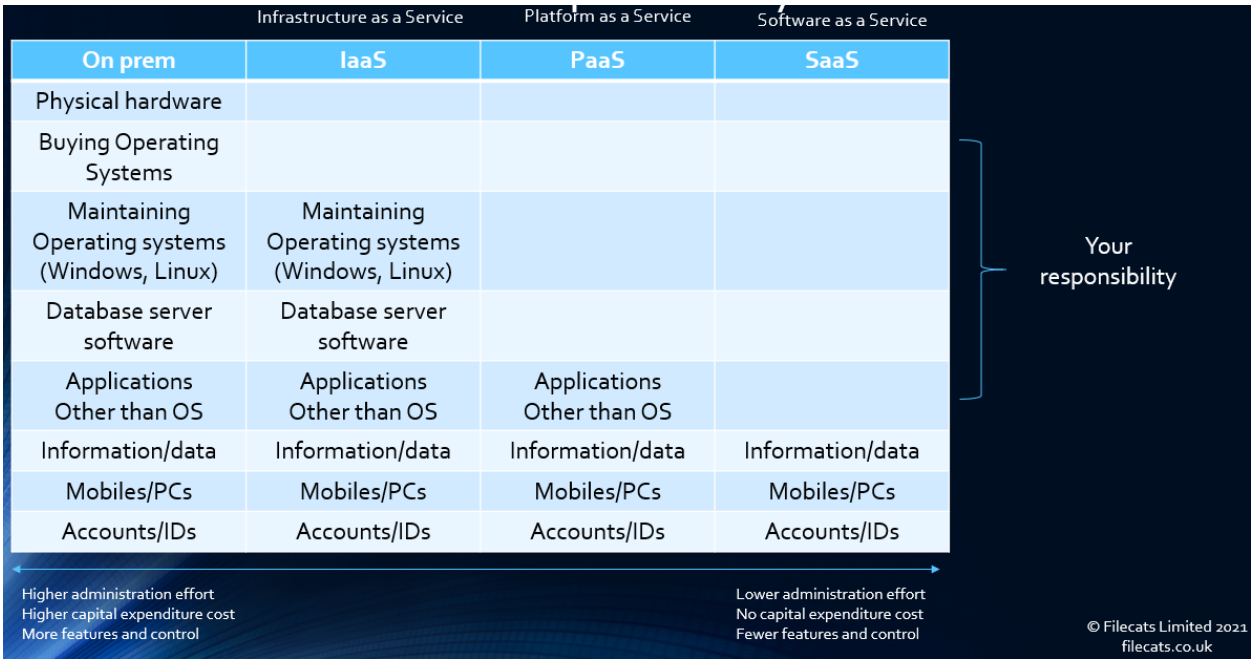
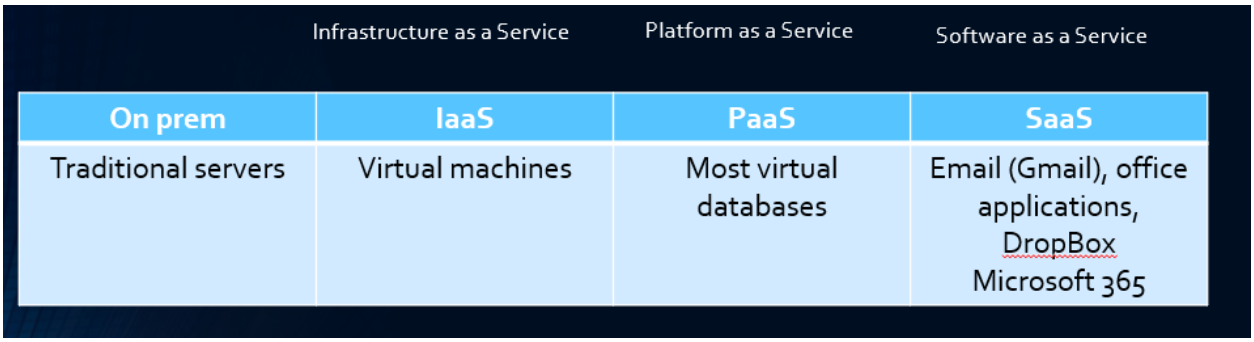
The number in the header gives the requirement number for the SC-900 exam.

Describe security and compliance concepts

1. Describe the shared responsibility model

On premises ("On prem")	The cloud (IaaS, PaaS, SaaS)
You know where your data is.	You have to trust the location of your data.
The physical location of your data is limited to places you own.	The location of your data can be worldwide.
You are in full control of security.	You have to trust your data's security, to an extent.
You are responsible for paying for the physical server boxes.	Your cloud provider pays for the physical server box, and you pay "rent" for the server.
To upgrade your memory, cores, hard drive space requires planning and purchase of equipment and probably several days/weeks.	To upgrade your memory, cores, hard drive space requires a click on a few buttons and a few minutes.
Capital expenditure	Operational expenses
You are responsible for doing hardware maintenance or upgrades.	Your cloud provider applies any hardware maintenance or upgrades.
You are responsible for doing any software updates.	Maybe you, maybe your cloud provider, are responsible for doing any software upgrades.





2. Define defense in depth

- This is the concept of having several layers, each defended. Broadly speaking:
    - Physical controls,
    - Technical controls – hardware and software, and
    - Administrative controls – policies and procedures.
- In Azure, this can be divided into:
    - Physical security layer – guarding the datacenter,
    - Identity and access layer – who has access,
    - Perimeter layer – DDoS protection,
    - Network layer – communications and access control,
    - Computer layer – access to VMs,
    - Application layer – secure applications,

- Data layer – access to data.

- Security posture is your ability to protect and respond to threats – divided into CIA:
    - Confidentiality – principle of least privilege,
    - Integrity – prevent unauthorized changes to data,
    - Availability – guard against DDoS attacks.

3. Describe the Zero-Trust methodology

- Zero Trust assumes that any request to connect to the network is uncontrolled.
- The motto of Zero Trust is “never trust, always verify”:
    - Verify Explicitly – authenticate, authorize identifies, location, classification of data, and look at risk (anomalies).
    - Have least privileged access. Limit access to only that which is needed, when it is needed.
    - Assume breach. Minimise how much breach, and where they can go if there is a breach. Have encryption of data, and constantly analyse.
- Why implement Zero Trust?
    - To go from on-premises to off-premises.
    - Go from on-premises identity with limited visibility of devices and logins, with a broad risk if breached.
    - To:
        - Confirm identities.
        - Access applications, networks and data.
        - Eliminate access where not needed on a very fine level.
        - Have automatic threat detection and response.
- There are six foundational elements:
    - Identities
        - People, services, or devices such as IOT.
        - Verify and give lease privilege access.
        - Go from on-premises identity.
        - To cloud identity with conditional access.
        - To authentication without passwords.

- Devices
    - Laptops, desktops, smart phones, tablets and more.
    - Go from needing to be on network, maybe through VPN (Virtual Private Network).
    - To having only devices registered with cloud being allowed access.
- Apps
    - How you use data, including apps installed by the end users, and not IT.
    - Go from on-premises and critical cloud apps.
    - To apps configured with Single Sign-on
    - To dynamic control with continuous verification.
- Infrastructure
    - Go from manually managed permissions.
    - To monitored workloads.
    - To granular visibility and access control, with access segmented for each workload.
- Network
    - Go from flat open network.
    - To multi micro-perimeters and micro-segmentation, and with encrypted internal traffic.
- Data
    - Go from authentication control.
    - To Smart Machine Learning classifications and encrypted.

- Use:
    - Strong authentication.
    - Policy-based access.
    - Micro-segmentation.
    - Automation for alerts and remediation.
    - Cloud intelligence and Artificial Intelligence to detect and respond to anomalies.
    - Classify, monitor and protect data.

-. Describe common threats

- Data breach
    - See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
    - "What is a personal data breach"
        - access by an unauthorised third party;
        - deliberate or accidental action (or inaction) by a controller or processor;
        - sending personal data to an incorrect recipient;
        - computing devices containing personal data being lost or stolen;
        - alteration of personal data without permission; and
        - loss of availability of personal data.
- Dictionary attack or password spraying
    - A more recent, novel tactic "sprays" several common passwords at tens of thousands of accounts at once to gain entry. Hackers cast a broad net at many organizations at once to better target where they wreak havoc.
- Malware
    - Short for "malicious software," these programs can steal information, lock your PC until you pay a ransom, or use it to send spam.
    - [Then scroll to 3.2Screen-locking ransomware]
- Ransomware
    - This malware locks a user out of their computer or network without access to files, folders, or drives. Attackers then demand a financial ransom to regain access; however, they don't always return access after payment.
- Phishing
    - Tricks users into giving out personal, financial, or company-specific information to gain unauthorized access to internal infrastructure.
- Disruptive attacks
    - Distributed Denial of Service (DDoS), targeted at a public endpoint

4. Describe encryption and hashing

- Encryption:
    - Protect data in motion,
        - Protects data from unauthorised people.

