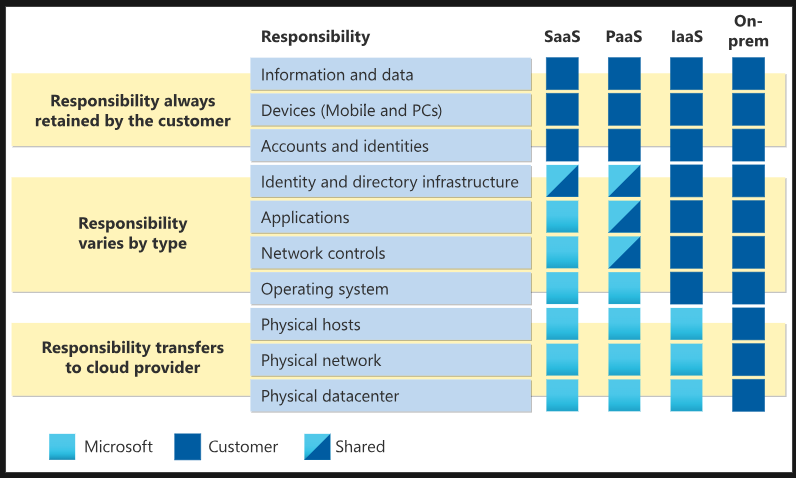
**Cloud**

* Delivery of computing services over the Internet using a pay-as-you-go pricing model.
* A way to rent compute power and storage from someone else’s data center.
* Pay as you go, you are only billed for what you use.
  + Renting CPUs and storage in your data for the time you need.
  + On-demand access, treat cloud resources like you would to your resources in your own data center. Give them back once you are done using.
* The real value of the cloud is **speed.**
  + Enables you to quickly solve your business challenges and bring cutting edge solutions to your users.
  + Fast to create and deploy a website on Azure.
* Foundational building block



**Advantages of Cloud**

* Move faster.
* Two-trends in world:
  + Teams are delivering new features to their users at record speeds:
  + End users expect an increasingly rich and immersive experience with their devices and with software.
  + Provides on-demand access to:
    - A nearly limitless pool of raw compute, storage, and networking components.
    - Speech recognition and other cognitive services that help make your application stand out from the crowd.
    - Analytics services that enable you to make sense of telemetry data coming back from your software and devices.

**Benefits of Cloud Computing**

* Not an all-or-nothing service
  + You can gradually move to cloud, called **lift and shift.**
  + Spend more time on what matters and less time managing the underlying details.
* **Cost Effective**
  + Provides pay-as-you-go or **consumption-based** pricing model.
    - No upfront infrastructure costs.
    - No need to purchase and manage costly infrastructure/hardware that you may not use to its fullest.
    - The ability to pay for additional resources only when they are needed.
    - The ability to stop paying for resources that are no longer needed.
  + Enables better cost predictions using pricing of individual resources/services.
    - You can analyze future growth using historical data.
* **Scalable**
  + Increase or decrease the resources and services used based on the demand or workload at any given time.
  + Cloud Computing supports both:
    - **Horizontal scaling / Scaling out.**
      * Adding more **resources** to increase the power of an existing server.
    - **Vertical Scaling/Scaling up.**
      * Adding resources to increase the power of an existing server.

**Note:** Scaling can be done manually or automatically based on e.g. specific triggers such as CPU utilization.

* **Elastic**
  + Cloud computing system can automatically add & remove resources to meet the current demand.
  + E.g.
    - Add resources for the peak operating hours during which most people access the application.
      * Only pay for increased resources during those hours.
    - Remove the resources when the traffic normalizes.
* **Current**
  + Eliminates the burdens of maintaining software patches, hardware setup, upgrades, and other IT management tasks:
    - Automatically done.
  + The computer hardware is maintained and upgraded by the cloud provider.
    - If disk fails, it’ll be replaced by the cloud provider.
* **Reliable**
  + Cloud provider offers data backup, disaster recovery, and data replication services.
  + Redundancy is often built into cloud services architecture.
    - If one component fails, a backup component takes its place.
    - This is referred to as **fault tolerance** and it ensures that your customers aren’t impacted when a disaster occurs.
* **Global**
  + Fully redundant datacenters located in various regions all over the globe.
  + Enables local presence close to your customers to give them the best response time.
  + Replicate your services into multiple regions for redundancy and locality.
  + Select a specific region to ensure you meet data-residency and compliance laws for your customers.
* **Secure**
  + **Physical Security**
    - Who can access the building, who can operate the server racks, and so on.
    - Walls, cameras, gates, security personnel, employees have access only to those resources that they’ve been authorized to manage.
  + **Digital Security**
    - Who can connect to your systems and data over the network.
    - Only authorized users will be able to log into VM or storage systems running in the cloud.
    - Tools to mitigate security threats that you can use.
  + Broad sets of policies, technologies, controls, and expert technical skills.
    - Can provide better security than most organizations can otherwise achieve.

**Types of Clouds**

* **Public Cloud**
  + Most common deployment models.
  + No local hardware to manage or keep up-to date, everything runs on your cloud provider’s hardware.
  + Save additional costs by sharing computing resources with other cloud users.
  + Can use multiple public cloud providers of varying scale.
  + **Example:**
    - Deploy a blog/web application quickly without worrying about purchasing, managing or maintaining the hardware on which it runs.
  + **Advantages**
    - High scalability/agility: you don’t have to buy a new server in order to scale.
    - Pay-as-you-go pricing: you pay only for what you use, no CapEx costs.

