# Describe cloud concepts (25–30%)

## Describe cloud computing

* define cloud computing
* describe the shared responsibility model
* define cloud models, including public, private, and hybrid
* identify appropriate use cases for each cloud model
* describe the consumption-based model
* compare cloud pricing models

## Describe the benefits of using cloud services

* describe the benefits of high availability and scalability in the cloud
* describe the benefits of reliability and predictability in the cloud
* describe the benefits of security and governance in the cloud
* describe the benefits of manageability in the cloud

## Describe cloud service types

* describe infrastructure as a service (IaaS)
* describe platform as a service (PaaS)
* describe software as a service (SaaS)
* identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)

# Describe Azure architecture and services (35–40%)

## Describe the core architectural components of Azure

* describe Azure regional, regional pairs, and sovereign regions
* describe availability zones
* describe Azure datacenters
* describe Azure resources and resource groups
* describe subscriptions
* describe management groups
* describe the hierarchy of resource groups, subscriptions, and management groups

## Describe Azure compute and networking services

* compare compute types, including container instances, virtual machines (VMs), and functions
* describe VM options, including Azure Virtual Machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop
* describe resources required for virtual machines
* describe application hosting options, including the Web Apps feature of Azure App Service, containers, and virtual machines
* describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and Azure ExpressRoute
* define public and private endpoints

## Describe Azure storage services

* compare Azure storage services
* describe storage tiers
* describe redundancy options
* describe storage account options and storage types
* identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync
* describe migration options, including Azure Migrate and Azure Data Box

Blob Storage, Disk, File and Storage tiers

VM or function anything requires storage

Azure storage account – General purpose v2, blob (containers), tables, queues, files

Azure data lake – huge data storage. Hierarchical namespace and cannot create after provisioning.

On demand storage – cheap. Pay per GB

Storage account is the cheapest

Blob – binary data. Just a file stored in storage account or data in database

Tiers –

Hot – Frequently accessed pay per GB and accessing fees,

cool – (infrequent, pay more for access, backup scenario) and

archive Tier - Backups

Performance tiers –

Standard,

premium(low latency, ssd, block bobs – high transaction low starage latency,, fileshares, page blobs – random read writes)

Location, region (affects cost in storage account)

Redundancy / replication – (in premimun no geo redundant GRS, Premium - local redundant storage LRS (Basic protection, server rack and drive failure. Non critical scenario) and Zone redundant storage ZRS – protection against DC level failure. Highly available, 3 copies in region)

Standard Redundancy – LRS, GRS – 3 copies in 1 DC, 3 copies in another region, ZRS and Geo ZRS –

GRS – Failover in secondary region. Backup scenario

Geo ZRS – GRS + ZRS

Failover options

Azure VM Disks

Managed Disks – used as vhds, in unmanaged its pay per gb, in managed disks its reserved capacity. Managed are optimized.

Unmanaged Storage – Storage Account,

Containers like s3 buckets

To access the items in storage – you need account keys and SAS shared access signatures.

Storage Life Cycle Management – Automated way of moving storage items between tiers Used for General purpose v2 and blob storage accounts.

Access strorage account - Storage explorer and Storage browser.

Explorer – for windows there is app

Storage browser – new way

## Describe Azure identity, access, and security

* describe directory services in Azure, including Azure Active Directory (Azure AD) and Azure Active Directory Domain Services (Azure AD DS)
* describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication, and passwordless
* describe external identities and guest access in Azure
* describe Azure AD Conditional Access
* describe Azure role-based access control (RBAC)
* describe the concept of Zero Trust
* describe the purpose of the defense in depth model
* Describe the purpose of Microsoft Defender for Cloud

Identity – person, app or device in digital world

Azure AD – Identity as a Service

Benefits of A AD – Security, reduced dev time, easier support

Features – Access reviews, central administration, Single Sign on, Integration with other services,

Authentication vs Authorization –

Auth – proving who you are – userid and pwd

Authorize – what is permitted.