        - TLS - Transport Layer Security. This is a form of asymmetric encryption, in which you need a public key and a private key pair. Both are required to decrypt, but only one is needed to encrypt.
        - The alternative to asymmetric encryption is symmetric encryption, in which there is only one key for encrypting and decrypting.
        - HTTPS also uses asymmetric encryption.
    - Encrypt data at rest, TDE - Transparent Data Encryption (on by default).
        - A virtual (cloud-based) hard drive, for instance.
        - Without the encryption keys, the data is not readable.
    - Limit access to Data in use, Always Encrypted (encrypt some plain text columns).
    - Hide parts of data (e.g. credit cards), Dynamic data masking.
- Hashing
    - Converts text to a hash value.
    - Deterministic (always the same value). This can be a weakness.
    - Cannot be converted back.
    - Used for password checking.
- Digital signing.
    - Verifies that the contents have not been tampered with.
    - Does not encrypt or alter the message.
    - “Hashes” before and after. If they match, the contents have not been tampered with.

5. Describe compliance concepts

- Microsoft says "We respect local laws and regulations and provide comprehensive coverage of compliance offerings."
- https://docs.microsoft.com/en-us/compliance/regulatory/offering-home lists some of those laws and regulations.
    - Compliance is being in line with these laws and regulations, where applicable.
- One of the most famous is the General Data Protection Regulation of the EU (GDPR), which California, for instance, has based its Consumer Privacy Act on.
- The public ("data subjects") have the right to manage their personal data. Data subjects have the right:
    - to be informed that their data is being collected,

- to access it with one month of request,
- to rectify it, to delete it, or to restrict or suppress it, or to object to its processing
- to copy it from one environment to another – but not necessarily out of the EU ("data adequacy"). Following Brexit, the UK was found to be adequate.

- If a data breach happens, then the authorities must be notified.
- Data protection impact assessments must be taken by organizations.

-. Describe cloud adoption framework

- The Cloud Adoption Framework for Azure is proven guidance for successful business and technology strategies.
- It comes in four stages:
- Strategy
    - What is your business objective? Why are you moving to the cloud? What do you hope the outcomes to be?
- Plan
    - What do you want moving to the cloud? How will you do it? Who will help you in your organization?
- Ready
    - Review the literature, create your subscriptions, make sure it means your needs, and find out what best practices are.
- Adopt. This can be:
    - Migrate to the cloud
        - Migrate existing processes to the cloud, making sure you can make it as easy as possible, while following best practices.
    - Innovate
        - Creating new processes in the cloud. Is reality in line with what you wanted? Accelerate development, while following best practices.
- While going from Plan to Innovate, you need to Govern and Manage:
- Govern:
    - Where do you want to be?
    - Where are you?
    - What is your way to get there, while retaining relevant controls?

- Manage:
    - How much do you want to manage? What are your commitments?
    - Why do you want to manage? (Increasing Resilience, availability, while reducing cost)
    - Manage, while applying best practices.
    - Do you have elements which require greater management? See what you need to do.
- All of this is an iterative process – you need to revisit stages to see if you can improve.

Define identity concepts

6. Define identity as the primary security perimeter

- It used to be that you went into a place of work, connected a network lead into your computer, and logged into your computer.
- This is no longer the case. You may have:
    - Users connecting from home, either using managed devices or unmanaged devices.
    - Software (SaaS) which connects to your server.
    - IoT devices which connect to your server.
- Users and devices need:
    - High Availability
    - Relevant Access (Role Based Access Control)
- All of these use identity to identify themselves.
    - Administration
        - How to create and maintain identities
            - Automated requests
        - Authentication
            - Who can log in.
            - Where can they log in from
        - Authorization
            - What users can access what resources
        - Auditing
            - Track what happens.
            - Alerts and Governance.

7. Define authentication

- Authentication (AuthN) – who are you?
    - Uses Azure Active Directory (Azure AD or AAD).
    - Can also use Multi-factor Authentication (MFA) with Azure AD.

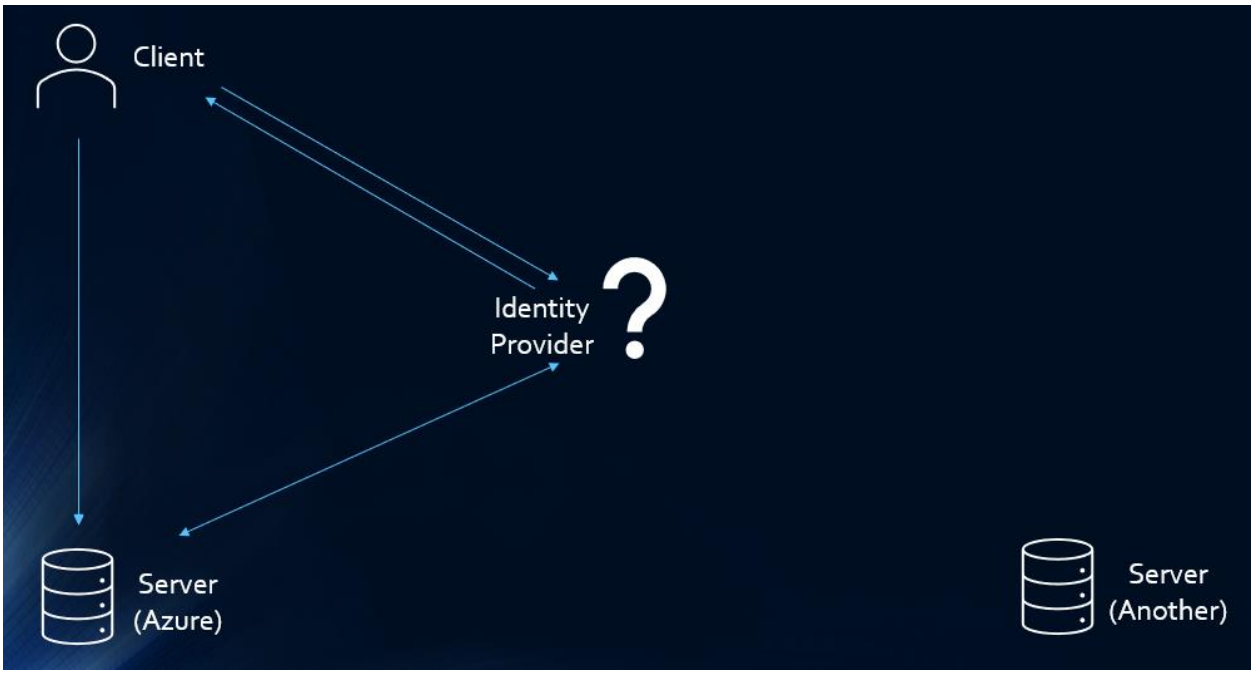
8. Define authorization

- Authorization (AuthZ) – what do you have access to?
- Uses Role-Based Access Control (RBAC).

9. Describe what identity providers are

- An identity provider verifies that a client (person, service) is who they are they are.
    - Allows for Single Sign-on to multiple apps or resources.
- Instead of logging into a server, the client logs into an Identity Provider.
- The Identity Provider passes a token back to the client, which can then be passed onto the server.
- The server can then validate this, either by checking that it is a valid key, or asking the identity provider.
- The token will include various payload claims (the header and signatures are not relevant to us):
    - aud – audience (the server),
    - idp – the identity provider,
    - iat – Issued At (when issued),
    - nbf and exp – Not Before and Expiration
    - preferred_username (mutable – may change),
    - and various permissions
- After expiration of token, new token is requested. This may not need user interaction, but is a useful time to check that permissions have not changed.
- Examples of identity providers include:
    - Google, Facebook, Instagram, Fitbit, Microsoft and Amazon Web Services.

