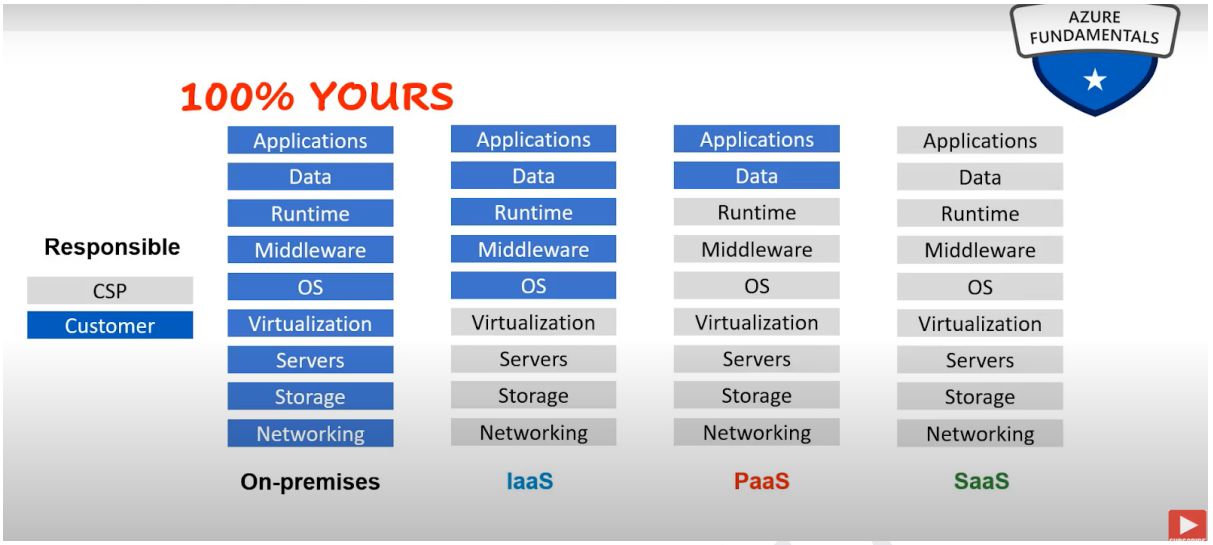
Share Responsibility model



IaaS examples - Azure virtual machines,azure files, Amazon EC2, GCP compute engine,azure storage

PaaS examples - Azure SQL Database, API management, Azure app service

SaaS examples - Microsoft office 365, servicenow,salesforce

A DNS server that runs on azure virtual machine is an example of PaaS

Legacy DB on IaaS, Legacy software on PaaS

Benefits of Cloud computing - cloud is cost effective, global, secure,scalable,elastic

Public cloud - everything runs on your cloud provider's hardware.advantages include scalability,agility,pay as you go, no maintenance and low skills.

Private cloud - a cloud environment in your own datacenter. Advantages include legacy support,control and compliance

Hybrid cloud - combines public and private clouds, allowing you to run your apps in the right location.advantages include flexibility in legacy,compliance and scalability scenarios

For only private and hybrid clouds we can deploy physical servers.

Scalability - the ability of a system to handle growth of users or work.

Elasticity - the ability of a system to automatically grow and shrink based on app demand.

Agility - the ability to react quickly to changes in demand without manual intervention.

Economies of scale - the ability to do things more efficiently or at a lower cost per unit when operating at a larger scale.

Capital Expenditure(CapEx) - is the spending of money on physical infrastructure upfront.

Operational Expenditure(OpEx) - is spending money on services or products now and being billed as you go. Also includes staff salaries and software leasing costs.

The cloud increases OpEx spending and reduces CapEx spending

Consumption based model - pay for what you use, typically per unit of time or capacity(min/gb/execution)

Fault tolerance - the ability of a system to handle faults in a service like power,network or hardware failures. Typically refers to component level failures.

High availability - the ability to keep services up and running for long periods of time. Typically refers to service level failures.