AZ Conditional Access – Signal , Decision and Enforcement

MFa - SMS ,email ,authenticator, phonecall

Passwordless - Pin, or biometric recognition, with windows devices

RBAC – Define role and assign users to role

Reader – Read only

Contributor – Standard read/write permission. Full access to read and write

Owner – Read/write + full control

**Zero Trust**

Locking all doors (Cabinets, rooms, lockers – needs keys for everything)

Don’t assume everything behind firewall is safe

Verify explicitly | Use least privileged access | Assume breach

Verify explicitly – use every method to validate identiy and authorization

Just in time – JIT

Just enough access - JEA

Ensure device compliance and health

Monitor user actions

Monitor attacks, behavior

Encrypt all

**Defense in Depth**

Security applied in all layers

Physical – Door locks and key card

Identiy and access – Azure AD

Perimeter – DDOS, firewalls

Netowrk – NSG, subnets, implicit deny

Compute- limit RDP, update

Application – API Management

Data – Virtual Network Endpoint

**MS Defender for Cloud**

Paid product

Security products for azure services

Per transation, per core, per vm etc..

Analysis of security, recommendations, security score,Compliance standards, Firewall manager, inventory. Data level protection using information manager.

# Describe Azure management and governance (30–35%)

## Describe cost management in Azure

* describe factors that can affect costs in Azure
* compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator
* describe the Azure Cost Management and Billing tool
* describe the purpose of tags

Different services are billed based on different factors

Free Services – resource groups, virtual network – 50, load balancers, Azure AD basic, NSG, Free tier we apps upto 10

Pay per Usage – Consumption model

Azure Functions – 1 million free / month

Functions, Logic Apps, storage pay per gb, out bandwidth, api call

Pay per time (Second, hour, month, year)

VM – per second billing

Reserved instance – 1 year or 3 year commitment discounts

Pay per bandwidth – first 5 GB free. Inbound data is free

**Pricing Calculator**

Differs from Region, tier, subscriptiontype, support options, licenses

**Total Cost of Ownership**

Foocus on other cost other than hardware

Electricity, cooling, internet, rack space, setup labor, maintenancelabor, backup

**Cost management**

Tool to analyze spending for azure over time

Tracking against bugets

Automate to stop apps from overscaling etc..

View past invoices and billing

Email report scheduling

Transactions, payment methods

**Resource tags**

Add metadata to resources for personal use

Billing and support – Generate report based on tags

## Describe features and tools in Azure for governance and compliance

* describe the purpose of Azure Blueprints
* describe the purpose of Azure Policy
* describe the purpose of resource locks
* describe the purpose of the Service Trust Portal

Compliance - Daily backup enabled, make policy

Tools to enforce the rules – or audit compliance

Tools – Azure Blueprints, Azure Policy, Resource Locks and Service Trust Portal

Blue prints – Azure subscription templates + roles and Policies already defined

Security roles, resource groups and policies

Useful with multiple subscriptions

Azure Policy – Can create rules across all the azure resources.

\*Programatically define rules

\*Regular basis – compliance is checked

\*Policies – Require sql server version, allowed storage accounts, allowed locations, allowed VM types, apply tags and check, not allowed resource types.

\*Create policy using JSON definition

Resource Locks – Mark a resource **readonly** (Cant be stopped, modify, delete)

**Cannotdelete** – can stop/start but cannot delete

Use RBAC

Service trust portal – Central location for documents for compliances

## Describe features and tools for managing and deploying Azure resources

* describe the Azure portal
* describe Azure Cloud Shell, including Azure CLI and Azure PowerShell
* describe the purpose of Azure Arc
* describe Azure Resource Manager and Azure Resource Manager templates (ARM templates)

5 - Azure CLI, powershell, portal, azure cloud shell, azure mobile app

Azure Portal – web based app.

Powershell and CLI – scripting. Operate on resources.

Scripting file is usually created

**Azure ARC - montior**

Manage your infra in all you environments, on premise, other clouds like aws, azure edge, etc…

Consolidated place to see all your environment.

VMs, SQL Servers, Kubernetes clusters,, Azure stack, Vmware vCenters.

