Microsoft

AZ-900T01 Module 03: Security, privacy, compliance, and trust

Lesson 01: Learning objectives

Module 3 – Learning objectives

- Understand and describe how to secure network connectivity in Microsoft Azure.
- Understand and describe core Azure identity services.
- Understand and describe security tools and features.
- Understand and describe Azure governance methodologies.
- Understand and describe monitoring and reporting in Azure.
- Understand and describe privacy, compliance, and data protection standards in Azure.

Lesson 02: Securing network connectivity in Azure

Azure Firewall

Stateful, managed, Firewall as a Service (FaaS) that grants/ denies server access based on originating IP address, to protect network resources.

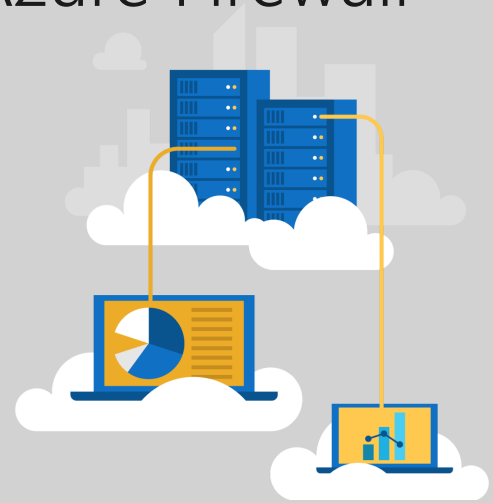
Azure Firewall features :

- applies inbound and outbound traffic filtering rules.
- built-in high availability.
- unrestricted cloud scalability.
- uses Azure Monitor logging.

Walkthrough-Implement an Azure Firewall using Azure Portal

- In this walkthrough task you will create two virtual machines, one which will simulate running a workload, and another which will act as a jump server, which we will use to connect to our workload server. We will then create an Azure Firewall through which all traffic from our workload server will be routed and create rules in Azure Firewall to *allow* access to a particular website.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time



Azure Distributed Denial of Service (DDoS) protection

DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

Azure DDoS Protection features :

- sanitizes unwanted network traffic, before it impacts service availability.
- basic service tier is automatically enabled in Azure.
- standard service tier adds mitigation capabilities, tuned to protect Azure Virtual Network resources.

Network security groups (NSGs)

Filters network traffic to, and from, Azure resources on Azure Virtual Networks.

Network security group features :

- set inbound and outbound rules to filter by source and destination IP address, port, and protocol.
- add multiple rules, as needed, within subscription limits.
- Azure applies default, baseline, security rules to new NSGs.
- override default rules with new, higher priority, rules.

Application Security Groups

Provides for the grouping of servers with similar port filtering requirements, and group together servers with similar functions, such as web servers

Application security group features :

- Allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses
- handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic