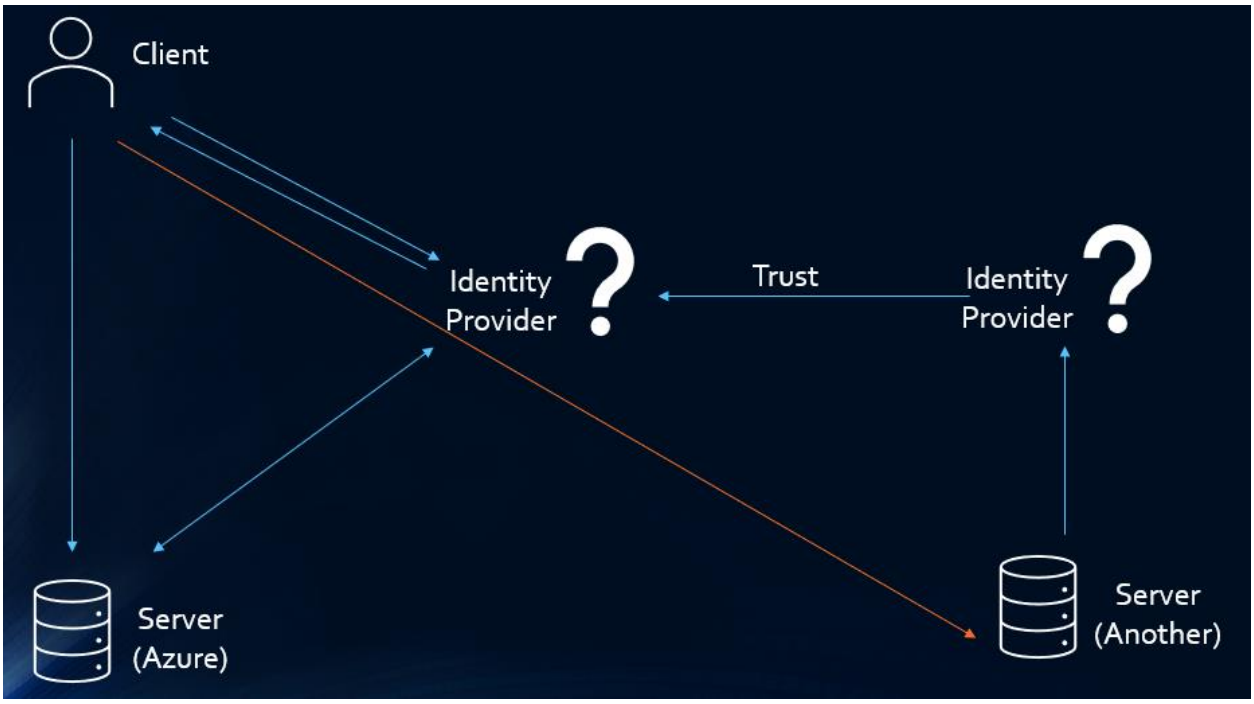
9. Describe what identity providers are



10. Describe what Active Directory is

- Active Directory is a Directory service. It is part of Microsoft Server 2000 onwards.
- It uses an Active Directory Domain Services (AD DS). This is a domain controller. A logical group of objects which share the same Active Directory.
- AD DS retains information of the devices and users, authenticate them, and gives them access (authorization).
    - Such as DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), WiFi, VPN (Virtual Private Network)
- Active Directory Domain Services allows for a single identity per user.
    - This means that a user's password needs only be changed once (on the server).
    - All client computers validate credentials against that stored in the server.
- Objects such as resources and security principals are arranged into domains, Domains are then grouped into trees, which are then grouped into a forest.
- It does not natively allow for mobiles, tablets, SaaS or more modern business apps.

11. Describe the concept of Federated services



-. Define common Identity Attacks

- Dictionary attack or password spraying
    - A more recent, novel tactic “sprays” several common passwords at tens of thousands of accounts at once to gain entry. Hackers cast a broad net at many organizations at once to better target where they wreak havoc.
- Keystroke logging
    - Monitoring what you enter on your computer, including user names and passwords to various (banking) websites.
- Phishing
    - Tricks users into giving out personal, financial, or company-specific information to gain unauthorized access to internal infrastructure.
    - Spear phishing – targeting a specific person. Research needed.
    - Whaling and CEO fraud – targeting specific ranks. May be a subpoena or complaint.
    - Clone phising – a previous email is taken and altered for bad reasons. Requires access to previous email.

Describe the basic identity services and identity types of Azure AD, part of Microsoft Entra

12. Describe what Azure Active Directory is

- Azure AD is an identity service for Microsoft Azure.
- It is not the same as Windows Server AD.
    - But it can be connected to it.
- It can be used by:
    - Users – to sign in to Azure and other services.
    - App Developers – they can use it in their applications for users to sign.
    - IT Administrators – to regulate AuthN and AuthZ.
- It is used by:
    - Azure Services,
    - Microsoft 365,
    - Dynamics 365, and
    - Power Platform.
- Azure AD allows for:
    - Self-service password reset (if enabled), and
    - Single Sign-on for apps.
- Different URL.
- It is available as:
    - Free,
    - Office 365 Apps
        - Company branding
        - self-service password reset for cloud users
        - Service Level Agreement
        - Device write-back
        - This is included with some Office 365 plans.
    - Premium P1 – all the above plus
        - Password Protection

- Self-service password reset, change, unlock.
- Hybrid Identities (see next video)
- Advanced Group access management
- Conditional Access
- This costs around $6/user/month.

- Premium P2 – all the above plus:
  - Identity protection
  - Identity Governance
  - This costs around $9/user/month.
- You may also be able to add-on additional features, such as Azure Active Directory Business-to-Customer (B2C), which can be useful for end users logging into Power Apps.

13. Describe Azure AD identity types (users, devices, groups, service principals/applications)

- Users
  - Regular users
  - If using Azure AD Business-to-Business (B2B), would include external guests from other tenants
- Groups
  - Multiple users
  - Allows you to assign similar rights
- Device
  - Mobile devices, laptops, servers, printers.
  - There are three different types:
    - Azure AD registered devices – Personally owned modern devices (Windows 10, iOS, Android, macOS)
    - Azure AD joined devices – Owned by an organization, they exist only in the cloud. Configure devices on Windows 10 Pro or above.
    - Hybrid Azure AD joined devices – Windows 7+ or Windows Server 2008+. Owned by an organization. Exist in cloud and on-prem.
- Service principals/applications
  - An identity for an application

- Must be registered with AAD first.

- Managed identities
    - Used for authenticating cloud applications.
    - Allows them to use some Azure services.
        - System-assigned ones are enabled by a service.
        - User-assigned ones are a standalone resource.

14. Describe what hybrid identity is

- Hybrid Identity is when you have two Active Directory structures:
    - Microsoft Server Active Directory (AD), using the Domain Services (AD DS) and
    - Microsoft Azure Active Directory (AAD).
- Changes to the AD DS (user accounts, contacts, groups) are synchronized to the Azure AD (AAD) using Azure AD Connect.
- Authentication is done using:
    - Azure AD (Managed authentication), or
    - Azure AD passing it to another Identity Provider (Federated Authentication).
- It uses:
    - Password hash synchronization (PHS)

        - The same credentials in AD as in AAD.
    - Pass-through authentication (PTA)
        - AAD validates users on-prem through AD.
    - Federated authentication (AD FS)
        - Another Identity Provider such as Active Directory Federation Services.

15. Describe the different external identity types (Guest Users)

- External identities, or guests, is supported through federated identity providers. It requires Premium P1 or P2.
- External users can sign in with their existing social media or other accounts.
- Single Sign On is allowed.
- There are two different types of Azure AD External Identities: B2B (business to business) and B2C (business to consumer).
- B2B
    - allows for sharing of apps and services with guests from other tenants.
    - uses invitations and redemptions.
    - users are integrated with tenants' users, with the same management, groups.
- B2C
    - allows for consumers to log into their social media or other accounts.
    - log-in screen is customizable with your company's branding.
    - allows for scaling, DDoS, password or other brute force attacks.
    - users are managed in its own B2C directory, separately from tenants' users.

Describe the authentication capabilities of Azure AD

16. Describe the different authentication methods

- Single Sign-On (SSO)
    - User name and Password
    - You only need to remember one set of credentials to gain AuthN to multiple systems.
    - There are other AuthN methods besides user name and password:
        - Certificates
        - Windows Hello for Business
        - Security keys

- Multifactor authentication. This can include:
    - Microsoft Authenticator app
    - Text messages
    - Voice call
    - Hardware.

17. Describe Multi-factor Authentication

- Why use MFA?
    - Passwords are easily hacked
- Multi-Factor Authentication (MFA)
    - Additional level of security, regarding at least two of the following:
    - Something you know – user name and password.
    - Something you have – mobile phone or phone call, email address verification, Microsoft Authenticator app [which may need your biometrics].
    - Something you are – fingerprint, face scan. These are collectively called Biometrics.
    - Microsoft Authenticator uses Open Authentication (OATH) – a one-time password (TOTP)
    - Fast Identity Online (FIDO2) is a passwordless authenticator, using an external security key.

18. Describe self-service password reset

- Allows users to change or reset their password, or unlock their account.
    - Does not require Help Desk, saving money.
    - Increases security and productivity
- Includes the following applications:
    - Microsoft 365,
    - Microsoft Azure,
    - Access Panel,
    - Federated apps, and
    - Custom apps using Azure AD.
- Requirements include:
    - Having an Azure AD license,

    - Enabled for Self-Service Password Reset, and
    - Authentication methods registered.
- When logging in, enter the user ID and pass a captcha.
- After passing checks, the user is guided through the process. The following methods are available (either 1 or 2 are required):
    - Microsoft Authenticator code (and maybe notification as well),
    - Email,
    - Mobile or Office phone, or
    - Security questions.
- In a hybrid environment using Azure AD Premium P1 or P2, Azure AD Connect can write back updates to passwords to the on-prem AD.

19. Describe password protection and management capabilities

- There are some well kn0wn weak passwords.
- These are banned in Azure AD Password Protection [live presentation].
    - This is a feature of Azure AD Premium P1 or P2.
- You can also passwords based on your own tenant, such as:
    - Brand and product names,
    - Locations,
    - Internal terms and abbreviations that have meaning in your tenant.
- In Hybrid security, Azure AD Password Protection can be integrated with an on-prem AD.
- One of the reasons why companies are moving away from user name and password, and going towards Multi-Factor Authentication.

- . Describe Windows Hello for Business

- Windows Hello is a more secure way for logging in. It incorporates the previously named Windows Passport product.
- It can authenticate to:
    - A Microsoft Account,
    - An AD account.
    - an Azure AD account, or
    - Identity Providers which support FIDO2 (Fast ID Online) authentication.
- Two Factor Authentication is required in the installation process.