Azure HCI – Edge computing

**Azure ARM Templates – Azure Resource manager**

Runs below Azure management service

Middle layer that connects portal, shell cli, rest, sdks to the services

ARM template - used to create resources

There is library – Resource is created and stored in RG (Template speck)

## Describe monitoring tools in Azure

* describe the purpose of Azure Advisor
* describe Azure Service Health
* describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application

Insights

**Azure Advisor –**

Analyzes resources and makes recommendations based on patterns

Cost saving recommendations

Performance recommendations

Security recommendations

Scaling recommendations

**Azure Service Health**

How azure environment is running

Setup alerts if any problems in regions or AZs etc..  
look historical events and issues and news

**Diagnostic Logs**  
Metrics and Logs

**Azure Monitor**Monitor all azure resources in 1 location  
Logs – Run various queries – uses KQL query language  
WorkBooks – Build custom reports

Chaos Studio – Simulate various failures in Azure

Global Reach –

Service Types – IaaS PaaS SaaS

CanNotDelete means authorized users can still read and modify a resource, but they can’t delete the resource.

– ReadOnly means authorized users can read a resource, but they can’t delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

cannot-delete lock on a resource group prevents Azure Resource Manager from automatically deleting deployments in the history. If you reach 800 deployments in the history, your deployments will fail.

ReadOnly lock on a SQL Database prevents you from deleting or modifying the database. It doesn’t prevent you from creating, updating, or deleting data in the database. Resource Manager locks apply only to operations that happen in the management plane, which consists of operations sent to <https://management.azure.com>

by default, a locked resource group cannot be directly deleted even by an administrator. The lock must be removed first before the resource group can be successfully deleted.

You can pay for the computing VM capacity by the second,

Graphical user interface, application

Description automatically generated

VPN Gateway

**send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. between Azure virtual networks over the Microsoft network.**

Each virtual network can have only one VPN gateway.

Azure Application Gateway

is a web traffic load balancer  
 Layer 7 intelligent routing. URL Path based routing. Host Header based routing

Azure Virtual Network (VNet)

Same like traditional network.  
 Scale, Availability, Isolation

Azure Virtual Network (VNet) – It is a logical isolation of the Azure cloud dedicated to your subscription.

Azure Network Security Group – Filter network traffic to and from Azure resources in an Azure virtual network.

Azure Application Gateway – Distribute traffic to your web applications.

Azure VPN gateway – Connect your on-premises network to Azure virtual network.

Azure Blob – Object store for text and binary data.

Azure Disks – Block-level storage volumes.

Azure Table – Structured NoSQL data in the cloud.

Azure Files – Shard access that utilizes Server Message Block (SMB) protocol.

Azure Monitor helps you maximize the availability and performance of your applications and services

Collects, analyze and act on telemetry. Cloud and onprem.

Azure Traffic Manager – DNS Based Load Balancer

Public Load Balancer – Outbound connections for VM inside your Vnet. LBs internet traffic to VMs

Azure Network Interface – Enables and Azure VM to communicate with Internet., azure and on prem.

Private Load Balancer – Used where private Ips are needed at the front end only. LBs traffic inside a Vnet. LB can be accessed from an on premise network in hybrid scenario.

Microsoft Sentinel – Scalable, cloud native, SIEM, SOAR. Alert detection, threat visibility, proactive hunting and threat response

Azure Sphere – Secure, high level app platform. IOT  
Azure cyclecloud – Secure and flexible cloud HPC and Big Compute env to end users. Dynamic cluster scaling.  
Microsoft defender for cloud – infra security mgmt.

VM States – Starting, Running, Stopped, Deleted

VM Scale Set - Group of load balanced vms that automatically scalesWebsite, timeline

Description automatically generated with medium confidence

Timeline

Description automatically generatedGraphical user interface, application

Description automatically generated

Management groups can be nested

Resource groups cannot be nested

CMK an platform keys – encrypted at rest

Import/Export jobs – import from on prem to azure

Export – from azure storage

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedDiagram

Description automatically generatedGraphical user interface, diagram

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, application

Description automatically generated

Fault domains – hardware rack withing datacenter, independent of other rack and cooling. Table

Description automatically generated

Update domain – like patching groups (Cluster patching, one by one) Diagram

Description automatically generated with low confidenceGraphical user interface, text, application, email, website