Disaster recovery - the ability to recover from an event which has taken down a cloud service. Generally refers to recovery in event of service or site failure.

Azure geography - a discrete market typically containing 2 or more regions that preserves data residency and compliance boundaries.

Azure region - a set of data centers deployed within a latency defined parameter and connected through a dedicated regional low-latency network.

Region pairs - a relationship between 2 azure regions within the same geographic region for disaster recovery purposes.

Availability Zones - unique physical locations within a region with independent power,network and cooling.comprised of one or more data centers.tolerant to datacenter failures via redundancy and isolation.

Management groups -> subscriptions -> resource groups -> resources

Each directory is given a single top level management group called the root Subscription - is a logical container used to provision resources in azure. Are a unit of management,billing and scale within Azure. Serve as a management boundary for assigning azure policies,governance and isolation.

We generally create multiple subscriptions when subscription limits are reached, to use different payment methods, to isolate resources between departments, projects etc.

Resource groups - a container that holds related resources for an azure solution. Used to group resources that share a common resource lifecycle.

Resources - an entity managed by azure like a VM, virtual network or storage account

Management group - can be used to aggregate policy and initiative assignments via Azure Policy. Can contain multiple subscriptions. All new subscriptions will be placed under the root management group by default.

Azure VM's - server virtualization(compute) on-demand without need for hardware purchase.

App service - an HTTP based service for hosting web applications, REST API's and mobile backends.

Cloud Orchestration is the process of automating the tasks needed to manage connections and operations of workloads on private and public clouds.

Serverless is a cloud-native development model that allows developers to build and run applications without having to manage servers.

Azure Container Instance(ACI) - runs docker container on-demand in a managed serverless azure environment. A solution for any scenario that can operate in isolated containers without orchestration.

Azure Kubernetes service(AKS) - a hosted kubernetes service, azure handles critical tasks like health monitoring and maintenance for you. AKS is free- you only pay for the agent nodes within your clusters not for the masters.

Windows Virtual desktop - a desktop and app virtualization service that runs in microsoft azure, it enables IT Pros and MSP's to create windows 10 virtual desktops in azure.

MSP - A managed service provider (MSP) is a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems

Virtual Network(VNet) - a logical representation of your network in azure. A VNet contains one or more subnets.VNet’s provide logical isolation in azure dedicated to your subscription.

Using VNet we can create a dedicated private cloud-only network, securely extend your data center(site-to-site VPN), and enable hybrid cloud scenarios.

VM’s in different VNets can't communicate by default.

VPN Gateway - a virtual network gateway that sends encrypted traffic between an azure VNet and on-premises location over the internet. This is the core component of hybrid cloud.
Traffic traverses the internet.

VNet Peering - enables seamless connection of 2 or more virtual networks in azure. The 2 networks function as one in terms of connectivity.

Express route - extends your on-premises networks into Azure over a private connection with the help of a connectivity provider. Traffic doesn't traverse the internet. Considered more secure.

Blob storage - storage optimized for storing massive amounts of unstructured data. Unlimited storage,no-resizing volumes,file system protocols.

File storage - fully managed file shares in azure accessible via SMB or NFS

SMB - Server message block is a client server communication protocol used for sharing access to files,printers, serial ports on a network. Runs on windows

NFS - Network file system. Similar to SMB runs on Linux

Disk storage - azure managed disks are block level storage volumes that are managed by azure and used with azure VM’s. choose SSD or HDD.

Storage tiers - azure storage hot,cool and archive access tiers to store blob object data in a cost effective manner.

Table storage - a service that stores structured NoSql data in azure,including a schemaless key/attribute store. It's relatively cheap ,fast and easy to manage.

Queue storage - a service for storing large numbers of messages,accessible from anywhere via authenticated HTTP or HTTPS calls.

Azure Databox/databox heavy - a rugged briefcase computer and storage designed to move terabytes or petabytes of data.

Azure archive storage - long term cold storage for when you need to hold onto files for years on the cheapest storage options.