*Capital expenditures (CapEx) are funds used by a company to acquire, upgrade, and maintain physical assets*

* + - You are not responsible for maintenance or updates of the hardware.
    - Minimal technical knowledge to set up and use: you can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.
* **Disadvantages**
  + Specific security requirements that cannot be met by using public cloud.
  + Government policies, industry standards, or legal requirements which public clouds cannot meet.
  + You don’t own the hardware or services and cannot manage them as you may want to.
  + Unique business requirements, such as having to maintain a legacy application might be hard to meet.

**Private cloud**

* Cloud environment in your own datacenter
* Provide self-service access to compute resources to users in your organization.
* A simulation of a public cloud to users, but you remain completely responsible for the purchase and maintenance of the hardware and software services you provide.
* Users can be external customer or specific internal departments such as Accounting or Human Resources.
  + E.g
    - Have data that cannot be put in the public cloud because a government policy requires specific data to be kept in-country or privately.
* **Advantages**
  + Ensure the configuration can support any scenario or legacy application.
  + Control (and responsibly) over security.
  + Meet strict security, compliance, or legal requirements.
* **Disadvantages**
  + Initial CapEx costs & must purchase the hardware for startup and maintenance.
  + Owning the equipment limits the agility – to scale you must buy, install, and setup new hardware.
    - These clouds require IT skills and expertise that’s hard to come by.

**Azure App Service**

* Scalable web hosting platform.

**Azure Functions**

* Create event driven serverless application.

**Container Instances and Kubernetes Services**

* Allows to deploy containerized applications.
* Offers fully relational databases.

**Azure Portal**

* Allows you create, configure and control all your services and resources in an easy-to-use interface.

**Physical Infrastructure**

* **Datacenters**
  + Facilities with resources arranged in racks, with dedicated power, cooling, and networking infrastructure.
  + Grouped into Azure Regions or Azure Availability Zones that are designed to help resiliency and reliability.
* **Regions**
  + A geographical area on the planet that contains at least one, but potentially multiple datacenters that are nearby and networked together with a low-latency network.
* **Availability Zones**
  + Physically separate datacenters within an Azure region.
  + Made up of one or more datacenters.
* **Region Pairs**
  + Azure regions are paired with another region within the same geography at least 300 miles away.
  + Allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect an entire region.
* **Sovereign Regions**
  + Instances of Azure that are isolated from the main instance of Azure.

**Resource**

* Anything that you create, provision, deploy, etc. is a resource. VMs, virtual networks, databases, cognitive services, etc. are all considered resources within Azure.

**Resource Groups**

* Grouping of resources
* A single resource can only be in one resource group.
* Resource groups can’t be nested.
* If you delete a resource group, all the resources will be deleted, same thing with access.

**Azure Subscriptions**

* Unit of management, billing, and scale.
* Allows to logically organize your resource groups and facilitate billing.
* Provides authenticated and authorized access to Azure products and services.

**Azure Management Groups**

* Manage access, policies, and compliance for those subscriptions.
* Provide a level of scope above subscriptions.

*All subscriptions within a management group automatically inherit the conditions applied to the management group, the same way that resource groups inherit settings from subscriptions and resources inherit from resource groups.*

**Azure Virtual Machines (VMs)**

* Provide IaaS in the form of virtualized servers and can be used in many ways.
* Gives flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM.

**Virtual Machine Scale Sets**

* Let’s you create and manage a group of identical, load balanced VMs.
* Allow you to centrally manage, configure, and update a large number of VMs in minutes.

**Virtual Machine Availability Sets**

* Help you build a more resilient, highly available environment.
* Ensures that VMs stagger updates and have varied power and network connectivity, preventing you from all your VMs with a single network or power failure.

*VMs are also an excellent choice when you move from a physical server to the cloud (also* ***lift and shift****)*

**Azure Virtual Desktop**

* Desktop and application virtualization service that runs on the cloud.
* Enables to use a cloud-hosted version of Windows from any location.
* Works across devices and operating systems and works with apps that you use to access remote desktops or most modern browsers.
* Provides centralized security management for user’s desktops with Microsoft Entra ID.

**Containers**

* Virtualized Environment
* Lightweight and designed to be created, scaled out, and stopped dynamically.

**Azure Container Instances**

* Offers the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services.
* PaaS.
* Allow you to upload your containers and then the services will run the containers for you.

**Azure Container Apps**

* Allows you to get up and running right away, they remove the container management piece, and they’re a PaaS offering.
* Ability to incorporate load balancing and scaling.

**Azure Kubernetes Service**

* Container orchestration service. An orchestration service manages the lifecycle of containers.
* Can make fleet management simpler and more efficient when deploying a fleet of **containers.**

**Azure Functions**

* Event-driven, **serverless** compute option that doesn’t require maintaining virtual machines or containers.
* Scale automatically based on demand.
* Runs your code when it’s triggered and automatically deallocates resources when the function is finished.

**Azure App Service**

* Enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure.
* Robust hosting option that you can use to host your apps in Azure.
* HTTP-based service for hosting web applications, REST APIs, and mobile back ends.