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

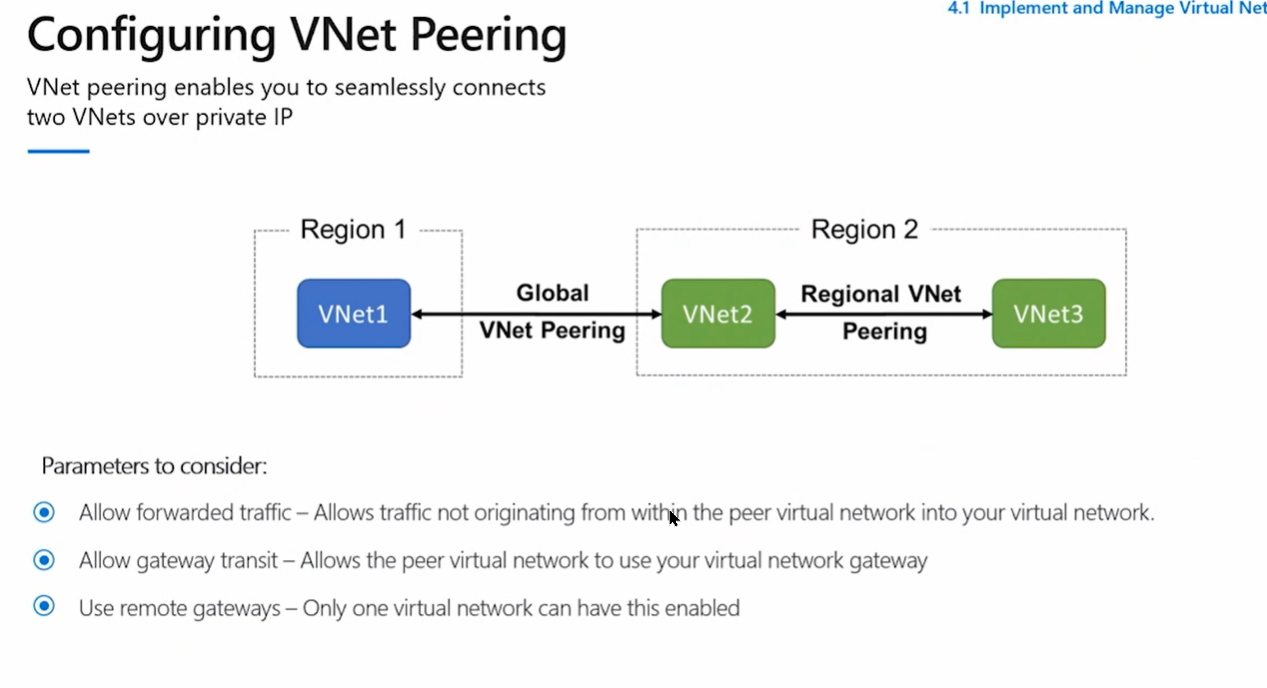
Description automatically generated

Vnet Peering – needs DNS to be set for name resolution.

Resource group moving – some resources cannot be moved like express route. Moving locks resources while moving.

Vnet – Vm to VM, Internet, On prem

Graphical user interface, text, application, Teams

Description automatically generatedGraphical user interface, text, application, Teams

Description automatically generated

AZ 900 Exam Cram Notes

Regions – Multiple physical locations. Multiple buildings close together in a physical location.

Sovereignty requirements can be met with regions

Azure China cloud, Azure Cloud, Azure German cloud, Azure US Government

China – operated by a Chinese company 21vianet. Own region

US gov – has its own region.

There are pairings in Azure for regions. Used for DR requirements

Multiple buildings have independent Cooling, power etc.. – These are called Availability Zones

ZRS Some services are zone redundant – Automatically spans across AZ

Zonal – Created in specific AZ

VMS cannot be zone redundant by default – you can put it in different AZ

Availability sets – separate clusers of resources like server racks within the same DC segregated.

AZ – Separate DC in same region.

Region – Geographical area with N+1 Datacenters.

Azure AD – Identity provider.

Authorization – RBAC

Conditional Access – Need Requirements. Users and Groups and also Cloud Applications that supports Azure AD.

Azure AD Connect – SSO Seamless sign on.

|  |  |  |
| --- | --- | --- |
| RBAC | Policy | Budget |
| Who can do what | What can be done  Intiatives – Group of policies and scope it.  Can be used to get compliance reports.  Audit mode | How much |

Azure -> AAD tenant -> Root -> Management Groups (Inheritance top to bottom)

RBAC, policy and budget can be set to management group.