- Windows Hello uses a biometric (facial or fingerprint recognition), or a PIN.
- The PIN is held in a more secure way than Windows Hello [not for Business].
    - It can be stored as a certificate or asymmetrical key pair.
    - The PIN is bound to that machine, and can be backed by a Trusted Platform Module chip.
    - The private key remains with the local machine. As it is not transmitted to the server, it cannot be stolen en route.

Describe access management capabilities of Azure AD

20. Conditional access

- Conditional Access
    - Determines whether you need to use Multi-Factor Authentication or be blocked.
    - You may be an already "trusted" computer – or maybe in a public place.
    - Uses a "What If" tool, to plan your Conditional Access policies.
    - You need Azure AD Premium P1 or P2 license, or Microsoft 365 Business Premium license.
- Takes into account:
    - User/group
    - Location
    - Device
    - Apps needed
    - Other risks, including Sign-in risk.
        - Whether the request is authorized by the identity owner.
- Use it when:
    - Some, or all users, need MFA.
    - Use approved client apps.
    - Use your trusted devices (e.g. company laptops, company mobile devices) or client app.
    - Require password change or protection policy.
    - Block untrusted devices.
    - Reduce access, e.g. block extraction of sensitive files.
- Requires Azure AD Premium P1 or P2 license.

21. Describe the benefits of Azure AD roles

- Built-in roles include:
    - Billing admin,
    - Global admin,
    - User admin,
- Custom roles can be added
    - Need Azure AD Premium P1 or P2 license.
- Role assignments are added in the Access Control (IAM) page.
    - Use to allow different people/services different permissions.
- Assign least privilege
    - Don't, for instance, use global admin roles, when more specific roles work do.

22. Describe the benefits of Azure AD role-based access control (RBAC)

- Use to allow different people/services different permissions.
- You can also deny people/services permissions.
    - Deny someone the ability to create new resource groups in a subscription, or new resources in a group.
- Role assignments are added in the Access Control (IAM) page, and consist of:
    - Security Principal – who (or what object) are you?
    - Scope - what do you want access to? This includes:
        - Management groups,
        - A subscription,
        - A resource group, and
        - A single resource.
    - Role definition (also known as "role") – how much access:
        - Owner – Full access, including delegating access.
        - Contributor – Full access, but not delegating access.
        - Reader – View access.
        - User Access Administrator – manage user access to Azure resources.

Describe the identity protection & governance capabilities of Azure AD

23. Describe what identity governance is

- Person – no access.
- Added to HR (e.g. Workday or SuccessFactors).
- HR then updates Azure.
- Identity created.
    - Or Microsoft Identity Management allows for the importing of records from on-prem HR systems.
- Gets permissions.
- Move roles.
- Gets different permissions.
- Leaves.
- Identity decommissioned (may be needed for auditing)
- Then repeat with [dynamic] groups.
    - Dynamic groups use attribute-based rules to determine whether a user is part of a group.

24a. Describe what entitlement management is

- "Entitlements" are access to resources. Management means allowing the right person to have these resources.
- However, doing it individually is not a good process. Instead, you can bundle up these entitlements into access packages (in containers called "catalogs"), which contain a bundle of resources and policies:
    - Members of Azure AD Security Groups,

    - Member of Microsoft 365 Groups and Teams,
    - Azure AD Enterprise Apps, and
    - SharePoint Online sites.
- Managers can define policies which contain:
    - Which users (internal and B2B external) which can request access,
    - The approval process, including who must approve access, and
    - The expiration of the access.
- Access packages are useful for:
    - Time-limited access to a resource.
    - Access which requires approval.
    - Departments who wish to manage their own access policies.
    - Multiple tenants collaborating on a project.
- This is available in Azure AD Premium P2 only.

24b. Describe what access reviews is

- Access reviews in Azure AD P2 allow you to manage group members, to ensure users have the least privileged permissions:
    - How do new employees have the access they need?
    - What about when they move teams or leave the company?
    - Too much access is bad – it may also result in negative audit finding.
    - Who is best to ensure who has access to resources? Is it really IT?
- The process includes:
    - Recertify and audit users' access to resources.
    - Reviewers are users (managers, group or app owners, or users themselves – self-reviews).
    - It recommends a decision based on user sign-in activity.
    - Reviews can automatically reoccur.
- . They are useful when:
    - There are too many high privilege users.
    - When permissions cannot be set up automatically.
    - When a group is used for a new purpose.

- When certain data is business critical.
- To maintain a policy's exception list.
- Ask group owners about their guests.
- Periodically, as per governance policies.

- See "Azure AD Access reviews" and PIM (next video).

25. Describe the capabilities of PIM

- PIM stands for Privileged Identity Management. It requires Azure AD Premium P2.
- It reduces the privileged access to Azure resources and Azure AD.
- It:
  - Provides just-in-time privileged access to Azure AD and Azure resources
  - Assign time-bound access to resources using start and end dates
  - Require approval to activate privileged roles
  - Enforce multi-factor authentication to activate any role
  - Use justification to understand why users activate
  - Get notifications when privileged roles are activated
  - Allows you to conduct access reviews to ensure users still need roles
  - is auditable.

26. Describe Azure AD Identity Protection

- Azure AD Identity Protection needs Azure AD Premium P2. It:
  - automates detection and remediation of identity-based risks,
  - investigates and exports risks.
- According to Microsoft:
  - Breach replay: 4.6BN attacks detected in May 2018 [a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants]
  - Password spray: 350k in April 2018 [multiple usernames are being attacked using common passwords in a unified, brute-force manner.]
  - Phishing: This is hard to quantify exactly, but we saw 23M risk events in March 2018, many of which are phish related
- Sign-in risk is the probability that it wasn't performed by the user:
  - Atypical location,

- Anonymous IP address (Tor browser, Anonymizer VPNs).
- unfamiliar sign-in properties.
- an IP linked to malware.
- password spray (brute-force attack of multiple usernames).

- User risk is the probability that an identity has been compromised:
  - leaked credentials.
  - Other threat intelligence.
- Azure AD Identity Protection reports on:
  - Risky users
  - Risky sign-ins, and
  - Risk Dections.
- After finding this out, remediate the risk or unblock users – quickly.

Describe basic security capabilities in Azure

27. Describe Azure DDoS protection

- DDoS are distributed denial of service attacks.
- They are huge numbers of machines making multiple requests of a resource.
- This can make the application slow or unresponsive.
  - Even Facebook, Twitter and Amazon can be targeted.
- DDoS Protection helps protect the perimeter layer. There are two levels:
- DDoS Protection Basic is free and automatically enabled.
  - Ensures that the Azure infrastructure is not affected.
- DDoS Protection Standard provides always-on traffic monitoring and real-time mitigation of attacks.
  - Specific for Microsoft Azure Virtual Networks.
  - The same defences Microsoft uses for its online services.
  - Gives logging, alerting and telemetry.
  - However, it does cost a lot!
  - Thankfully, if you get it for one subscription, you can extend it to other subscriptions at no extra cost.

28. Describe what Azure Firewall is

- A managed, cloud-based network security service
- Enables VMs and other compute resources to communicate with:
    - Each other,
    - The Internet (both inbound and outbound), and
    - Networks on-premises.
- Azure Firewall:
    - Is a stateful firewall:
        - It analyses the context of a connection, not just an individual piece of data.
    - Allows High availability.
    - Is scalable
- You can configure:
    - Application rules
    - Network rules, and
    - NAT rules
        - translates inbound requests to IP addresses
- Features include:
    - High availability with availability zones – up to 99.99% uptime.
    - It can scale up.
    - Limit outbound web and SQL traffic to a specified list of Fully Qualified Domain Names.
    - Centrally create network filtering rules which allow/deny traffic.
    - Outbound SNAT and DNAT: Source/Destination Network Address Translation – translate addresses with Multiple public IP Addresses.
    - And more.
- More details: https://azure.microsoft.com/en-us/services/azure-firewall/

29. Describe what Web Application Firewall is

- Web applications can be attack by exploiting vulnerabilities.
- You can have centralized protection by using Web Application Firewall (WAF)
- Protection against:
    - SQL-injection protection.

    - Cross-site scripting protection.
    - other common web attacks, crawlers and scanners.
- Detection of common application misconfigurations (for example, Apache and IIS).
- Configurable request size limits with lower and upper bounds.
- Create custom rules to suit the specific needs of your applications.
    - Geo-filter traffic to allow or block certain countries/regions from gaining access to your applications. (preview)
- Protect your applications from bots with the bot mitigation ruleset.
- Setup:
- Web Application Firewalls work with:
    - Application Gateway
    - Front Door
    - Content Delivery Network (CDN)

30. Describe Network Segmentation with Azure Virtual Networks

- Virtual Networks (VNets) enable resources to connect to other Azure resources.
    - Group related assets together, and isolate them.
    - By default, no traffic is allowed between VNets, but you can open paths when needed.
        - Helps with a Zero-Trust model.
    - Network Security Groups allows for communication between resources within the VNet.
    - A VNet is limited to a single region.
- VNets can be subdivided into smaller Virtual subnets.
- They allow for:
    - Communications, both between Azure resources using:
        - Virtual networks (for VMs, Power Apps, Kubernetes Service and VM Scale Sets).
        - Service endpoints (other Azure resources),
    - Communications between VNet and on-premises using VPN Gateways.
    - Route and filter network traffic using Azure Firewall
    - Internet communications
        - An Azure VM can connect to the Internet by default.

