Document/Website	Info	Offers	Audience
Microsoft Privacy Statement	Collection, Purpose and Usage of Personal Data	All Microsoft offers including services, applications, websites, software, servers, devices	Everyone - end customers or companies
Online Services Terms (OST)	Licensing Terms (legal agreement) - usage rights about Azure services. What can be done and what is forbidden.	Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps, etc.	Organizations - legal teams
Data Protection Addendum	Appending to OST describing obligations by both parties (Microsoft and you) with regards to the processing of customer and personal data	Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps, etc.	Organizations - legal teams, security teams
Trust Center	One stop shop web portal for everything related to security, compliance, privacy, policies, best practices, etc.	Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps, etc.	Organizations - legal teams, security teams, business managers, administrators
Azure Compliance Documentation	Web portal focusing on compliance offerings in Azure, simmilar to the trust center but narrowed down	Azure	Organizations - legal teams, security teams, business managers, Azure administrators

Azure Sovereign Regions

Azure Sovereign Regions provide Azure services in markets with very strict regulatory requirements

- Azure Government designed for the US government
  - Separate instance of Azure (lifecycle, services, portal, etc.)
  - Physically isolated from other Azure regions
  - Only autorized scanned personel can get access
- Azure China designed for the Chinese market
  - Separate instance of Azure (lifecycle, services, portal, etc.)
  - Physically isolated from other Azure regions
  - Operated by a Chinese telecom company called 21Vianet

Cost Affecting Factors

- Base Cost
  - **Resource Types** – All Azure services (resources) have resource-specific pricing models. Typically consisting of one or more metrics.
  - **Services** – Azure specific offers (Enterprise, Web Direct, CSP, etc.) have different cost and billing components like prepaids, billing cycles, - discounts, etc.
  - **Location** – running Azure services vary between Azure regions
  - **Bandwidth** – network traffic when uploading (inbound/ingress) data to Azure or downloading (outbound/egress) from Azure
- Savings
  - Reserved Instances
  - Hybrid Benefits

Azure Reservations

Purchase Azure services for 1 or 3 years in advance with a significant discounts

- **Reserved instances** – Azure Virtual Machines
- **Reserved capacity** – Azure Storage, SQL Database vCores, Databricks DBUs, Cosmos DB RUs

- **Software plans** – Red Hat, Red Hat OpenShift, SUSE Linux, etc.
- **Reservations** are made for 1 or 3 years

Azure Spot VMs

Purchase unused Virtual Machine capacity for significant discount

- How it works
    - **Significant dicount** for Azure VMs
    - **Capacity** can be **taken away at any time**
    - Customer can **set maximum price** after discount to keep or evict the machine
- **Best for interruptable workloads** (batch processing, dev/test environments, large compute workloads, non-critical tasks, etc.)

Hybrid use Benefit

Use existing licenses in the cloud

- Use existing licenses in the Azure
    - **Windows Server**
        - Azure VM
    - **RedHat**
        - Azure VM
    - **SUSE Linux**
        - Azure VM
    - **SQL Server**
        - Azure SQL Database
        - Azure SQL Managed Instance
        - Azure SQL Server on VM
        - Azure Data Factory SQL Server Integration Services

Tools

- **Pricing calculator** – estimate the cost of Azure services
    - Select service
    - Adjust parameters (usage)

    - View the price
- **Total Cost of Ownership (TCO) calculator** – estimate and compare the cost of running workloads in datacenter versus Azure
    - Define your workloads
    - Adjust assumptions
    - View the report

Azure Cost Management

- A centralized service for reporting usage and billing of Azure environment
- Self-service cost exploration capabilities
- Budgets & alerts
- Cost recommendations
- Automated exports

Minimizing Costs in Azure

1. Azure Pricing Calculator to choose the low-cost region
    - Good latency
    - All required services are available
    - Data sovereignty/compliance requirements
2. Hybrid use benefit and Azure Reservations
3. Azure Cost Management monitoring, budgets, alerts and recommendations
4. Understand service lifecycle and automate environments
5. Use autoscaling features to your advantage
6. Azure Monitor to find and scale down underutilized resources
7. Use tags & policies for effective governance

SLA

Service Level Agreement (SLA) is a formal agreement between a service provider and a customer.