**Azure Virtual Networks**

* Supports both public and private endpoint to enable communication between external or internal resources with other internal resources.
  + Public endpoints have a public IP address and can be accessed from anywhere in the world.
  + Private endpoints exist within a virtual network and have a private IP address from within the address space of that virtual network.
* Allow you to create multiple isolated virtual networks.
* Virtual networks can connect not only VMs but other Azure resources.
* Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts.

**//Include the question from the assessment regarding the VPN and expressroute.**

**Peering**

* Allows two virtual networks to connect directly to each other.
* Enables resources in each virtual network to communicate with each other.

**Virtual Private Network**

* Uses an encrypted tunnel within another network.
* Deployed to connect two or more trusted private networks to one another to one another over an untrusted network (typically the public internet).

**VPN Gateways**

* Is a type of virtual network gateway.
* The instances are deployed in a dedicated subnet of the virtual network and enable the following connectivity.
* Use to connect to multiple locations.
* Two types:
  + **Policy-based**
    - Specify statistically the IP address of packets that should be encrypted to each tunnel.
  + **Route-based**
    - Decides which one of these tunnel interfaces to use when sending each packet.
* Deployed as two instances:
  + **Active**
    - Assign a unique public IP address to each instance.
    - Can extend the high availability by deploying an additional VPN device on-premises.
* **ExpressRoute failover**
  + High-availability option for VPN
* **Zone-redundant gateways**
  + Deploying gateways in Azure availability zones physically and logically separates gateways within a region while protecting your on-premises network connectivity to Azure from zone-level failures.

**Azure ExpressRoute**

* Let’s you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider.

**Co-location at a cloud exchange**

* Co-location refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP.

*ExpressRoute doesn’t travel over the public internet. It is a private connection from you on-premises infrastructure to your Azure infrastructure.*

**Azure DNS**

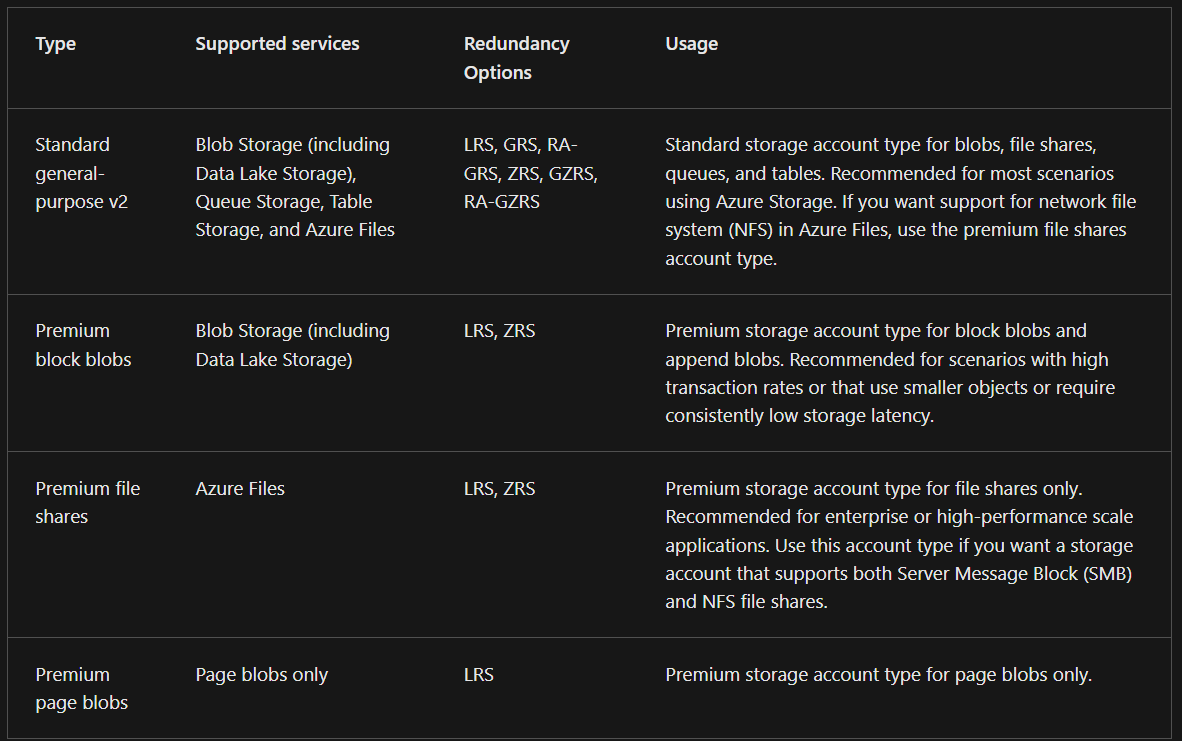
* Hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure.
* Based on Azure Resource Manager
  + Azure role-based access control (Azure RBAC) to control who has access to specific actions for your organization.
  + Activity Logs to monitor how a user in your organization modified a resource or to find an error when troubleshooting.
  + Resource locking to lock a subscription, resource group, or resource. Locking prevents other users in your organization from accidentally deleting or modifying critical resources.