Walkthrough-Secure Network traffic using NSGs and ASGs

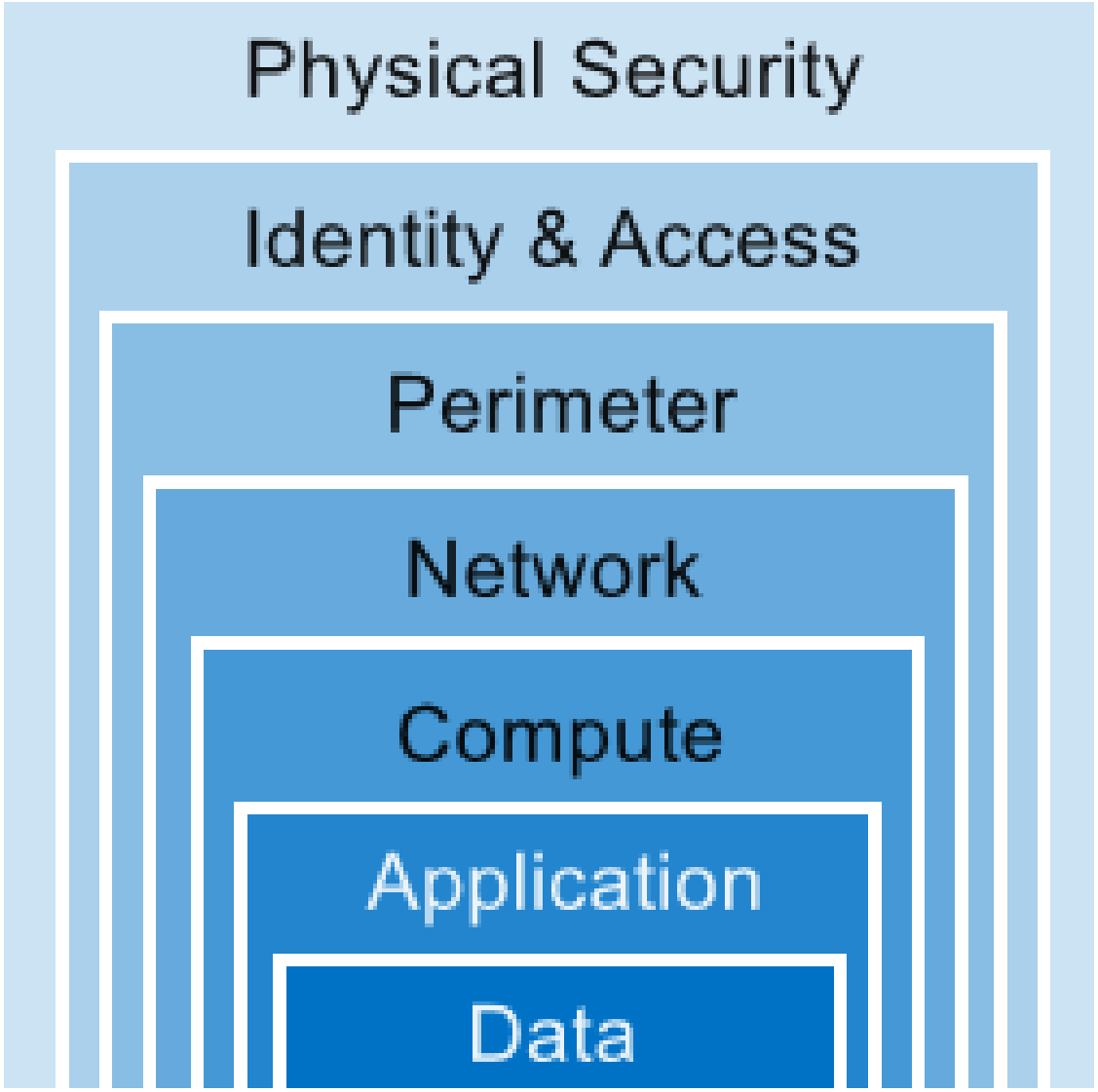
- In this walkthrough task we will create a virtual network and subnet, we will create two ASGs, then create a NSG and associate that NSG to the subnet. We will then create two inbound network security rules.
  We will then create two virtual machines and associate those virtual machines with their respective application security groups, and then with the network security group (NSG). We will then test the network security rules we have created and applied

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

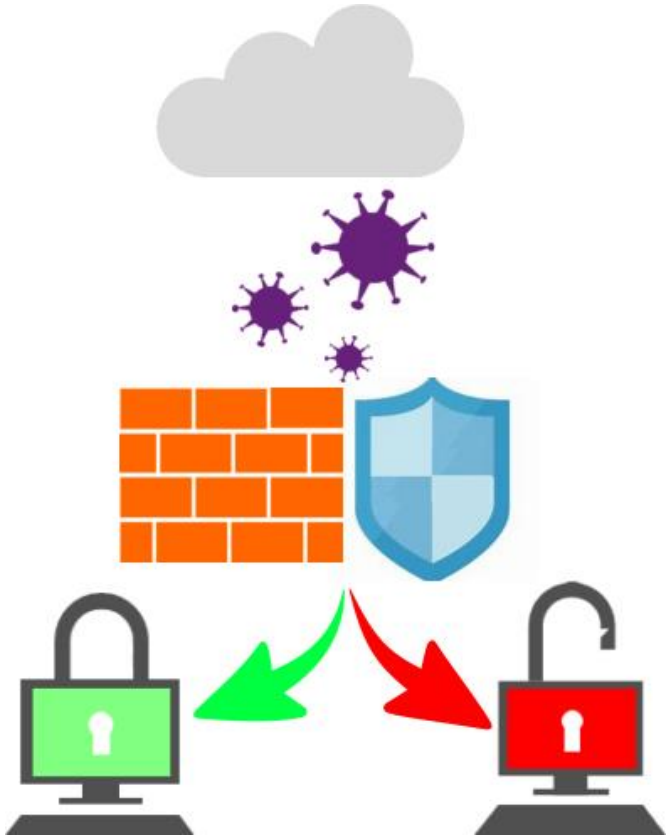
Defense in Depth

A layered approach to securing computer systems.

- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Choosing Azure network security solutions



- **Perimeter layer**: protect your networks' boundaries with Azure DDoS Protection and Azure Firewall.
- **Networking layer**: only permitted traffic should pass between networked resources with Network Security Group (NSG) inbound and outbound rules.

Azure supports combined network security solutions. For example, NSGs with Azure Firewall; Web Application Firewall (WAF) with Azure Firewall.

Shared responsibility

Migrating from customer-controlled to cloud-based data centers shifts the responsibility for security.

Security becomes a shared concern between cloud providers and customers.

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Lesson 03: Core Azure identity services

Authentication and authorization

Two concepts are fundamental to understanding identity and access.

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

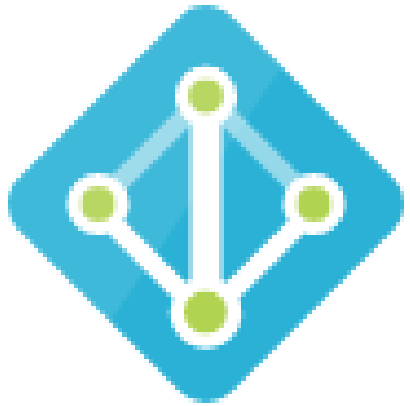
- determines an authenticated person's or service's level of access.
- defines which data they can access, and what they can do with it.

Azure Active Directory (AD)

Microsoft Azure's cloud-based identity and access management service.

Services provided by Azure AD include :

- authentication (employees sign-in to access resources)
- single sign-on (SSO)
- application management
- Business to Business (B2B) and Business to Customer (B2C) identity services



Azure Multi-Factor Authentication

Provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- *Something you know:*
- *Something you possess:*
- *Something you are:*

Lesson 04: Security tools and features

Azure Security Center

A monitoring service that provides threat protection across all your Azure, and on-premises, services.

Azure Security Center features :

- provides security recommendations based on your configurations, resources, and networks.
- monitors security settings across your on-premises and cloud workloads.
- automatically applies your security policies to any new services you provision.

Azure Security Center usage scenarios

- You can use Security Center in the D*etect*, *Assess*, and *Diagnose* stages of an incident response.

- Use Security Center recommendations to enhance security.

Walkthrough-Implement Azure Security Center.

- In this walkthrough task we will create Azure resources to monitor, enable Security Center for your subscription and then from within Security Center, install Agents on a virtual machine to allow more detailed monitoring. We will then evaluate and apply a security recommendation to increase the Secure score value in Security Center.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Azure Key Vault

Stores application secrets in a centralized cloud location, to securely control access permissions, and access logging.

Use Azure Key Vault for :

- secrets management.
- key management.
- certificate management.
- storing secrets backed by hardware security modules (HSMs).

Walkthrough-Create Password secret with Azure Key Vault

- In this walkthrough task we will create an Azure Key vault and then create a password secret within that key vault, providing a securely stored, centrally managed password for use with applications.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Azure Information Protection (AIP)

Classifies and protects documents, and emails, by applying labels.

AIP labels can be applied :

- automatically using rules and conditions defined by administrators.
- manually, by users.
- by combining automatic and manual methods, guided by recommendations.

Azure Advanced Threat Protection (Azure ATP)

Cloud-based security solution for identifying, detecting, and investigating advanced threats, compromised identities, and malicious insider actions.

Consists of Azure ATP :

- **Portal** : dedicated portal for monitoring and responding to suspicious activity.
- **Sensors** : installed directly onto your domain controllers.
- **Cloud service** : runs on Azure infrastructure.

