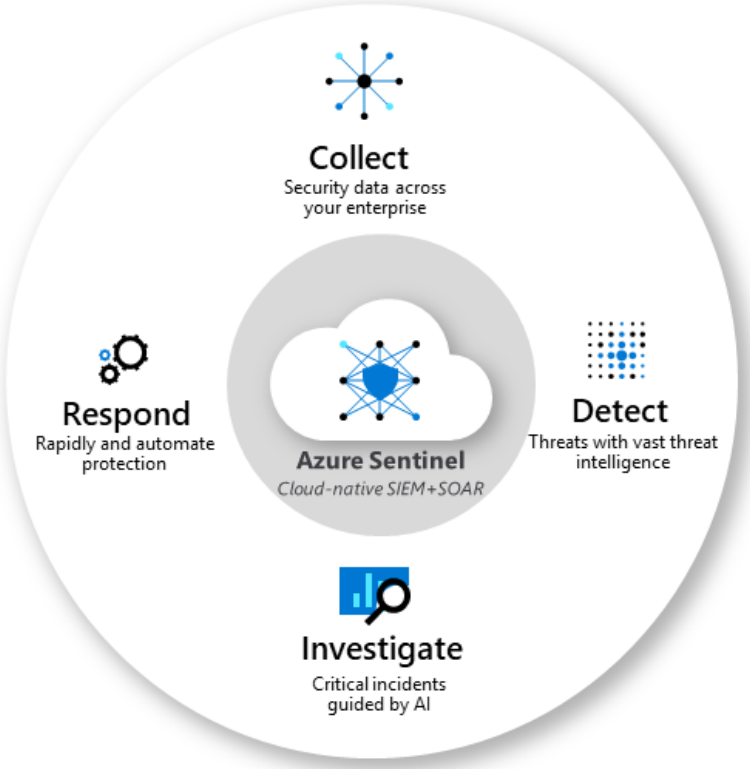
Recommendations based on existing workload with instructions on how to implement them.

Threat Protection

Analyze attempted threats through alerts and impacted resource reports.

Azure Sentinel

Azure Sentinel is a security information management (SIEM) and security automated response (SOAR) solution that provides security analytics and threat intelligence across an enterprise.



Connector and Integrations:

- Office 365
- Azure Active Director
- Azure Advanced Threat Protection
- Microsoft Cloud App Security

Azure Key Vault

Azure Key Vault stores application secrets in a centralized cloud location in order to securely control access permissions and access logging.

- Secrets management.
- Key management.
- Certificate management.
- Storing secrets backed by hardware security modules (HSMs).

Azure Dedicated Host

Azure Dedicated Host provides physical servers that host one or more Azure virtual machines that is dedicated to a single organization's workload.

Benefits

- Hardware isolation at the server level
- Control over maintenance event timing
- Aligned with Azure Hybrid Use Benefits

Module 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

Module Review

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

- Azure Security Center and resource hygiene
- Key Vault, Sentinel, and Dedicated Hosts
- Defense in depth
- DDoS protection

Module – additional resources

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

- AZ-900 Episode 25 | Azure Identity Services | Authentication, Authorization & Active Directory (AD) https://youtu.be/b_WIjY-burU
- AZ-900 Episode 26 | Azure Security Center https://youtu.be/tyztKP9rszU
- AZ-900 Episode 27 | Azure Key Vault | Secret, Key and Certificate Management https://youtu.be/AA3yYg9Zq9w
- AZ-900 Episode 28 | Azure Role-based Access Control (RBAC) https://youtu.be/4v7ffXxOnwU
- AZ-900 Episode 29 | Azure Resource Locks https://youtu.be/eDH20Ve0eI0
- AZ-900 Episode 30 | Azure Resource Tags https://youtu.be/J40eJR4qQ0w
- AZ-900 Episode 31 | Azure Policy https://youtu.be/9WO4EBgUJXk
- AZ-900 Episode 32 | Azure Blueprints https://youtu.be/3rSCnAZPNfo
- AZ-900 Episode 33 | Cloud Adoption Framework for Azure https://youtu.be/d6usiB4MKq8
- AZ-900 Episode 34 | Core tenets of Security, Privacy, Compliance (Trust Center, DPA, OST, and more.) https://youtu.be/zBzsDYZw98M
- AZ-900 Episode 24 | Azure DDoS Protection | Distributed Denial of Service https://youtu.be/MUVFMF9DgM0