**DNS Domains**

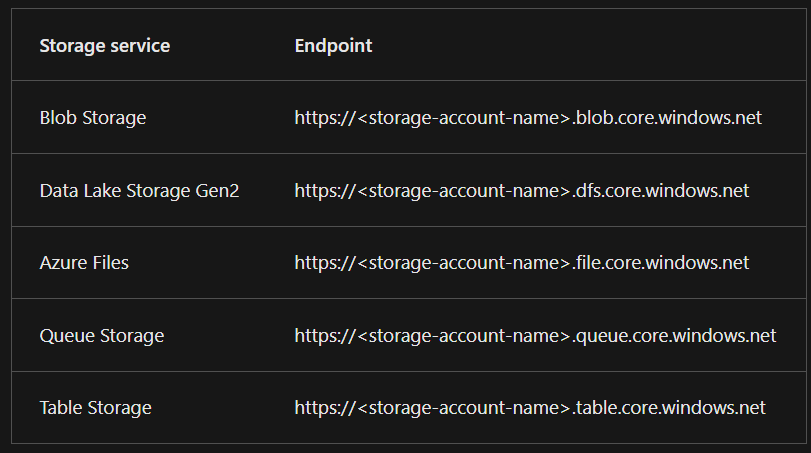
* Provides resiliency and high availability.

**Storage Account**

* Provides a unique namespace for your Azure Storage data that’s accessible from anywhere in the world over HTTP or HTTPS.
* Redundancy Options:
  + Locally redundant storage (LRS)
  + Geo-redundant storage (GRS)
  + Read-access geo-redundant storage (RA-GRS)
  + Zone-redundant storage (ZRS)
  + Geo-zone-redundant storage (GZRS)
  + Read-access geo-zone-redundant storage (RA-GZRS)

****

The following table shows the endpoint format:

****

**Azure Storage**

* Stores multiple copies of your data so that it’s protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters.

**Redundancy**

* Ensures that your storage account meets its availability and durability targets even in the face of failures.

*Data is always replicated* ***three times*** *in the primary region.*

**Locally redundant storage**

* Replicates your data three times within a single data center in the primary region.

**Zone redundant storage**

* Replicates your Azure Storage data synchronously across three Azure availability zones in the primary region.
* data is still accessible for both read and write operations even if a zone becomes unavailable.

**Redundancy in a secondary region**

* You can choose to additionally copy the data in your storage account to a secondary region that is hundred miles away from the primary region.

**Geo-redundant storage**

* Copies your data synchronously three times within a single physical location in the primary region using LRS.

**Geo-zone-redundant storage**

* Copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a secondary geographic region, using LRS, for protection from regional disasters.
* Provides 16 nines of durability

**Azure Blobs**

* A massively scalable object store for text and binary data.
* Unstructured, there are no restrictions on the kinds of data it can hold.

**Azure Files**

* Managed file shares for cloud or on-premises deployments.
* Accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols.

**Azure Queues**

* A messaging store for reliable messaging between application components.

**Azure Disks**

* Block-level storage volumes for Azure VMs.

**Azure Tables**

* NoSQL table option for structured, non-relational data.

**Blob storage tiers**

* **Hot Access Tier**
  + Optimized for storing data that is accessed frequently.
* **Cool Access Tier**
  + Optimized for data that is infrequently accessed and stored for at least 30 days.
* **Cold Access Tier**
  + Optimized for storing data that is infrequently accessed and stored for at least 90 days.
* **Archive Access Tier**
  + Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements.

**Azure Migrate**

* Service that helps you migrate from an on-premises environment to the cloud.
* Helps manage the assessment and migration of your on-premises datacenter to Azure.

**Azure Data Box**

* Physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way.
* Suited to transfer data sizes larger than 40tbs in scenario with no to limited network connectivity.

**AzCopy**

* Is a command-line utility that you can use to copy blobs or files to or from your storage account.
* Help move files back and forth between clouds.

**Azure Storage Explorer**

* Is a standalone app that provides a graphical interfaces to manage files and blobs in your Azure Storage Account.

**Azure File Sync**

* Tool that lets you centralize your files shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server.
* Keeps files between an on-premises Windows server and an Azure cloud environment updated.
* Maintains bidirectional synchronization of files between your on-premises and cloud Windows servers.

**Microsoft Entra ID**

* **Authentication**
  + Verifying identity to access applications and resources.
  + Includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
* **Single sign-on**
  + Enables to remember only one username and one password to access multiple applications.
* **Application management**
  + Manage cloud and on-premises apps by using Microsoft Entra ID.
* **Device management**
  + Support registration of devices which enables devices to be managed through tools like Microsoft Intune.
  + Allows for device-based conditional access policies.
* **Microsoft Entra Connect**
  + Synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems.
* **Microsoft Entra Domain Services**
  + A service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication.

**Authentication**

* Process of establishing the identity of a person, service, or device.

**Single sign-on**

* Enables user to sign in one time and use that credential to access multiple resources and applications from different providers.

**Multifactor authentication**

* Process of prompting a user for an extra form of identification during the sign-in process.
* Provides additional security for your identities by requiring two or more elements to fully authenticate.

**Microsoft Entra multifactor authentication**

* Enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.

**FIDO2 security keys**

* Fast Identity Online (FIDO) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication.
* An unphishable standards-based passwordless authentication method that can come in any form factor.