Lesson 05: Azure governance methodologies

Azure Policy

Stay compliant with your corporate standards and service level agreements (SLAs) by using policy definitions to enforce rules and effects for your Azure resources.

Azure Policy features :

- 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.

Policies : Example policy definitions

Allowed Storage Account size

- conditions and rules define acceptable sizes for new storage accounts.
- requests to create storage accounts outside the defined sizes are denied.

Allowed Locations

- defines the Azure locations where your organization can deploy resources, to enforce geographic compliance requirements.
- requests to deploy resources outside the defined locations are denied.

More Azure Policy examples :

docs.microsoft.com/azure/governance/policy/samples/

Initiatives

Initiatives work alongside policies in Azure Policy.

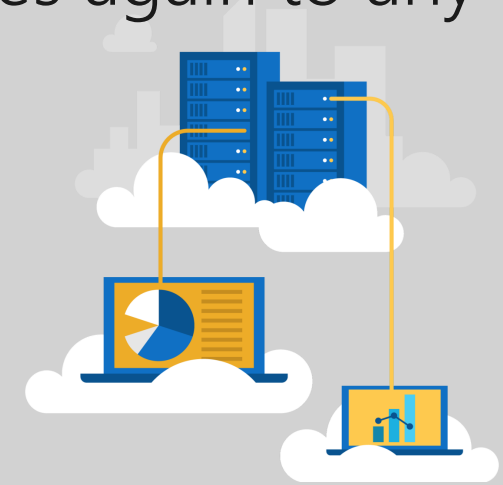
- **Initiative definitions** : Group multiple policy definitions into a single unit, to track compliance at greater/ macro-level scope.

  For example, one initiative can monitor all of your Azure Security Center recommendations.

- **Initiative assignments** : Initiative definitions that are assigned to a specific scope. Initiative assignments reduce the need to make an initiative definition for each scope.

Walkthrough-Create a policy assignment with Azure Policy

- In this walkthrough task we will locate an Azure Policy to restrict deployment of Azure resources to a particular Datacenter, and then assign that allowed location policy to a subscription. We will then verify that creating an Azure resource, such as a virtual machine, outside of the allowed location is blocked. We will finally remove the allowed location policy assignment, to allow us deploy resources again to any Datacenter location using that same subscription.



- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Role-based access control (RBAC)

Fine-grained access management control over your Azure resources.

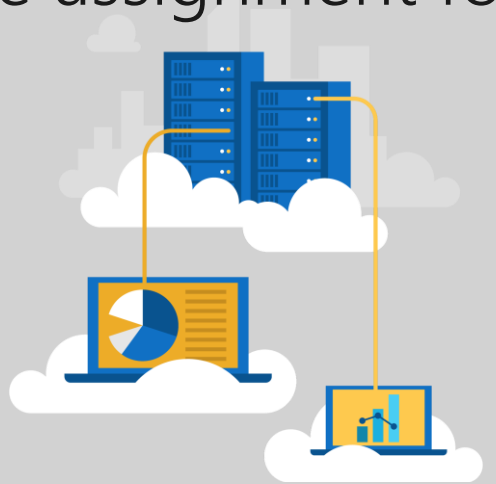
Available to *all* Azure subscribers, at no additional cost.

Example uses of Azure RBAC :

- Grant specific access rights to particular users for certain jobs. One user can manage VMs, while another manages virtual networks.
- Allocate particular database types to certain database administration groups.

Walkthrough-Manage access to Azure resources using RBAC

- In this walkthrough task we will create some Azure resources that we can manage using Role-Based-Access-Control (RBAC), then we will view access control at subscription level, then view roles and permissions at resource group level for azure resources, and view individual user and all role assignments. You will then add a new role assignment for the virtual machine contributor role and then remove a role assignment for the resources you deployed.



- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Locks

Protect your Azure resources from accidental deletion or modification .