    - Incoming connections can be enabled.
- VNets can be linked together using Virtual Network Peering.
- For more information: https://azure.microsoft.com/en-us/services/virtual-network

31. Describe Azure Network Security groups

- Network Security Groups filter network traffic within a VNet (Virtual Network).
    - This helps protect the Network layer.
- You can specify rules based on:
    - IP Address,
    - Port, and
    - Protocol.
- You also determine the Priority (a number):
    - The lower number priorities are processed first.
    - Default rules have high numbers.
    - You cannot remove default rules, but you can add your own rules which supersede them.

32. Describe what Azure Bastion is

- To connect to a virtual machine, you could use Remote Desktop Protocol (RDP), or maybe Secure Shell (SSH).
    - This means that, by default, you have to open up ports 3389 (RDP) or 22 (SSH). A port scanner can check for ports that are open.
- A more secure way than opening these ports is by using an Azure Bastion host.
    - It stands between your VPNs and the outside world. You still use RDP/SSH, but in a different way.
- This provides RDP/SSH connectively over SSL (Secure Sockets Layer).
    - This uses an encrypted port 443, the same one that HTTPS uses.
- This means that you don't need a public IP address.
    - Protection against port scanning.
    - Protection against zero-day exploits.
- You deploy Azure Bastion to a virtual network, and to all of the Virtual Machines which are in that network.
- Your VMs do not require additional software, including Azure Network Security Groups (NSGs).

- Charges at around 20 cents per hour.

33. Describe ways Azure encrypts data

- Client-side encryption
    - So that Azure cannot decrypt the data.
- Server-side encryption
    - Keys or other secrets can be stored in the Key Vault, and can be Azure-managed or customer-managed. Secrets can also be stored in Hardware.
- Azure disk, Storage Service encryption and Data Lake
    - Encryption of data at rest
    - Windows BitLocker or Linux DM-Crypt
- Azure SQL Database
    - Transparent Data Encryption – encrypt data in real time.
- Encryption of data in transit
    - Transport Layer Security
- Virtual Private Networks
    - Create a secure tunnel.
    - Use certificate authentication.

Describe security management capabilities of Azure

34. Describe Cloud security posture management (CSPM)

- Cloud Security Posture Management, or CSPM, is a series of tools for security management – it is not just one tool.
- It uses:
    - Zero trust-based access control, considering the active threat level.
    - Real-time risk scoring: To provide visibility into top risks.
    - Threat and vulnerability management (TVM): look at the totality of the attack surface, and therefore, the risk.
    - Threat modeling systems and architectures: Used alongside other specific applications.
    - As part of this, you will also understand your risks and what you can do to help safeguard against it, your policies.

35. Describe Microsoft Defender for Cloud

- Monitoring service

- On-premises and cloud.
    - You can install the Log Analytics agent on both Windows and Linux servers.
- Continuous monitoring of resources
- Security recommendations for you
- Apply required security settings to new resources
- Block malware from your VMs and other resources.
    - Also, application control rules can define a list of allowed applications that can be installed.
- Detect potential inbound attacks, and investigate threats
    - Such as brute force attacks.
- Provide just-in-time access control for network ports.

- PaaS services are automatically monitored by Azure Security Center.
- Integrates with Microsoft Defender for Endpoint.
- Policy Compliance
    - How you are doing against your policy requirements
- Security Alerts
    - Create automated responses with workflow automation (Azure Logic Apps)
- Regulatory Compliance
    - Security issues and vulnerabilities, with respect to regulatory standards.
- Azure Security Center is free of charge. However, Azure Defender is chargeable.

35. Describe Secure score in Microsoft Defender Cloud

- Secure Score
    - Measurement of security posture
    - Report on current state.
    - Improve security posture.
    - Compare with benchmarks.
- Recommendations are grouped into security controls, a logical group of recommendations.
    - Enable MFA
    - Secure management ports

- Apply system updates
- Remediate vulnerabilities
- Encrypt data in transit
- Enable encryption at rest
- Restrict unauthorized network access
- Manage access and permissions
- Remediate security configurations
- Apply adaptive application control
- Protect your applications with Azure advanced networking solutions, such as DDoS Protection Standard.
- Enable endpoint protection

36. Describe enhanced security of Microsoft Defender for Cloud

- The enhanced security of Azure Defender provides:
    - Alerts,
    - Advanced protection, and
    - Vulnerability assessment.
    - Threat protection for Virtual Machines and PaaS services.
    - Just in Time Virtual Machine access.
    - Adaptive application controls and network hardening.
    - Regulatory compliance dashboard and reports
    - Threat Protection for non-Azure servers and virtual machines in other clouds.
- Go to Getting started.
- The enhanced security of Azure Defender comes as:
    - for servers adds threat detection and advanced defenses.
    - for App Service identify attacks targeting applications running over App Service.
    - for Storage detects potentially harmful activity on your Azure Storage accounts (blob containers, file shares, or data lakes).
    - for SQL secures your databases and their data wherever they're located.
    - for Kubernetes provides the best cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.

- for container registries protects all the Azure Resource Manager based registries in your subscription.
- for Key Vault provides an extra layer of security intelligence.

37. Describe security baselines for Azure

- Microsoft, the Center for Internet Security (CIS), and the National Institute of Standards and Technology (NIST) have developed security benchmarks. Some of these have been included in the Azure Security Benchmark.
- They are included in:
  - Network security,
  - Identity Management,
  - Privileged Access,
  - Data Protection,
  - Asset Management,
  - Logging and Threat Detection,
  - Incident Response,
  - Posture and Vulnerability Management,
  - Endpoint Security,
  - Backup and Recovery, and
  - Governance and Strategy.
- Clicking on one of them shows:
  - The Azure Security Benchmark, the CIS Controls and NIST IDs.
  - Recommendation and Guidance,
  - Who is Responsible, and
  - the Customer Security Stakeholders.

Describe security capabilities of Microsoft Sentinel

38. Define the concepts of SIEM, SOAR, XDR

- SIEM [prounced SEEM] stands for security information and event management. Azure Sentinel is a SIEM tool. SIEM does:
  - aggregating data from multiple sources, including network, security, servers, databases and applications.
  - Looking for common attributes.

    - Alerting correlated events.
    - Transforming it into dashboards to assist in seeing patterns or other activity.
    - Automating the gathering of compliance data.
- SOAR is a security orchestration, automation and response tool.
    - It takes action based on the alerts from the SIEM system.
- XDR stands for eXtended detection and response. Microsoft 365 Defender and Azure Defender are XDR tools.
    - It natively integrates multiple security products into a security operations system.
    - Azure Defender is integrated with Azure Sentinel, so the XDR data can be integrated in just a few clicks.

39. Describe how Azure Sentinel provides integrated threat protection

- Security information and event management (SIEM) system
- Collect cloud data at scale
    - Across users, devices, applications and infrastructure
- Detect previously undetected threats
    - With built in and custom analytics
    - Workbooks allow you to monitor data using templates.
    - Hunting allows you to proactively search for security threats.
        - Notebooks allow you to use Azure Machine Learning Python and Jupyter
- Investigate threats with AI and respond to incidents rapidly
    - Azure Monitor Workbooks can automate analyses, and then trigger an action.
- Respond
    - Orchestration and automation of common tasks using playbooks
- Azure costs:
    - a price per Gigabyte of volume ingested (around $2.50 per GB), or
    - Capacity Pricing, which gives a discount of 50%-60% if you commit to a capacity of at least 100 Gb per day.

Describe threat protection with Microsoft Defender XDR

40. Describe Microsoft Defender XDR services (formally Microsoft 365 Defender)

- Microsoft Defender for Endpoint

    - Previously known as Microsoft Defender Advanced Threat Protection (ATP)
    - A unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.
- Microsoft Defender for Office 365
    - Previously known as Office 365 ATP
    - Guards against threats in emails, malicious links or URLs, and collaboration tools.
- Microsoft Defender for Identity and Azure AD Identity Protection
    - Previously known as Azure ATP
    - Uses Active Directory for threat detection, sign-in risk and user risk.
- Microsoft Cloud App security
    - A SaaS solution to help your cloud apps with strong data controls, a high level of visibility, and enhanced threat protection.
- They work together instead of in silos:
    - Central dashboard helps security professionals focus on what is important.
    - As signals are shared and actions are automated, it helps protect against attacks and allows for coordinated defensive responses.
    - With joined-together data on incidents, the full story of an attack across different security teams can be views.
    - Impacted resources can start to heal through automated response and remediation.
    - Security teams and hunt threats across endpoints and Office data.

41. Describe Microsoft Defender for Office 365 (formerly Office 365 Advanced Threat Protection)

- Guards against threats in emails, malicious links or URLs, and collaboration tools.
- It includes:
    - Threat protection policies
        - Define threat-protection policies to protect your organization.
    - Reports
        - Monitor Defender for Office 365 using reports.
    - Threat investigation and response capabilities
        - Investigate, understand, simulate, and prevent threats.
    - Automated investigation and response capabilities

- Save time and effort investigating.