Azure data lake storage - a centralized repo that allows you to store all your structured and unstructured data at any scale.

Cosmos DB - a fully managed NoSql database for modern app development. It features ultra low response latency and API's for several languages and DB platforms.

MS SQL - a fully managed Paas database engine that handles most management functions such as upgrading,patching,backups and monitoring.

PostgreSQL - a relational database service in the Microsoft cloud based on PostgreSQL community edition.
MySQL - a relational database service in the Microsoft cloud based on MySQL community edition.

SQL Managed instance - cloud database service that combines the broadest SQL server database engine compatibility with all the benefits of a PaaS.

Azure marketplace -catalog of apps and services. Deploy seamlessly and simplify billing with a single bill for all microsoft and third party applications.

IOT Hub - a central message hub for bi-directional communication between your IOT app and the device it manages. The IOT hub is bi-directional but the event hub is not.

IOT central(fully managed SaaS solution) - an IOT application platform that simplifies the creation of IOT solutions.helps to reduce burden and cost of IOT management operations and development.

Azure Sphere - secure,high level application platform with built in communication and security features for internet connected devices. Basically a linux based OS and cloud based security service that provides continuous,renewable security.

Azure sphere is created by microsoft to run on an azure sphere certified chip(microcontroller chip) and to connect to azure sphere security service.

Data Lake - a technology that enables big data analytics and AI. provides cloud storage that is less expensive than relational databases cloud storage.stores data from business systems and data warehouses as well as device and sensor data.

Data lake is a place to store ,organize and analyze large volumes of structured and unstructured data of diverse data from diverse resources.

Synapse Analytics - an integrated analytics service that accelerates time to insight across data warehouses and big data systems. Intended to run SQL queries against large databases for things such as reporting.Was formerly known as Azure SQL Data Warehouse.

Azure database migration service - migrates your databases to cloud with no application code changes.

Azure cache for redis - caches frequently used and static data to reduce data and application latency.

Azure table storage - wide-column NoSql db. A NoSql store that hosts unstructured data independent of any schema.

HDInsight - a cloud distribution of Hadoop components that makes it easy,fast and cost effective to process massive amounts of data.supports open source frameworks such as Hadoop,Spark,Hive,LLAP,Kafka,Storm,R etc.

Databricks - a data analytics platform optimized for the microsoft azure cloud services platform.
It offers 2 environments for developing data intensive applications : Azure Databricks SQL Analytics and azure databricks workspace.

Azure Machine Learning - a cloud based environment you can use to train,deploy,automate ,manage and track ML models.

Cognitive services - cloud based services with REST API and client library SDKs available to help you build cognitive intelligence into your applications. Provides cognitive understanding categorized into 5 main pillars:
vision,speech,language,decision and search

Azure bot service - a managed bot development service that helps you connect to users via popular channels. Provides an integrated environment that is purpose-built for bot development.

Serverless : 1) logic app 2) functions 3) event grid.

Logic app- a cloud service that helps you schedule,automate and orchestrate tasks, business,processes and workflows. You can choose from a gallery of hundreds of pre-built connectors for 3rd party services.

Functions - an event driven,compute on demand experience that extends the existing azure application platform with capabilities to implement code triggered by events occurring in azure as well as on-premises systems.

Event grid - enables you to easily manage events across many different azure services and applications. Once a subscription is created, the event grid will push events to the configured destination. Makes it easy for any developer to utilize the push model instead of the inefficient pull across their serverless architecture.

Paas	Serverless
More control over deployment environment	Less control over deployment environment
Application has to be configured to auto-scale	Application scales automatically
Application takes a while to spin up	Application code only executes when invoked

Azure Devops - a single platform for implementing Devops deploying code using CI/CD framework facilitating agile software development.

Github - a web based repository hosting service for source code management(SCM) and distributed revision control.

Azure DevTest labs - provides a self service sandbox environment to quickly create Dev/test environments while minimizing waste and controlling costs.