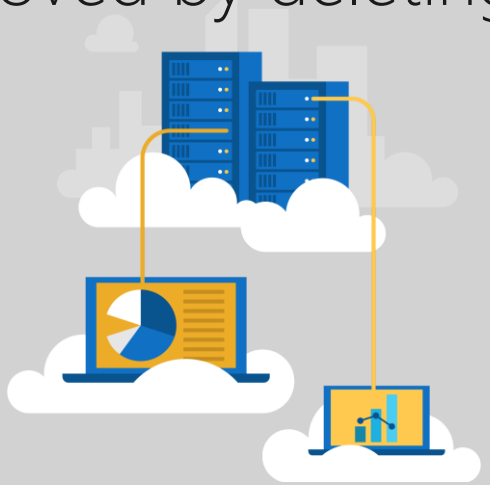
Manage locks at subscription, resource group, or individual resource levels within Azure Portal.

	User Actions		
Lock Types	**Read**	**Update**	**Delete**
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No

Walkthrough-Manage Azure resources using Locks

- In this walkthrough task we will create Azure resources to allow us to create a lock against them, then you will add a **Delete** Lock to prevent deletion of a resource group. You will then verify that deletion of the resource group is indeed blocked, and also that any resources within the resource group are also blocked from being deleted by the parent Lock. You will then remove the lock and verify it has been removed by deleting the resource group.

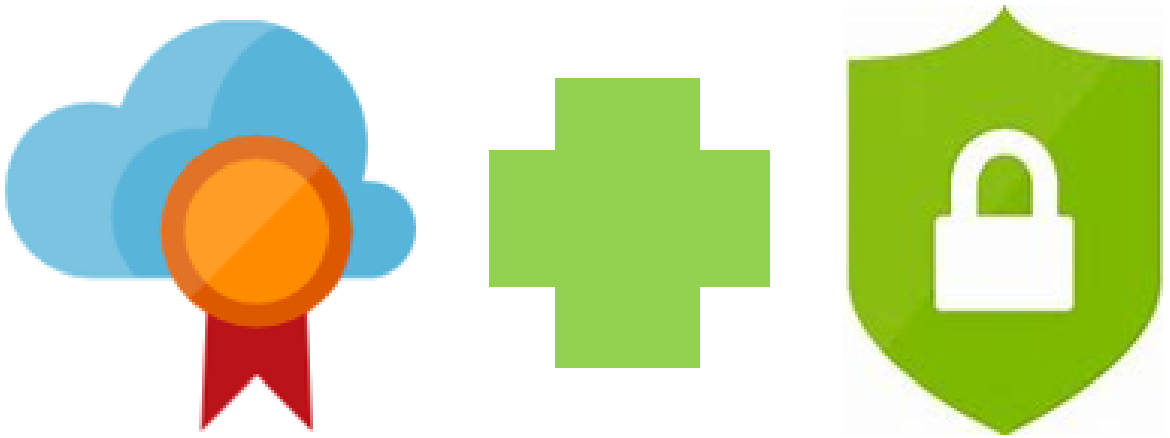
- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time



Azure Advisor security assistance

Get personalized advice and recommendations to improve and enhance security.

- Integrates with Azure Security Center to provide in-depth security recommendations.
- View recommendations in the Azure Advisor dashboard.

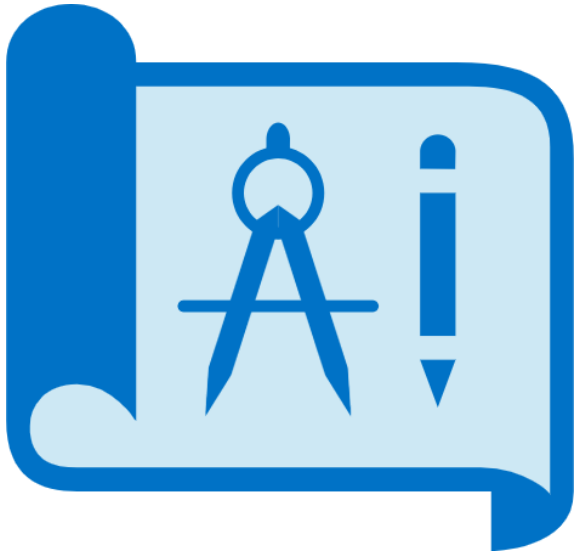


Azure Blueprints

Create reusable environment definitions that can recreate your Azure resources and apply your policies instantly.