SLA is a **promise** of a service’s **availability** (uptime & connectivity). **Availability** is a measure of time that a service remains operational.

Identity

- **Centralized/unified** infrastructure and platform **security management service**
- **Natively embedded** in Azure services
- **Integrated** with **Azure Advisor**
- Two tiers
    - **Free** (Azure Defender OFF) – included in all Azure services, provides continuous assessments, security score, and actionable security recommendations
    - **Paid** (Azure Defender ON) – hybrid security, threat protection alerts, vulnerability scanning, just in time (JIT) VM access, etc.

Azure Key Vault

- **Managed service** for **securing sensitive information** (application/platform) (PaaS)
- **Secure storage service** for
    - **Keys**,
    - **Secrets** and
    - **Certificates**
- **Highly integrated** with other Azure services (VMs, Logic Apps, Data Factory, Web Apps, etc.)
- **Centralization**
- Access **monitoring** and **logging**

What is a Role?

Role (role definition) is a **collection of actions** that **the assigned identity** will be able to perform.

Role definition is an answer to a question "**What** can be done?"

What is a Security Principal?

Security Principal is an Azure object (identity) that
can be assigned to a role (ex. users, groups or applications).

Security Principal assignment is an answer to a question "**Who** can do it?"

What is a Scope?

Scope is one or more Azure resources that the access applies to.

Scope assignment is an answer to a question "**Where** can it be done?"

What is a Role Assignment?

Role assignment is a combination of the **role definition**, **security principal** and **scope**.

Azure Role-based Access Control (RBAC)

- Authorization system built on Azure Resource Manager (ARM)
- Designed for fine-grained access management of Azure Resources
- Role assignment is combination of
  - Role definition – list of permissions like create VM, delete SQL, assign permissions, etc.
  - Security Principal – user, group, service principal and managed identity and
  - Scope – resource, resource groups, subscription, management group
- Hierarchical
  - Management Groups > Subscriptions > Resource Groups > Resources
- Built-in and Custom roles are supported

What is an Azure Resource Lock?

- Designed to **prevent accidental deletion** and/or **modification**
- Used in conjunction with RBAC
- Two types of locks
  - **Read-only** (**ReadOnly**) – only read actions are allowed
  - **Delete** (**CanNotDelete**) – all actions except delete are allowed
- Scopes are **hierarchical** (**inherited**)
  - Subscriptions > Resource Groups > Resources
- **Management Groups** can't be locked
- Only **Owner** and **User Access Administrator** roles can manage locks (**built-in** roles)

Azure Resource Tags

- Tags are simple **Name** (key) - **Value pairs**
- Designed to help with **organization of Azure resources**
- Used for resource **governance**, **security**, **operations management**, **cost management**, **automation**, etc.
- Typical **tagging strategies**
  - **Functional** – mark by **function** (ex: environment = production)
  - **Classification** – mark by **policies used** (ex: classification = restricted)
  - **Finance**/**Accounting** – mark for **billing purposes** (ex: department = finance)
  - **Partnership** – mark by **association of users/groups** (ex: owner = adam)
- Applicable for **resources**, **resource groups** and **subscriptions**
- **NOT inherited** by default

Azure Policy

- Designed to help with resource **governance**, **security**, **compliance**, **cost management**, etc.
- **Policies** focus on **resource properties** (**RBAC** focused on **user actions**)

- Policy **definition** – Defines what should happen
    - Define the **condition** (if/else) and the **effect** (deny, audit, append, modify, etc.)
    - Examples include allowed *resource types*, *allowed locations*, *allowed SKUs*, *inherit resource tags*
- **Built-in** and **custom** policies are supported
- Policy **initiative** – a **group** of policy definitions
- Policy **assignment** – assignment of a policy definition/initiative to a scope
    - Scopes can be assigned to
        - management groups,
        - subscriptions,
        - resource groups, and
        - resources
- Policies allow for **exclusions of scopes**
- Checked during **resource creation** or **updates** and **existing ones with remediation tasks**