Azure portal - a web based unified console where you can manage your azure subscription using a GUI.

Azure cloud shell - an interactive,authenticated,browser-accessible shell for managing azure resources.

Azure mobile app - app for ios and android that enables managing tracking health and status ,troubleshooting your resources.

Azure CLI - azure CLI is a set of commands used to create and manage azure resources. Available on windows,macOS,linux,docker and azure cloud shell

Azure advisor - scans your azure configuration and recommends changes to optimize deployments,increase security and save money. Analyzes the configuration of the resources present in the azure subscriptions.

Azure advisor focuses mainly on high availability,security,performance and costs.

ARM(azure resource manager) templates - a JSON file that defines the infrastructure and configuration for your project. Templates use declarative syntax and are idempotent which means you can deploy many times and get the same resources and state.

ARM templates are used in IaaS

Azure Resource Manager templates provides a common platform for deploying objects to a cloud infrastructure and for implementing consistency across the
Azure environment.

Azure policies are used to define rules for what can be deployed and how it should be deployed. Whilst this can help in ensuring consistency, Azure policies do not provide the common platform for deploying objects to a cloud infrastructure.

Azure monitor - a service that collects monitoring telemetry from a variety of on-premises and azure sources. Management tools like azure security center,push log data to azure monitor.

Azure monitor aggregates and stores this telemetry in an azure log analytics instance.

Azure service health - notifies you about azure service incidents and planned maintenance so you can take action to mitigate downtime.

Azure security center - a unified infrastructure security management system that strengthens the security posture of your data centers(cloud and on-premises).provides security guidance for compute,data,network,storage,app and other services.

Key vaults - a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to such as API keys,passwords,certificates or cryptographic keys.

Azure sentinel - a cloud native SIEM(security information event management) and security orchestration automated response(SOAR) solution.

Dedicated hosts - a service that provides dedicated physical servers able to host one or more
Virtual machines in one azure subscription.

Defense in depth - a layered approach that doesn't rely on one method to completely protect your environment.

Network security group - contains security rules that allow or deny inbound network traffic to or outbound network traffic from several types of azure resources.For each rule you can specify source and destination,port and protocol.can be applied to a subnet or network adapter(NIC).

Azure firewall - a managed cloud based network security service that protects your azure virtual network resources. It's a fully stateful firewall as a service with built in high availability and unrestricted cloud scalability.

Azure DDoS - standard tier provides enhanced DDoS mitigation features to defend against DDoS attacks. Also includes logging,alerting and telemetry not included in the basic tier by default.

AuthN - is the process of proving that you are who you say you are.(basically identity)

AuthZ - is the act of granting an authenticated party permission to do something.(basically access)

Azure AD(active directory) - is microsoft's cloud-based identity and access management service which helps your employees sign in and access resources in either internal or external resources.

Internal resources such as apps on your corporate network or custom cloud apps.

External resources such as microsoft 365,the azure portal and many SaaS apps.

SSO(Single sign on) - SSO means a user doesn't have to sign into every application they use. The user logs in once and that credential is used for multiple apps. SSO based authentication systems are often called “modern authentication”.

MFA - azure AD MFA works by requiring 2 or more of the following authentication methods: something you know(pin/password),something you have(trusted device), something you are(biometric)

Conditional Access - used by azure AD to bring signals together to make decisions and enforce organizational policies.

Azure RBAC helps you manage who has access to azure resources, what they can do with those and which areas/resources they have access to.built on azure resource manager that provides fine-grained access management of azure resources.

Resource locks - prevents other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

Policy - the definition of the conditions which you want to control/govern

Initiative - collection of azure policy definitions that are grouped together towards a specific goal

Blueprint - a container for composing set of standard,patterns and requirements for implementation of azure cloud services,security and design.blueprint is often used in the same sense as “new environments”.

Tags - a name and a value pair used to logically organize azure resources,resource groups and subscriptions into a logical taxonomy. Tags can be the basis for applying business policies or tracking costs. You can also enforce tagging rules with azure policies.