Use Azure Blueprints to:

- help audit and trace your deployments, and maintain compliance using built-in tools and artifacts.
- associate blueprints with specific Azure DevOps build artifacts, and release pipelines, for rigorous tracking.



Subscription governance

There are mainly three aspects to consider in relation to creating and managing subscriptions:

- *Billing*: Reports and chargeback can be generated per subscriptions
- *Access Control*: A subscription is a deployment boundary for Azure resources and has the ability to set up role-based access control (RBAC
- *Subscription Limits*: Subscriptions are also bound to some hard limitations If there is a need to go over those limits in particular scenarios, then additional subscriptions may be needed. If you hit a hard limit, there is no flexibility.

Lesson 06: Monitoring and reporting in Azure

Tags

You can apply tags to your Azure resources providing metadata to logically organize them into a taxonomy such as an organization structure, workload, geography or any other logical grouping.

Each tag consists of a name and a value pair

Name	Value
Environment	Production
Department	IT

- Tags are useful when you need to organize resources for billing or management.

Walkthrough-Use Tags with Azure resources

- In this walkthrough task we will create Azure resources to allow us to apply Tags to them. We will then view the tags for a resource and a resource group, and then add Tags to resource groups and resources. We will then bulk assign tags to resources and view all resources with a specific tag. We will finally delete assigned tags.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Azure Monitor

Collect, analyze, and act on telemetry from cloud and on-premises environments, to maximize your applications' availability and performance.

- starts collecting data as soon as you create an Azure subscription and add resources.
- *Activity Logs* record all resource creation and modification events.
- *Metrics* measure resource performance and consumption.
- add an Azure monitor agent to collect operational data for a resource.

Walkthrough-Monitor VMs using Azure Monitor

- In this walkthrough task we will view the default available monitoring data from within the VM resource data and then from within Azure Monitor. We will view some of the monitoring options available in Azure Monitor, create a Log Analytics workspace, enable Insights in our VM, then review the retrieved data in Azure Monitor. We will enable diagnostic settings in the VM and query and analyze virtual machine logs in Log Analytics workspace and Azure Monitor Logs.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Azure service health

Evaluate the impact of Azure service issues with personalized guidance and support, notifications, and issue resolution updates.

Components of Azure service health :

- **Azure Status** : provides a global overview Azure services' state of health.
- **Service Health** : customizable dashboard for tracking the state of services in the regions you use.
- **Azure Resource Health** : diagnose and obtain support for Azure service issues affecting your resources.

Monitoring applications and services

Integrate Azure Monitor with other Azure services to improve your data monitoring capabilities, and gain better insights into your operations.

Analyze	Use variants of Azure Monitor for resources (containers, virtual machines, etc.), with Azure Application Insights for applications.
Respond	Azure Alerts can respond proactively to critical conditions identified in your monitor data, and use Auto-scale with Azure Monitor Metrics.
Visualize	Use Azure Monitor data to create interactive visualizations, charts, and tables with Power BI.
Integrate	Integrate Azure Monitor with other systems to build customized solutions to suit your needs and requirements.

Lesson 07: Privacy, compliance and data protection standards in Azure

Compliance Terms and Requirements

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

CJIS (Criminal Justice Information Services)	**HIPAA** (Health Insurance Portability and Accountability Act)
CSA STAR Certification	**ISO/IEC 27018**
General Data Protection Regulation (GDPR)	**National Institute of Standards and Technology (NIST)**

You can view all the Microsoft compliance offerings at Microsoft Compliance Center - Compliance Offerings.

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 :

- which data Microsoft process,
- how Microsoft processes it,
- and for what purposes.

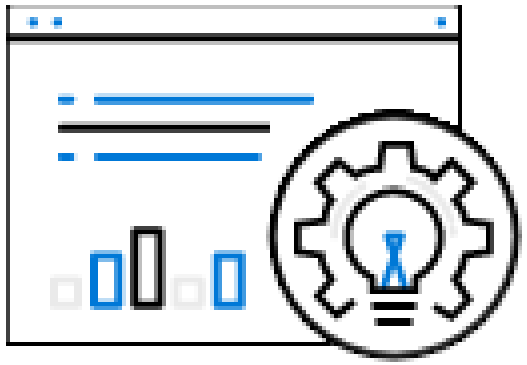
Review Microsoft's Privacy Statement at :

microsoft.com/privacystatement

Trust Center : microsoft.com/trustcenter

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

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, legal teams, and more.