- There are two plans for Microsoft Defender for Office 365
  - Plan 1 is included in Microsoft 365 Business Premium.
  - Plan 2 is included in Office 365 E5, Office 365 A5, Microsoft 365 E5 Security, and Microsoft 365 E5.
  - You can also add it as an add-on into some other plans.
- Plan 1 includes:
  - Safe Attachments, for email, SharePoint, OneDrive, and Microsoft Teams
    - Checks against known virus and malware signatures, then applies Machine Learning and Analysis techniques to detect malicious intent.
  - Safe Links
    - Malicious links are dynamically blocked while good links can be accessed.
  - Anti-phishing
    - Checks incoming messages for indicators that a message might be a phishing attempt. Uses Machine Learning models to analyze messages
  - Real-time detections.
- Plan 2 adds to this with automation, investigation, remediation, and simulation tools:
  - Threat Trackers
    - Widgets and views that provide intelligence on cybersecurity issues.
  - Threat Explorer
    - Lets authorized users identify and analyze recent threats.
  - Automated investigation and response (AIR)
    - By automating some tasks, your security operations team can operate more efficiently and effectively
  - Attack Simulator
    - Lets you run realistic attack scenarios in your organization.
  - Campaign Views
    - Allows you to investigate and respond to phishing attacks, and understand the scope of the attack.

42. Describe Microsoft Defender for Endpoint (formerly Microsoft Defender Advanced Threat Protection)

- It is designed to help enterprise networks prevent, detect, investigate, and respond to threats in Windows 10 and Microsoft cloud services.
- It uses:
    - Endpoint behavioral sensors in Windows 10, to collect and process behavioral signals.
    - Cloud security analytics using big-data, device-learning, and unique Microsoft optics to create into insights, detections, and recommended responses to advanced threats.
    - Threat intelligence to identify attacker tools, techniques, and procedures, and generate alerts.
- There are seven parts to Microsoft Defender for Endpoint:
    - Threat and vulnerability management
        - an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.
        - Discover vulnerabilities and misconfigurations in real time with sensors, without the need of agents or periodic scans.
        - It allows real-time discovery, intelligence-driven prioritization and seamless remediation.
    - Attack surface reduction
        - Reduces vulnerabilities,
        - Protect and maintain the integrity of a system,
        - Use application control so that your applications must earn trust in order to run
        - Help protect operating systems and apps your organization uses from being exploited.
        - Secure your devices against web threats and help you regulate unwanted content
        - two-way network traffic filtering.
        - Works with Microsoft Defender Antivirus (an additional product) for network protection and controlled folder access.
- Next-generation protection in Windows using Microsoft Defender Antivirus:
    - Behavior-based, heuristic, and real-time antivirus protection,
    - Cloud-delivered protection,

    - Dedicated protection and product updates.
    - A chargeable extra.
- Endpoint detection and response
    - Provide advanced attack real-time and actionable detections.
    - It creates alerts which are aggregated into incidents.
- Automated investigations and remediation (AIR)
    - Starts when an alert is triggered or an investigation is manually started.
    - Examines alerts and takes action to resolve any breaches.
- Microsoft Threat Experts
    - Targeted attack notification and access to experts on demand
    - Experts on Demand is a chargeable extra.
- Microsoft Secure Score for Devices
    - Looks at application, operating system, network, accounts and security controls.
- It can also integrate, using APIs, with raw data streaming and SIEM [seem] integration.
- It integrates with:
    - Azure Security Center,
    - Azure Sentinel,
    - Intune (which we'll look at in a later section),
    - Microsoft Defender for Identity, and for Office,
    - Skype for Business, and
    - Microsoft Cloud Add Security.

43. Describe Microsoft Defender for Cloud Apps

- Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy.
- It is available with Azure Active Directory Premium P1 and P2.
    - There is also Office 365 Cloud App Security, which is a reduced version concentrating on Office 365.
- CASBs act a gatekeeper to broker access in real time between your users and cloud resources.
- It
    - Discovers and provides visibility into Shadow IT and app use,

    - monitors user activities for odd behaviors,
    - controls access to your resources, allow you to classify and prevent sensitive information leak, protect against bad actors, and assessing the compliance of cloud service
- CASBs help you do by providing a wide array of capabilities:
    - Visibility: assign cloud services a risk ranking; identify users and third-party apps that can log in
    - Data security: identify and control sensitive information
    - Threat protection: analyse user and entity behavior and mitigate malware
    - Compliance: create cloud governance reports and dashboards, including with respect to regulatory compliance needs.
    - Addressing Shadow IT in your organization
        - Discover all cloud apps and services used in your organization
        - Assess the risk and compliance of your cloud apps
        - Detect when data is being exfiltrated from your corporate apps
    - Protect your information in the cloud
        - Gain visibility into corporate data stored in the cloud
        - Enforce compliance policies for sensitive data stored in your cloud apps
    - Detect and protect against cyberthreats
        - Record an audit trail for all user activities across hybrid environments
        - Identify compromised user accounts
    - Assess and protect your IaaS (Infrastructure-as-a-Service) environment
        - Audit the configuration of IaaS environments
        - Monitor user activities to protect against threats in your environments
        - Capture user activities within custom cloud and on-premise apps
- It uses Cloud Discovery
    - This uses traffic logs to analyze the cloud apps that your organization is using. You can also upload log files from your firewalls for analysis.
- Sanctions and unsanctions apps in your cloud.

    - This uses the Cloud app catalog, which has over 16,000 cloud apps that are ranked and scored based on industry standards and 80 risk factors. So it will let you know how risky an app is.

- Allow you to have APIs (Application Programming Interfaces), for visibility and governance of apps that you connect to.
    - Microsoft Cloud App Security works with app providers on optimizing the use of APIs for best performance.
- Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps.
    - Avoid data leaks by blocking downloads in real time.
    - Set rules that force data to be encrypted
    - Monitor unprotected endpoints – what is happening on unmanaged devices
    - Control access from non-corporate networks or risky IP addresses
- Helping you have continuous control by setting, and then continually fine-tuning, policies.
    - You can use policies to integrate remediation processes to achieve complete risk mitigation.

44. Describe Microsoft Defender for Identity (formerly Azure Advanced Threat Protection)

- Uses on-prem Active Directory Data
    - Protects the Active Directory Federation Services (AD FS) in hybrid environments.
- Monitor users, entity behavior, and activities with learning-based analytics
    - Identifies anomalies, given you insights into suspicious events, showing threats and compromised users.
- Protect user identities and credentials stored in Active Directory
    - Gives you security best practices, reducing your attack surface, making it harder to attack your user credentials.
    - Its Lateral Movement Paths allow you to know how attacks can move from identities to endpoints, apps and data.
    - It also identifies users who sign in using clear-text passwords.
- Identify and investigate suspicious user activities and advanced attacks
    - Identify rogue users and attackers' attempts to gain user names, IP address, group memberships and more.
    - Identifies brute force attacks and other attempts to compromise user credentials.

- Detects attempts to move laterally in the network.
- Highlights attacker behavior

- Provide clear incident information on a simple timeline for fast triage
  - So you can stay focused on what matters, using smart analytics.

45. Describe the Microsoft 365 Defender portal

- The Microsoft 365 Security is at https://security.Microsoft.com
- It brings together functionality from:
  - Microsoft Defender for Office 365,
    - with its email and link protection
  - Microsoft Defender for Endpoint
    - with its devices and Windows 10 protection
  - Microsoft 365 Defender.
- To use it, you need:
  - Global administrator permissions,
  - Security administrator, Security Operator
  - Global Reader, Security Reader
- Home – overall dashboard
  - common cards, which may vary depending on their role-based access control.
  - Identities cards – keep track of suspicious or risky behavior.
  - Data risks – activity that could lead to unauthorized data disclosure
  - Devices – alerts, breach activities and other threats, and
  - Apps – how cloud apps are used.
- Reports have items regarding:
  - a general security report. Cards are similarly grouped by category, but can be regrouped by topic:
    - Risk – possible sources of risk, and
    - Detection trends – new threat trends
    - Configuration and health – security controls
    - Other

- Endpoints, and
- email and collaboration

45. Describe how to use Microsoft Secure Score

- Unlike Azure Secure Score, this is a measurement of your Microsoft 365 identities, apps, and devices.
- Again, it reports on the current stage, gives recommendations, and compares with benchmarks and Key Performance Indicators.
- Points are given for actions. Unlike Azure, some points may be available for actions done on only some devices or users.
- Includes recommendations for:
    - Microsoft 365 (including Exchange Online)
    - Azure Active Directory
    - Microsoft Defender for Endpoint
    - Microsoft Defender for Identity
    - Cloud App Security
    - Microsoft Teams

45. Describe the Microsoft 365 Security Center

- Hunting
    - Search for threats across:
        - Devices managed by MS Defender for Endpoint,
        - Email processed by Microsoft 365,
        - Cloud app activities, tracked by Microsoft Cloud App Security and Microsoft Defender for Identity
    - Uses the Kusto query language.
- Action Center
    - See pending, approved and completed remediation actions.
        - Quarantine actions (release or stop item, or run antivirus),
        - Restrict code execution,
        - Isolate device
- Threat Analytics
    - Active threat actors,

    - New attack techniques
    - Common attack surfaces and malware
- Policies and rules
    - Threat and alert policies, and activity and advanced alerts
- Permissions and roles, including:
    - Azure Active Directory,
    - Endpoints roles and groups, and
    - Email and collaboration roles.