Security - protecting the data that's entrusted to microsoft by using strong encryption and access controls.

Privacy - privacy is about making meaningful choices for how and why data is collected and used

Compliance - compliance with regulations is critical and microsoft aims to ease this task for azure customers.

Azure compliance documentation - to make it easier to find,compliance documentation is grouped geographically and by industry.

Microsoft privacy statement explains: 1) what data microsoft processes 2) how microsoft processes it 3) for what purpose data is utilized

OST(Online service terms) /Product terms site- contains all terms and conditions for software and online services through microsoft commercial licensing programs.

Data protection addendum(DPA) - defines data processing and security terms for online services including data compliance,disclosure,security,transfer and retention.

Trust center - 4 foundational principles of trust security,privacy,compliance and transparency

Azure sovereign regions - special regions that you might need for compliance or legal purposes. the government ,china,germany. Operated by special trustees.

Cost impact - factors that can affect azure resource costs include types,services,locations,ingres and egress traffic.

Reducing costs - factors that can reduce costs include reserved instances,reserved capacity,hybrid use benefit,spot pricing

Reserved instances - reserve VM in advance and save upto 72% compared to PAYG pricing with 1yr/3yr commitment.

Reserved capacity - achieve significant savings on azure SQL db,azure cosmos db and azure synapse analytics and azure cache for redis. Enables you to more easily manage costs across predictable and variable workloads and helps optimize budget and forecasting

Hybrid use benefit - a licensing benefit that helps you to significantly reduce costs of running your workloads.lets you use your on-premises software assurance enabled windows server and SQL server licenses on azure.

Spot pricing - access unused azure compute capacity at deep discounts upto 90% compared to PAYG.applies to azure VM's only.

Pricing calculator(before you deploy) - interactive calculator that allows you to estimate azure resource costs. Enables you to choose region,instance,tiers etc to match functionality and budget needs.

Azure cost management - a suite of tools provided by microsoft that helps you analyze,manage and optimize the costs of your workloads. Only for resource groups and virtual machines(for 3 months)

Azure SLA(service level agreement) - to provide a clear explanation of availability and sometimes performance of an azure service. Services in public preview don't include an SLA

Private preview is open only to companies or users invited for seeing how the service works i.e evaluation only.

Public preview - open to the public but preview limitations apply.(not available in all azure regions)

General availability(GA) - fully released approved for production use.

Scaling in - removing more servers of the same size

Scaling out - add more servers of the same size

Azure VM scale sets - automatically increase or decrease in response to a demand or a defined schedule.

SQL server stretch database - dynamically stretch warm and cold transactional data from microsoft SQL server to azure.

Azure Geo-redundant storage(GRS) - replicates data to a secondary region automatically,ensuring the data is durable even in the event that the primary region isn't recoverable.

Azure cloud service are grouped into 3 categories

1) Foundational - when GA ,immediately or in 12 months in recommended and alternate regions.
2) Mainstream - when GA immediately or in 12 months in recommended regions may become available in alternate regions based on customer demand
3) Specialized - available in recommended or alternate regions based on customer demand.

An availability zone is physical location with one or more datacenter

A region will generally contain 3 availability zones.

Fault domain - a logical grouping of hardware to avoid a single point of failure within an AZ. group of VM's that share a common power source and network switch.

Update domain - azure may need to apply updates to the underlying hardware and software.update domain ensure your resources do not go offline.

Availability set - a logical grouping that you can use in azure to ensure that the VM's you place in the availability set are different fault/update domains to avoid downtime.

Azure service fabric - Tier-1 container as a service. Distributed systems platform.runs in azure or on-premises. Easy to package,deploy and manage scalable and reliable microservices.

Azure functions - event-driven,serverless compute run code without provisioning or managing servers, executes code, is always stateful

Azure Batch - plans,schedules and executes your batch computer workloads across running 100+ jobs in parallel. Use spot VM's to save money.