**Microsoft Entra External ID**

* Refers to all the ways you can securely interact with users outside the organization.
* **Business to business (B2B) collaboration**
  + Collaborate with external users by letting them use their preferred identity to sign-in to Microsoft applications or other enterprise applications.
* **B2B direct connect**
  + Establish a mutual, two-way trust with another Microsoft Entra organization for seamless collaboration.
* **Microsoft Azure Active Directory business to customer (B2C)**
  + Publish modern SaaS apps or custom-developed apps to consumers and customers, while using Azure AD B2C for identity and access management.

**Conditional Access**

* is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals.
* collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

**Role-based access control (RBAC)**

* applied to a scope, which is a resource or set of resources that this access applies to.
* **Scopes include:**
  + A management group (a collection of multiple subscriptions).
  + A single subscription.
  + A resource group.
  + A single resource.

. Resource Manager is a management service that provides a way to organize and secure your cloud resources.

Zero Trust is a security model that assumes the worst case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.

A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

**Pricing Calculator**

* Is designed to give you an estimated cost for provisioning resources in Azure.
* Focus on the cost of provisioned resources in Azure.
* Can estimate the cost of any provisioned resources, including compute, storage, and associated network costs.

**TCO calculator**

* designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure. **The Total Cost of Ownership calculator lets you input your current infrastructure and requirements and provides you with an estimate for running in the cloud.**

Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

 cost analysis, you can quickly view the total cost in a variety of different ways, including by billing cycle, region, resource, and so on.

Cost alerts provide a single location to quickly check on all of the different alert types that may show up in the Cost Management service. The three types of alerts that may show up are:

* Budget alerts notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget.
* Credit alerts notify you when your Azure credit monetary commitments are consumed.
* Department spending quota alerts notify you when department spending reaches a fixed threshold of the quota.

**Microsoft Purview**

* A family of data governance, risk, and compliance solutions that helps you get a single, unified view into your data.
* Brings insight about your on-premises, multicloud, and SaaS data together.

**Azure Policy**

* A service in Azure that enables you to create, assign, and manage policies hat control or audit your resources.
* Enables you to define both individual policies and groups of related policies, known as initiatives.
* Evaluates your resources and highlights resources that aren’t compliant with policies you’ve created.
* Prevent noncompliant resources from being created.
* Set each level, enabling to set policies specifically for the resource, resource group, and subscription.
* Can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources.

**Resource locks**

* Prevent resources from being deleted or updated, depending on the type of lock.
* Can be applied to individual resource, resource groups, or even an entire subscription.
* Inherited
* Types:
  + **Delete –** they can modify but can’t delete.
  + **ReadOnly –** can read but can’t delete or update.

**Microsoft Service Trust Portal**

* Is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.
* Contains details about Microsoft’s implementation of controls and processes that protect our cloud services and the customer data therein.

**Azure Portal**

* Web-based, unified console that provides an alternative to command-line tools.
* UI to build, manage, and monitor everything from simple web apps to complex cloud deployments.
* Custom dashboards
* Designed for resiliency and continuous availability.

**Azure Cloud Shell**

* Browser-based shell tool that allow you to create, configure, and manage Azure datacenter.
* Supports both Azure PowerShell and the CLI, which is Bash Shell.

**Azure PowerShell**

* Shell with which developers, DevOps, and IT professionals can run commands called command-lets (cmdlets).

**Azure CLI**

* Functionally equivalent to Azure PowerShell, with the primary difference being the syntax of commands.
* Provides the same benefits of handling discrete tasks or orchestrating complex operations through code.

**Azure Resource Manger**

* Deployment and management service for Azure.
* Provides a management layer that enables you to create, update, and delete resources in your Azure account.
* Lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations.

**Azure Arc**

* Simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.
* Helps you manage Azure, on-premises, and multicloud environments.
* Extends your Azure compliance and monitoring to hybrid and multicloud configurations.

**ARM templates**

* Can describe the resources you want to use in a declarative JSON format.

**Bicep**

* Language that uses declarative syntax to deploy Azure resources.

**Azure Advisor**

* Evaluates your Azure resources and makes recommendation to help improve reliability, security, and performance, achieve operational excellence, and reduce costs.
* Designed to help you save time on cloud optimization.
* Displays personalized recommendations for all your subscriptions.

Azure Service Health helps you keep track of Azure resource, both your specifically deployed resources and the overall status of Azure.

Azure Monitor is a platform for collecting data on your resources, analyzing that data, visualizing the information, and even acting on the results. Azure Monitor can monitor Azure resources, your on-premises resources, and even multi-cloud resources like virtual machines hosted with a different cloud provider.

Azure Log Analytics is the tool in the Azure portal where you’ll write and run log queries on the data gathered by Azure Monitor. Log Analytics is a robust tool that supports both simple, complex queries, and data analysis.

Azure Monitor Alerts are an automated way to stay informed when Azure Monitor detects a threshold being crossed.

Application Insights is capable of monitoring applications that are running in Azure, on-premises, or in a different cloud environment.

**The five recommendation categories for Azure Advisor are: Reliability, Security, Performance, Operational Excellence, and Cost.**

**Cloud Computing**

* Practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

**4 IaaS common types**

* **Compute**
  + Virtual computer that can run application, programs, and code.
* **Storage**
  + Virtual hard drive.
* **Networking**
  + Virtual network being able to define internet connections or network isolations.
* **Databases**
  + Virtual database for storing reporting data or a database for general purpose web-application.