-. Describe incidents and incident management capabilities

- Alerts indicate malicious or suspicious events. They are typically part of a broader attack, which are aggregated together into incidents.
- Incidents may involve devices, users and other entities.
- The incident overview gives you:
    - Top impacted assets,
    - Risk level, and
    - Investigation priority.
    - The chronological order of alerts,
        - together with their reasons.
    - Remediation status.
- Alerts
    - View severity, entities involves, source of alerts, and why they were linked together.
    - Generated from Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Defender for Office 365
    - Devices, users and mailboxes related to the incident.
        - Clicking on a user will take you to their Cloud App Security page.
        - Clicking on a mailbox will take you to the Microsoft Defender for Office 365 page.
    - Investigations are the automatic investigations.
        - Remedial status.
    - Evidence – really drill down in an alert

- All of the emails, email clusters, user activities, files, processes, IP address and URLs (links).

Describe the compliance management capabilities of Microsoft

46. Describe the offerings of the service trust portal

- **Service Trust Portal** – home page.
- **Compliance Manager** – measures your progress in completing actions that help reduce risks around data protection and regulatory standards. To find out more, see the Microsoft Compliance Manager documentation in the Learn More section below.
- **Trust Documents** – links to a security implementation and design information.
- **Industries & Regions** – contains compliance information about Microsoft Cloud services organized by industry and region. The Industry Solutions link currently displays the home page for Financial Services.
- **Trust Center** – links to the Microsoft Trust Center, which provides more information about security, compliance, and privacy in the Microsoft Cloud.
- **Resources** – links to resources including information about the features and tools available for data governance and protection in Office 365, the Microsoft Global Datacenters, and Frequently Asked Questions.
- **My Library** – allows you to add documents and resources that are relevant to your organization. Everything is in one place. You can also opt to have email notifications sent when a document is updated, and set the frequency you receive notifications.

47. Describe Microsoft's privacy principles

Microsoft has six privacy principals:

- **Control**: Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.
- **Transparency**: Being transparent about data collection and use so that everyone can make informed decisions.
- **Security**: Protecting the data that's entrusted to Microsoft by using strong security and encryption.
- **Strong legal protections**: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.
- **No content-based targeting**: Not using email, chat, files, or other personal content to target advertising.
- **Benefits to you**: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

Describe the compliance management capabilities of Microsoft 365/Purview

48. Describe the compliance center

- If you have data, you need to ensure that it is handled correctly.

Describe the compliance management capabilities of Microsoft 365/Purview

- Companies have to not only abide by the law of a country, together with state and local laws, but also by their industry's rules.
- You may be required to keep records of user activities for years, but also maintain user privacy and the right to request, amend, and remove such information.
- This is the Microsoft 365 Compliance Center
    - https://compliance.microsoft.com
- The home gives you several cards.
    - We'll have a look at the Compliance Manager and Score in later videos.
    - The solution catalog card links to integrated solutions for managing compliance scenarios.
- It is organised into:
    - Information protection & governance. This is for protecting and governing data in your organization.
        - Data loss prevention
        - Information governance
        - Information protection, and
        - Records management
    - Insider risk management. This shows how you can identity, analyze and reduce internal risks before they materialise.
        - Communication compliance, and
        - Insider risk management.
    - Discovery & response. Deal with compliance issues.
        - Audit
        - Data investigation and data subject requests under the General Data Protection Regulation (GDPR).
        - eDiscovery (we will be looking at that later).
    - On the left-hand side we have access to other things ("Show All" shows more solutions) which are contain in the Solution catalog" page.
- Active alerts card
    - The most active alerts and their Severity, Status, Category and Last Activity.
    - More details are available in the Alerts section in the left-hand pane.

- You may have additional cards that you can add.

49. Describe compliance manager

- Compliance Manager, which used to be in the Microsoft Service Trust Portal, is now in the Microsoft 365 compliance center.
- It helps you manage your company's compliance requirements.
- It includes:
    - Pre-built assessments for industry, regional and country requirements. You can also build custom assessments for your compliance needs.
    - Takes the lawyer-speak out of requirements, and puts them into Plain English.
    - Maps regulatory requirements to recommended improvement actions, and guidance on suggested improvement actions for those requirements.
    - Workflows for completing your risk assessments.
    - And a compliance score, which we will look at in the next video.
- It is built around:
    - Assessment templates.
        - There are over 150 assessments templates. You can also build a custom template for internal business process control, and regional data protection standards.
    - Assessments
        - A big group of controls.
    - Solutions
        - A smaller group of controls.
    - Controls.
        - Individual requirements.
        - Go to Assessments – Data Protection Baseline – Controls.
        - Controls are either None (not tested), In progress, Passed, Failed, or Out of Scope.
        - Your requirements.
        - Microsoft managed controls,
        - Your customer managed controls,
        - Shared controls.

- Improvement actions
    - Recommended guidance to help you with comply with data protection regulations and standards.
    - You can assign action to your users, store implementation notes, and documents.

50. Describe use and benefits of compliance score

- Compliance scores measures your progress in completing recommended improvement actions within controls.
    - They have an improvement action score.
        - This helps you prioritise actions that will have the highest impact.
    - Control score. For you to gain this score:
        - Implemented Status needs to be Implemented or Alternative Implementation, and
        - Test Result equals Passed.
    - Assessment score.
        - The total of your control scores.
- The initial score is based on the Microsoft 365 data protection baseline. This draws from:
    - NIST CSF ((National Institute of Standards and Technology Cybersecurity Framework),
    - ISO (International Organization for Standardization),
    - FedRAMP (Federal Risk and Authorization Management Program) and
    - GDPR (General Data Protection Regulation of the European Union).
- Compliance Manager automatically updates your status based on your Microsoft 365 environment.
    - The action status is updated every 24 hours.
- There are:
    - Technical actions, such as changing a configuration.
    - Non-technical actions, either documentation or operational.
- Additionally,
    - Preventative actions – against specific risk, such as actions against attacks, breaches and fraud. These are worth 9 points.

    - Detective actions – identity irregular behaviors which either represent risk or could be used to detect intrusions or breaches, such as system access auditing and privileged admin actions. These are worth 1 point.
    - Corrective actions – reversing the damage of a security incident if possible. They are also worth 1 point.
- There are also:
    - discretionary actions – these rely upon users to understand and do a policy.
    - Mandatory actions – these are required, such as a password policy. Mandatory actions multiple the points value by 3.

Describe information protection and governance capabilities of Microsoft 365/Purview

51. Describe data classification capabilities

- Microsoft Information Protection (MIP) helps you discover, classify, and protect sensitive information.
    - There's also MIG, Microsoft Information Governance.
- It is based around 4 principals:
- Know your data
    - Understand where your data is, and what is important.
    - Sensitive information types – identifies sensitive data using trainable classifiers
    - Data classification – sensitivity labels, retention labels, or classification
- Protect your data
    - Flexible protection
    - Sensitivity labels – across apps, services and devices to label and protect your data.
    - Encryption – at rest or in transit
    - Microsoft Cloud App Security – protects sensitive information
- Prevent data loss
    - Accidental oversharing of sensitive information.
    - Data loss prevention policies (DLP)
    - Endpoint data loss prevention
    - Protect sensitive information in Microsoft Teams
- Govern your data

- For compliance and regulatory requirements
- Retention policies and retention labels – retain or delete content with a workflow for email, documents, messages and more
- Records management – incorporates retention requirements into an overall plan.

52. Describe the value of content and activity explorer

- Context Explorer shows a snapshot of your items that have:
  - a sensitivity label,
  - a retention label or
  - have been classified as a sensitive information type in your organization
- Use in Microsoft 365 compliance center > Data classification > Content explorer.
- Export
- Search using:
  - A Microsoft Exchange mailbox email address,
  - A SharePoint/OneDrive site name, folders and files.
- Click on a file allows you to read the contents and metadata.
- Because you can read the contents of scanned files, you need either:
  - Content Explorer List viewer
  - Content Explorer Content viewer
- Activity Explorer monitors your labelled content across:
  - SharePoint Online, and
  - OneDrive.
  - It does not work for Exchange Online.
- It monitors activities such as:
  - label applied
  - label changed (upgraded, downgraded, or removed)
  - auto-labeling simulation
  - files copied
- There are over 30 different filters available for use, including:
  - date range

    - activity type
    - location
    - user
    - sensitivity label
    - retention label
    - file path
    - DLP policy
- You need to have one of the following roles:
    - Global administrator
    - Compliance administrator
    - Security administrator
    - Compliance data administrator

53. Describe sensitivity labels and sensitivity label policies

- Sensitivity labels are:
- Customizable.
    - Specific to your organization and business needs, you can create categories for different levels of sensitive content in your organization. For example, Personal, Public, General, Confidential, and Highly Confidential.
- Clear text.
    - The label is stored in clear text in the metadata for files and emails. Other applications can read it and act on it.
- Persistent.
    - As the label is stored in metadata, the label moves with the content, no matter where it's saved or stored. You can then create policies based on this label.
- When using the encrypted settings, you can protect the content:
    - Only users in your organisation can open it.
        - It can be decrypted only by authorised users.
    - Only users in marketing and edit and print, but others can only read it.
    - It cannot be forwarded or copied.
        - Remains encrypted, even if renamed.