Management Group - > Structure and control governance features

Under Management Group is Subscription -> Isolation, Base unit of azure interaction, Billing Model, Billing boundary.

RBAC policy and budget can be applied to subscriptions as well.

Resources gets created in resource group – in a subscription

Resource groups cannot be nested

RBAC, Policy and Budget can be applied to Resource groups

Resource groups resources can be interconnected.

Resource groups – Has common lifecycle. Created, run and deleted together (Grouping)

Azure Resource Manager – ARM (How we talk to azure)

Azure is made up of resources defined in resource providers

Talk with azure

1. Portal – Not good for privisoning resources in large or efficient way
2. Cloud shell – Powershell + Bash
3. Mobile App – IOS android
4. Powershell AZ cli module – Windows linux macos

Cmd – az vm list

1. ARM JSON template – every metadata is in JSON (Good for provisioning) (parallel provisioning)

Declarative configuration (Desired End State)

1. Azure Bicep – Converts into ARM JSON Template.

**Governance**Resource Locks – Subscription, Resource, Resource groups

CanNotDelete –

ReadOnly –

Tags – Metadata. Tags do not inherit by default. KEY:Value

BluePrint – Contains artefacts. Resource groups, arm templates, rbac and policy (Assign to subscription)

Blueprint – quick creation of governed subscriptions. Create and design environments with best practices.

Lock Assignment – Control plane applied

Don’t Lock – No lock

Do Not Delete – Can change but cant delete

Read Only – Read only

Cloud Adoption Framework – things to get started with best practices

Types of Resources –

In cloud there are different SKUs – Stock Keeping Unit. Different resources with different computes and power.

**VM Scale set** – Pick some Template, config and Scale policy. (Schedule, trigger based scaling)

If no need to have multitenant (Same Host is shared) then use Azure Dedicated Host

**Azure Dedicated Host** – Buy host fully for yourself. **Pay per Hour**

**Fault domain** - Racks

**Azure Batchs** – Large scale parallel workloads

**ACI** – Azure Container Instances, Isolated.

ACI can have public endpoints, Vnet etc…

**AKS** – Azure Kubernetes Service – Management Plane/Control Plane

**PaaS –** Focus on Code

App Service – Web App, API, Mobile Apps

**Serverless –** Pay for work it does. Event Driven

Azure functions – Just give code and pay for the work it does

Azure Logic Apps – No or low code. Graphical Workflow, connectors using designer.

**Azure Virtual Desktop** – Host virtual desktop solution  
Azure Key Vault – Store Secret, Keys, Certificates

Can be done using Access Policy (Vault level)

Can be done using RBAC (Individual level)

Virtual Network –

Exists withing a Region and within a subscription.

Within virtual network we can have virtual subnets.

Subnets spans across the Availability zones

For every subnet we create we lose 5 IPs – first, last, 1 gateway, 2 dns,

Peering – Connecting different regions

On Premise – VPN Gateway device on Azure and On Prems (Site to Site VPN)

Policy based vpn – one connection, static route, legacy

Route based vpn – N number of connections, point to site vpn, multiple tunnels

Microsoft back bone network

Private connection using Express route

Express route – Not over the internet but a **private connection** like colocation, mpls, cable drop

Control the flow of network using **NSG ,** source, destination, service tag, IP, port, protocol, and other rules. (allow /deny)

NSG linked to subnets

NSG is layer 4

Azure Firewall – Network rules, application rules, **Layer 7,**

Azure firewall – Premium has more

Service endpoint and Private endpoint

DDos – Default azure provides. But there is Basic and Standard

DDOS Basic – Provides only Active traffic monitoring and always on detections and Automatic attack mitigations

DDOS Standard – Provideds Metrics,Availability, reports, support etc..

Storage – Basic building block is Storage account.

Storage account – lives in a region.