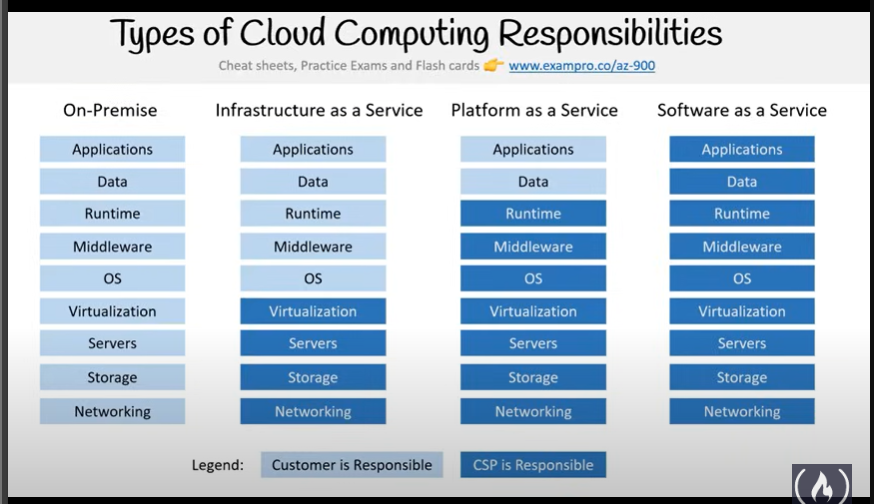
**Benefits of Cloud Computing**

* **Cost-effective**
  + You pay for what you consume.
* **Global**
  + Launch workloads anywhere in the world, just choose a region.
* **Secure**
  + Cloud provider takes care of physical security. Cloud services can be secure by default, or you can configure access down to granular level.
* **Reliable**
  + Data backup, disaster recovery, and data replication, and fault tolerance.
* **Scalable**
  + Increase or decrease resources and services based on demand.
* **Elastic**
  + Automate scaling during spikes and drop in demand.
* **Current**
  + The underlying hardware and managed software are patched, upgraded and replaced by the cloud provider without interruption to you.

**Types of Cloud Computing**

* **Software as a Service (SaaS)**
  + Product that is run and managed by the service provider.
  + *For customers*
  + E.g., salesforce, Gmail, microsoft365
* **Platform as a Service (PaaS)**
  + Focus on the deployment and management of your apps.
  + *For Developers*
  + E.g., Heroku, Google API
* **Infrastructure as a Service**
  + Basic building blocks for cloud IT. Provides access to networking features, computers and data storage space.
  + *For Admins*
  + E.g., Microsoft Azure, AWS, Oracle Cloud

**Types of Cloud Computing Responsibilities**

****

**Azure Deployment Models**

* **Public Cloud**
  + Everything built on the Cloud Provider
  + Cloud-Native
* **Private Cloud**
  + Everything built on company’s datacenter.
  + On-premises
* **Hybrid**
  + Using both On-Premises and a cloud service provider.

**Cloud Computing**

* is a model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
* Delivery of computing services over the internet

**Benefits of Cloud Computing**

* Cloud is cost-effective, global, secure, scalable, elastic, and always current.

**Public Cloud**

* Everything runs on your cloud provider’s hardware.
* Advantages: scalability, agility, PAYG, no maintenance, and low skills required.

**Private Cloud**

* Cloud environment in your own datacenter
* Advantages: legacy support, control, compliance
* Use when you need more control.

**Hybrid Cloud**

* Combines public and private clouds, allowing you to run your apps in the right location.
* Advantages: Flexibility in legacy, compliance, and scalability scenarios.

**Economies of Scale**

* 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 up front.

**Operational Expenditure (OpEx)**

* Spending money on services or products now and being billed as you go.
* Associated with **Public Cloud** PAYG.

*The cloud increases OpEx spending and reduces CapEx spending.*

**Consumption-based Model**

* Pay for what you use.

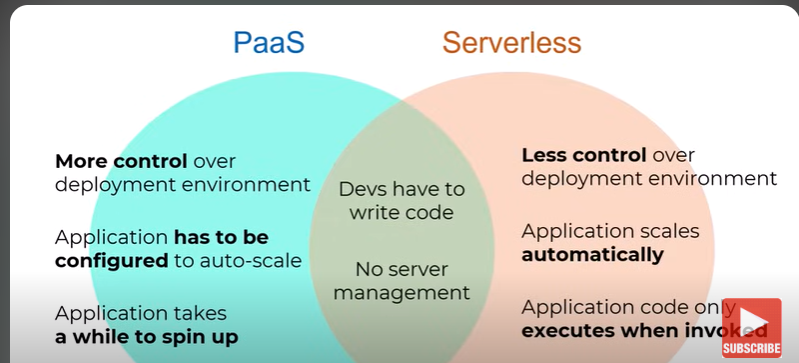
**Fixed Price Model**

* Pay for instances whether you use them or not.
* Ensures predictable costs for cloud services.

**Serverless Architecture**

* Cloud computing execution model where the cloud provider dynamically manages the allocation and provisioning of servers.
* PAYG
* Resources are stateless, servers ephemeral and often capable of being triggered.