Azure notifications hub - pub/sub send push notifications to any platform from any backend

Azure API apps - API gateway quickly build and consumes API's in cloud.

Azure service bus - service bus reliable cloud messaging as a service(MaaS) and simple hybrid integration.

Azure stream analytics - serverless real-time analytics from the cloud to edge.

Azure logic apps - schedule,automate and orchestrate tasks,business processes and workflows. Integration with enterprise SaaS and enterprise apps, runs only in the cloud

Azure API management - hybrid,multi-cloud management platform for API's across all environments.

Azure Queue storage - messaging queue. A data store for queuing and reliability delivering messages between applications.

Azure SignalR service - real-time messaging for applications like push.

Xamarin(microsoft owned) - mobile app framework create powerful and scalable apps

Azure boards - Kanban.deliver value to your users faster using proven agile tools to plan,track and discuss work across your teams.

Azure front door - scalable and secure entry point for fast delivery of your global applications.

Azure traffic manager - operates at the DNS layer to quickly and efficiently direct incoming DNS requests based on the routing method of your choice.

Azure DNS allows you to host your domains on azure.you can create DNS zones and manage your DNS records. Azure DNS does not allow you to purchase domains,only the ability to manage DNS records.

Azure load balancer operates on layer 4(transport)

IOT central connects your IOT devices to cloud

IOT hub enables highly secure and reliable communication between your IOT application and devices it manages.

IOT edge - a fully managed service built on IOT hub which allows data processing and analysis nearest the IOT devices.

An NSG is more targeted and is deployed to particular subnets and/or network interfaces, whereas an Azure Firewall monitors traffic more broadly.

An application should connect to Active directory to retrieve security tokens.

Types of plans: basic(10GB) -> developer(50 GB) ->standard -> professional direct -> premier

95% SLA for single instance virtual machines using Standard HDD-Managed Disks for OS and Data disks.
99.5% SLA for single instance virtual machines using Standard SSD-Managed Disks for OS and Data disks.
99.9% SLA for single instance virtual machines using Premium SSD or Ultra Disk for all OS and Data disks.
99.95% SLA for all virtual machines that have two or more instances in the same Availability Set or Dedicated Host Group.
99.99% SLA for all virtual machines that have two or more instances deployed across two or more Availability Zones in the same region.

An Azure Reserved Virtual Machine Instance (RI) is a virtual machine (VM) on the Microsoft Azure public cloud that has been reserved for dedicated use on a one- or three-year basis. ... Azure RIs are available for all Azure VM types, except for the A-series, A_v2 series and the G-series

Azure DevTest Labs **helps developers and testers quickly create environments in Azure to deploy and test their applications**. Easily provision Windows and Linux machines in Labs using reusable templates and artifacts while minimizing waste and controlling cost.

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. ... P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content.

Identity Protection identifies risks of many types, including:
Anonymous IP address use
Atypical travel
Malware linked IP address
Unfamiliar sign-in properties
Leaked credentials
Password spray

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

A Local Network Gateway is an object in Azure that represents your on-premise VPN device. A Virtual Network Gateway is the VPN object at the Azure end of the
VPN.

To increase azure subscription limits we need to create a new support request

You need an Azure Active Directory account to manage a subscription, not a Microsoft account.

Outbound data transfer is charged at the normal rate and inbound data transfer is free.

Users in the azure active directory are not organized using resource groups.

Only the hot and cool access tiers can be set at the account level. The archive access tier can only be set at the blob level
The Azure File Sync agent enables data on a Windows Server to be synchronized with an Azure File share.

The permissions you apply to the resource group apply to all resources contained in the resource group.

Azure CLI cant execute any powershell scripts

The Log Alert Rule is not a feature of Azure AD

Azure Virtual Machines support Windows and Linux

Application gateway can make load balancing decisions based on the URL path, while a load balancer can't.

Azure arc allows you to manage windows and linux machines running on-premises or other cloud providers as if they were Azure VM’s.