**Storage Resiliency types**

LRS Local redundant – 3 copies of data within same cluster (Same datacenter)

ZRS Zone Redundant – 3 copies spread across multiple AZs in a region

GRS G - 3 coopies in 1 region and 3 copies in another paired region

ZGRS – GRS + ZRS – 3 AZ in primary (Disributed in 3 AZ in primary) + 3 in a different datacenter (Single Datacenter)

ZGRS – Replicates Asynchronously

RA – Read only

Storage Performance –

Standard - LRS, ZRS, GRS, GZRS

Premium – LRS , LRS and ZRS for different blobs

**BLOBS**

Block – Stored in containers, no folders, very flat (Like S3). Azure datalakes gen2, Hierarchical file systems,

PAGE - Disks use page blob,

Disks – Standard HDD, Standard SSD, Premium SSD (S variant VM), Ultra Disk (S variant VM)

Snapshots

FILES – SMB and NFS Shares

Sync on prem files to Azure File share

Can Tier Data – Cold, Hot and Transaction optimized

Queues

Tables – Key value schemaless

BLOCK and FILES Blob

Premium – HOT, Cool, Archive

Standard –

Lifecycle Management – Move between tiers

**Databases**

Migration Data services

PosgresSQL

MySQL

CosmosSB – Multiple Models (APIs, Graphs, key values etcc..)

Azure Marketplace –

Internet of Things -

**Azure IoT Hub**

Talk to IoT via SDKs

Azire Io T Central – Dashboards, send email, get telemetry, call logic apps, customization

Azure Sphere – Securing IoT devices.

AS3 Service – Security Service

Data Services -

Orchestrate Data using Azure Data Factory

Extract – Transform – Load

Extract – Data Lake

HD insight – Transform, Databricks apache spark,

Azure Synapse Analytics – Orchestration of data services

**AI Services –**

Azure Machine Learning – Platform for predictions.

Azure Cognitive Services – Prebuilt Models, languages, Speech to text, Verification, vision services, decision, videos

Azure Bot Services – Chatbot, voice, interactions

Azure DevOps - Repositories, Boards, Pipelines – CI CD CDeploy, Artefacts – Libraries, test plans

GitHub – Repos, GitHub Actions – CI CD + All, Projects

Dev Test Labs - create, use, tear down, for testing development.

**Costs**

Type, SKUs, Tiers, Locations

Is it running

How many?

How much work its doing

How much its storing – capacity, interactions, transactions

Licensing

Cost Optimization – Autoscale, SKU optimization, Deallocation, resource groups, Lifecycle mgmt.

IaaS to PaaS, Tags for billing

Azure Advisor – Recommendations about cost, performance, resiliency, reliability

Azure reservations – 1 or 3 year terms

Hybrid Licensing – bring licenses from on prem to azure

Azure spot instance – Not critical workloads. Like batch process. Cheap as possible.

How do I know my cost – Pricing calculator

**Azure Monitor and Service Health**

**Azure Monitor -**  Azure AD Logs, Subscription Activity Logs, Resource Metrics and resource logs,

Diagnostic settings in Resource Logs can be sent to places like Log analytics, Storage AC, Event Hub

Log analytics – 2 years

Storage AC – Cheap Low cost

Event Hub – Publish/Subscribe

Alert rules can be created in azure monitor.

Action rules can be created based on alert rules which triggers actions (Action Group)

Azure Service Health – Azure infrastructure – Health alerts can be created

**SLA, Status, Documents and Compliance**

Every service has SLA

with AZ you get 99.99 SLA

Same AZ with Availability sets – (VMs in different Racks but same DC) – 99.95 SLA

Single

Premium 99.9

Standard 99.5

Private preview – Customer can apply – No SLA no support

Public Preview – anyone can try – No SLA no support

General Availability – Anyone can use – SLA and Support

Documents – Microsoft Privacy Statement, Online Servies terms, Data protection addendum

Azure Compliance – Security, Privacy and Compliance

Azure Trust Center

**Security, Defender for cloud and Azure Sentinel**

Physical security ,Identity and Access, Perimeter, Network NSG, Compute, Application layer

Confidentiality -

Integrity – nothing changed

Availability – protection

Az security center – Defender for cloud

How secure Azure subscription is

Azure Sentinel – On top of Log analytics workspace and adds SIEM

Recognizes patterns, queries, security orchestration and automation

SIEM and SOAR