**PaaS vs Serverless**

****

**Words associated by serverless**

* **Logic App**
* **Functions**
* **Event Grid**

**Logic App**

* Cloud service that helps you schedule, automate, and orchestrate tasks, business processes, and workflows.

**Functions**

* Event driven, compute-on-demand experience that extends the existing Azure application platform.
* 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.
* It will push events to the configured destination.
* Utilize the push model instead of the inefficient pull across their Serverless architecture.

**Availability**

* Encompasses availability of the infrastructure, applications, and services.

***Uptime*** *measures the amount of time a system is running.*

**Scalability**

* The ability of a system to handle growth of users or work.
* Ability of a system to handle more traffic.

**Elasticity**

* Ability of a system to automatically grow and shrink based on **app demand.**
* Focuses on the ability of a system or service to scale quickly to spikes in demand.

**Agility**

* Focuses on the speed and ease of allocating and deallocating resources.

**Fault Tolerance**

* Ability of a system to handle faults in a service like power, network, or hardware failures.
* Component-level failures.

**High Availability**

* Ability to keep services up and running for long period of time.
* Service level failures.

**Disaster Recovery**

* Ability to recover from an event which has taken down a cloud service.

**Reliability**

* Ability of a system to recover from failures and continue to function.
* Resiliency and availability.
* **Resiliency:** aims to return an application to a fully functioning state after a failure occurs.
* **Availability:** to provide consistent access to your application.

**Predictability**

* Enables solutions with predictable cost and performance.
* *Level of service and performance and the associated cost are known in advance.*

**Security**

* Protection of customer data (access control, encryption)
* Protection of cloud applications
* Protection of cloud infrastructure.

*IaaS gives the customer more control versus PaaS and SaaS, but also places more security responsibility on the customer.*

**Azure DDoS**

* Standard tier provides enhanced DDoS mitigation features to defend against DDoS attacks.
* Includes logging, alerting, and telemetry not included in the free Basic tier present by default.

**Governance**

* Set of rules and policies that guide an organization’s cloud operations.
* To ensure data security, manage risk, control costs, and improve efficiency.

*The guidance and guardrails that ensure we’re as secure, consistent, and efficient as possible.*

* Deployment templates ensure deployed resources meet corporate standards and regulatory requirements.

**Cloud Adoption Framework**

* Guidance designed to help you create and implement the business and technology strategies to succeed in Azure.

*Includes government framework based on “Five disciples of cloud governance.*

**Manageability**

* Automatically scale resource deployment based on need.
* Monitor the health of resources and automatically replace failing resources.
* Speaks to how you’re able to manage your cloud environment and resources:
  + Through a web portal
  + Using APIs
  + Using PowerShell

**Azure Geography**

* Discrete market, typically containing two or more regions, that preserves data residency and compliance boundaries.

**Azure Regions**

* Set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

**Azure Sovereign Regions**

* Special regions that you might need to for compliance or legal purposes:

**Region Pairs**

* A relationship between 2 Azure Regions within the same geographic region for disaster recovery purposes.
* **300+ miles**

**Management Groups**

* Provide a level of scope above subscription.
* Each directory is given a single top-level management group called the “Root”

**General Data Protection Regulation**

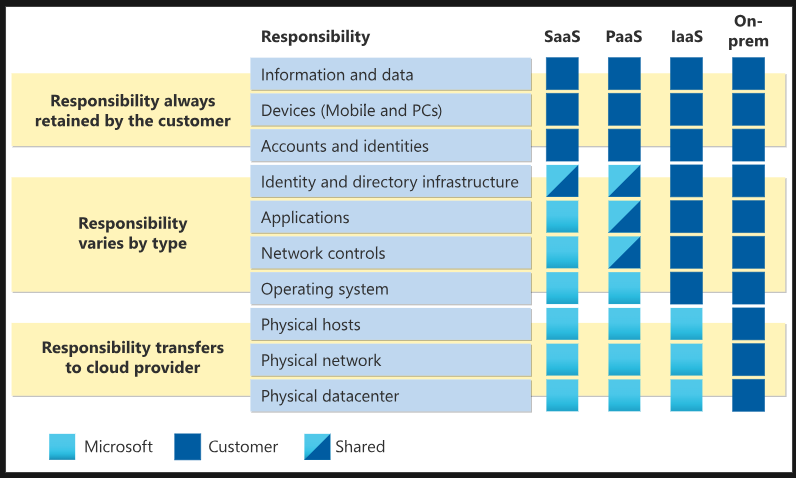
* Defines data protection and privacy rules.
* Defines how the data that a company or organization collects from its customers.

**The public cloud is a shared entity whereby multiple corporations each use a portion of the resources in the cloud.**

Azure reservations serve as a discount mechanism when we want to save some costs for running our virtual machines in Azure. Reserving a VM can save up to 72% of the pay-as-you-go price that one incurs for running a VM 24/7 and 365 days.

**Cloud Computing**

* Delivery of computing services over the internet.