Service Trust Portal (STP) : servicetrust.microsoft.com

A Trust Center companion website for compliance-related publications about Microsoft cloud services. Hosts the Compliance Manager service.

Use STP to access :

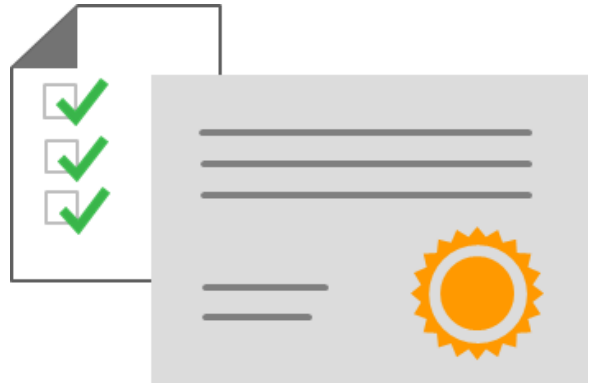
- audit reports across Microsoft cloud services.
- guides to using Microsoft cloud services for regulatory compliance.
- publications about trust, and how Microsoft cloud services protect your data.

Compliance Manager

Workflow-based, risk assessment tool in Trust Portal that supports your organization's regulatory compliance activities.

Compliance Manager features :

- assign, track, and verify your compliance and assessment-related activities.
- provides a score by evaluating your compliance status.
- stores and manages your compliance-related artifacts in a secure digital repository.



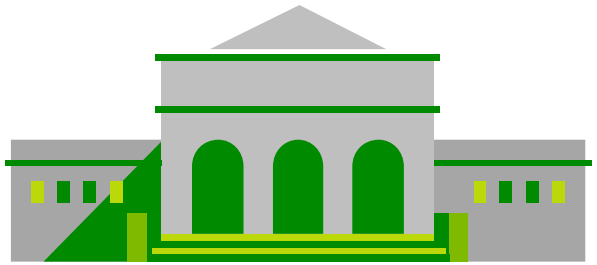
Walkthrough-Accessing Trust Center, STP and Compliance Manager

- In this walkthrough task we will access the Trust Center and browse through some of its content. Then we will access the Service Trust Portal (STP) and some of its resources and content, and finally we will access Compliance Manager and some of its available resources.

- You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time

Azure Government services

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



Azure Government :

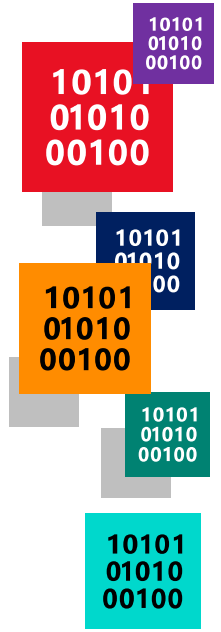
- separate instance of Azure.
- physically isolated from non-US government deployments.
- accessible only to screened, authorized personnel.

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

Azure Germany services

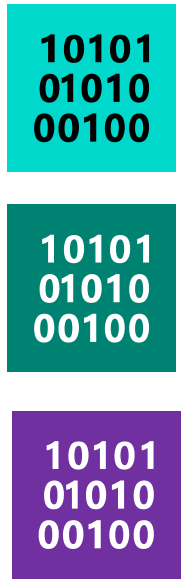
Meets strict data protection, access, and control requirements under German law. Features of Azure Germany include:

- customer data and supporting systems reside in German data centers.
- data centers are managed by an independent, German data trustee.
- data replication confined to German data centers to support business continuity.
- anyone who requires data to reside in Germany can use this service



Azure China 21Vianet

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



Azure China 21Vianet features :

- physically separated instance of Azure cloud services, located in China.
- operated by 21Vianet (Azure China 21Vianet).

Lesson 08: Module 3 review questions

Module 3 review questions

1. There has been an attack on your public-facing website. The application's resources have been overwhelmed and exhausted, and are now unavailable to users. What service should you use to prevent this type of attack?
2. Azure AD is capable of providing which services?
3. Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?