****

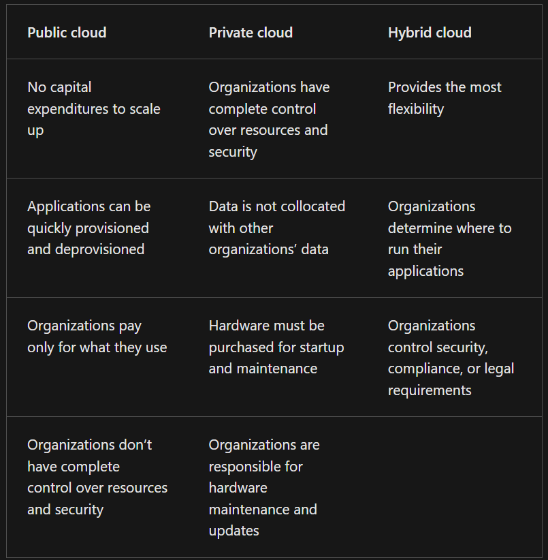
**Private Cloud**

* Provides much greater control for the company and its IT department.

**Public Cloud**

* Built, controlled, and maintained by a third-party cloud provider.
* Anyone that wants to purchase cloud services can access and use resources.
* General public availability

**Hybrid Cloud**

* Computing environment that uses both public and private clouds in an inter-connected environment.
* Can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources.
* ****Can be used to provide extra layer of security.

**Multi-cloud**

* Use multiple cloud providers.
* Example, you started your cloud journey with one provider and are in the process of migrating to a different provider.
* Deals with two or more public cloud providers and manage resources and security in both environments.

**Azure Arc**

* Set of technologies that helps manage your cloud environment.
* Implement consistent inventory, management, governance, and security for servers across your environment.

**Azure VMware Solution**

* Lets you run your VMware workloads in Azure with seamless integration and scalability.

**Capital Expenditure (CapEx)**

* Typically, a one-time, up-front expenditure to purchase or secure tangible resources.
* New building, repaving the parking lot, building a datacenter, or buying a company vehicle are example of CapEx.

**Operational Expenditure (OpEx)**

* Spending money on services or products over time.
* Renting a convention center, leasing a company vehicle, or signing up for cloud services.
* Cloud computing, operates in a consumption-based model. You pay for the IT resources you use.
* Benefits:
  + No up front costs.
  + No need to purchase and manage costly infrastructure that users might not use to its fullest potential.
  + The ability to pay for more resources when they’re needed.
  + The ability to stop paying for resources that are no longer needed.

**Cloud Computing**

* Delivery of computing services over the internet by using Pay as you go pricing model.
* A way to rent compute power and storage from someone else’s datacenter.

**High Availability**

* Focuses on ensuring maximum availability, regardless of disruptions or events that may occur.

**Scalability**

* Ability to adjust resources to meet demand. The ability to scale means you can add more resources to better handle the increased demand.

**Vertical Scaling**

* Focused on increasing or decreasing the capabilities of resources.
* Scale up to add more CPUs or RAM to the virtual machine.
* Ofc, you could also scale down.

**Horizontal Scaling**

* Adding or subtracting the numbers of resources.
* Adding virtual machine.
* Scaled out (either automatically or manually) deployed resources.

**Reliability**

* Ability of a system to recover from failures and continue to function.

**Predictability**

* Can be focused on performance predictability or cost predictability.

**Performance**

* Focuses on predicting the resources needed to deliver a positive experience for you customers.
* Autoscaling, load balancing, and high availability support performance predictability.

**Cost**

* Focused on predicting or forecasting the cost of the cloud spend.

**Cloud-based auditing**

* Helps flag any resource that’s out of compliance with the corporate standards and provides mitigation strategies.

*If you want maximum control of security the IaaS it is. It provides you with physical resources but lets you manage the operating systems and installed software, including patches and maintenance.*

*If you want patches and maintenance taken care of automatically then PaaS and SaaS it is.*

**Management of Cloud**

* Automatically scale resource deployment based on need.
* Deploy resources based on preconfigured template, removing the need for manual configuration.
* Monitor the health of resources and automatically replace failing resources.
* Receive automatic alerts based on configured metrics, so you’re aware of performance in real time.

**Management in the Cloud**

* You can manage these:
  + Through a web portal.
  + Using a command line interface.
  + Using APIs.
  + Using Powershell.

**Infrastructure as a Service**

* It provides you the maximum amount of control for your cloud resources.
* Cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical security.
* Essentially renting the hardware in a cloud datacenter.

**Scenarios**

* **Lift-and-shift migration:** You’re standing up cloud resources similar to you on-premise datacenter, and then simply moving the things running on-premise to running on the IaaS infrastructure.
* **Testing and development:** Established configurations for development and test environments that you need to rapidly replicate.

**Platform as a Service**

* Middle ground between renting space in a datacenter (IaaS) and paying for a complete and deployed solution (SaaS)
* Is a well suited to provide a complete development environment without the headache of maintaining all the development infrastructure.

**Scenarios**

* **Development Framework:** 
  + PaaS provides a framework that developer can build upon to develop or customize cloud-based applications.
  + Let’s developers create applications using built-in software components.
* **Analytics or business intelligence:**
  + Tools provided as a service with PaaS allow organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.

**Software as a Service**

* Essentially renting or using a fully developed application, and connectivity software.
* Least flexible, easiest to get up and running.
* Requires least amount of technical knowledge or expertise to fully employ.
* Most responsibility is with the cloud provider.
* Customer is only responsible for the data and access.

**Scenarios**

* Email and messaging.
* Business productivity applications.
* Finance and expense tracking

**Hybrid Cloud Bursting**

* Expanding to the public cloud when local resources are insufficient.