        - It is encrypted both at rest and in transit.
    - It cannot be opened after it expires.
- Data can be classified in three different ways:
- Manually
- Automatically using:
    - Keywords or metadata
    - Data which fits sensitive information:
        - National identity/ID card/social security numbers,
        - Bank accounts,
        - Business numbers,
        - Company/legal entity numbers,
        - Driver's license numbers
        - Medical account numbers,
        - Passport numbers,
        - Tax identification, value added/sales tax numbers, tax file numbers,
        - Database connection strings,
        - Computer keys.
    - Trainable classifiers – mostly in English, unencrypted items
        - Pre-trained classifiers (status: "Ready to use"):
            - Resume/CV,
            - Source data, e.g. C#, JavaScript, Python, R, Ruby
            - Targeted Harassment - offensive conduct about race, ethnicity, religion, national origin, gender, sexual orientation, age, disability
            - Offensive Language
            - Profanity - expressions that embarrass most people
            - Threat - threats to commit violence or do physical harm or damage to a person or property
        - Custom classifiers – needs examples to work.
            - Legal documents

        - Strategic business documents – press releases, deals, Intellectual property.
        - Pricing information – invoices, work orders, quotes
        - Financial information – company results, investments
- Sensitivity labels may results in:
    - Protection settings that include encryption and content markings
        - A “Confidential” label encrypts the document/email and adds a “Confidential” watermark to a document/email.
    - Protect content in Office apps across different platforms and devices
    - Protect content in third-party apps and services by using Microsoft Cloud App Security
        - such as SalesForce, Box, DropBox
    - Protect containers that include Teams, Microsoft 365 Groups, and SharePoint sites.
        - set privacy settings, external user access and external sharing, and access from unmanaged devices
    - Extend sensitivity labels to Power BI
        - Protect when data saved outside of Power BI.
    - Extend sensitivity labels to assets in Azure Purview and third-party apps and services
        - Apply sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more.
    - Classify content without using any protection settings.
- Label policies can:
    - Choose which users and groups see the labels.
    - Apply a default label to all new documents and unlabeled emails
    - Require a justification for changing a label.
    - Require users to apply a label
    - Provide help link to a custom help page

54. Describe Data Loss Prevention

- DLP policies help prevent company data from being accidentally made public.
- Identify sensitive information from:
    - Exchange Online,

    - SharePoint Online,
    - OneDrive for Business,
    - Microsoft Teams chat and channel messages,
    - Windows 10 users or groups, and
    - Microsoft Cloud App Security.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users stay compliant without interrupting their work.
- View DLP alerts and reports showing content that matches your organization's DLP policies.
- A policy contains:
    - Where to protect,
    - Rules, containing:
        - Conditions – what to look for (can use AND/ORs), and
        - Actions – what to happen if conditions are met.
            - Restrict access to content for everyone.
            - Restrict access to content for people outside the organization.
            - Restrict access to "Anyone with the link."
    - Priority – which rule to process first.
- Alerts and Incident reports
    - Can be sent to your compliance officer.
- Endpoint data loss prevention (Endpoint DLP) extends this to Windows 10 machines.
- Allows you to audit and restrict activities on these machines:
    - upload to cloud service, or access by unallowed browsers
    - copy to other app, USB stick, Bluetooth device, remote session or network share,
    - print a document,
    - create or rename an item (not restricted, just auditable).
- Endpoint DLP supports monitoring of these file types:
    - Word files (always)

- PowerPoint files (always)
- Excel files (always)
- PDF files (always)
- .csv files (always)
- Optionally:
    - .tsv files
    - .txt files
    - .rtf files
    - .c files
    - .class files
    - .cpp files
    - .cs files
    - .h files
    - .java files

- Data loss prevention can be extended to Microsoft Teams.
    - The default DLP policy tracks all the credit card numbers shared, for all users.

55. Describe Records Management

- Full version requires either:
    - Microsoft 365 E5 Compliance or
    - Microsoft 365 E5.
- Records Management starts with retention.
    - Create retention labels to mark content as a record.
        - Configure retention and deleting settings.
        - Set different retention periods when an event occurs.
    - Manage your requirements with a file plan.
- When content is labelled as a record:
    - Some actions are blocked
        - What you can do depends on whether a record has been locked
            - delete blocked, edit or move may be blocked, or

- if it is a regulatory record (even more restrictive – most actions are blocked, including removing or changing the label, editing contents and properties).

- Additional item activities are logged.
- You get proof of disposition when the items are deleted at the end of their retention period.

- Review, validate and export disposition items.
- Give appropriate personnel the "Records Management admin" role group.
- Common scenarios for records management:
  - Deleting and update records
  - Manually applying retain/delete actions.
  - Starting the retention period when an event occurs.
  - Restricting changing to policies for regulatory requirements.
  - Disposition reviews of content and records.
  - Monitoring how retain/delete are applied to items.

56. Describe Retention Polices, Retention Labels and retention label policies

- Data may need to be retained for a certain period of time, due to short-term eDiscovery holds or other legal reasons, or long-term regulatory reasons.
  - In America, the Sarbanes-Oxley Act, created after the collapse of Enron, may require retaining documents for 7 years.
  - Medical and legal industries may require longer for some data.
- However, do you need to keep everything?
  - If there is a lawsuit or security breach, the more data you have, the greater the potential discovery.
- What data do you need to retain?
  - Your employees should only have current and relevant data.
- Retention records can be applied in:
  - Exchange email
    - Deleted items will be retained in the "Recoverable Items" folder.
  - SharePoint site
  - OneDrive accounts

        - Deleted items for these two will be retained in the “Preservation Hold” library.
    - Microsoft 365 Groups
    - Skype for Business
    - Exchange public folders
    - Teams channel messages and chats
    - Yammer community messages and private messages
        - Deleted items for these two will be held in a hidden folder “Recoverable Items/SubstrateHolds”.
- Retaining data beats deleting data.
    - This includes holds for eDiscovery.
    - The longest time period wins.
    - For deletions, a retention label (on a specific item) beats a retention policy (over a folder).
    - Otherwise, the shortest delete time wins.
- Retention labels
    - Allow it to be applied manually.
    - Apply it automatically based on:
        - Sensitive information,
        - Specific keywords,
        - Trainable classifier.
    - Start the period from when the content was labelled in SharePoint/OneDrive.
        - For Calendar items, the period starts from when it was sent.
    - Start the period from when an event happens
        - Contracts expire, employees leave.
    - Apply a default retention label to a document library, folder or document set.
    - Only one retention label at once (multiple retention policies may be applied, though).

Describe insider risk capabilities in Microsoft 365/Purview

57. Describe Insider risk management solution

- One of the big risks for data is not from outside, but inside.

Describe insider risk capabilities in Microsoft 365/Purview

- Microsoft's Insider Risk Management is designed to deal with:
    - Data spillage,
    - Confidentiality violations,
    - Intellectual Property (IP) theft,
    - Fraud,
    - Policy violations,
    - Leaks of sensitive data,
    - Security violations, and
    - Regulatory compliance violations.
- To use Microsoft's Insider Risk Management solutions, you will need either:
    - Microsoft 365 E5 or A5 subscriptions, or
    - E3 or A3 subscriptions with either the Compliance add-on or the Insider Risk Management add-on.
    - You can also use the G5 or G3 with add-on subscriptions, but you will not get access to the Information Barriers solution.
- Insider risk management is based around:
    - Transparency
        - Having a balance between user's privacy and the risk to the company.
    - Configurable
        - Policies can be based on industry or location groups.
    - Integrated
        - Across Microsoft 365.
    - Actionable
        - Providing insights.
- Insider risk management uses:
    - Policies
        - Pre-built policies and policy conditions, such as:
            - Data theft by departing users
            - General data leaks or security policy violations

        - Data leaks or security policy violations by priority users or disgruntled users

- Alerts
    - Based on the policies, these alerts are displayed in the alerts dashboard, containing:
        - Status, Severity, Time detected, case and case status
- Triage
    - Any activities which need investigating are then assigned a “Needs review” status.
    - You can then review the cases and prioritise them by status, severity or time detected.
    - You can see the activities, other affected user activities, the alert severity, and review user information.
- Investigate
    - This builds a picture of cases or a particular case.
    - You can see user activity over time, content explorer (with data files and email messages), and your case notes.
- Action
    - How to resolve the case. It could be a reminder based on a template.
    - It may be that you need to share it with others in your company.
    - You may need to escalated it and use Advanced eDiscovery.
    - You could use your SIEM (seem) services via Office 365 Management APIs (Application Programming Interface).

58. Describe communication compliance

- Act on inappropriate messages in your company.
- Communication compliance can be used for:
    - Corporate policies
        - Acceptable use, ethical standards and other policies – for example, no harassment or threats.
    - Risk management
        - Minimise legal risk before it gets out of hand.
        - Scan messages for unauthorized communications or conflicts of interest.

- Regulatory compliance (reduce risk of fines).
    - Guard against potential money laundering, insider trading, collusion, or bribery activities.

- Process:
    - Enable permissions for communication compliance. You need to be subscribed into the:
        - the Communication Compliance role, or
        - the Communication Compliance Admin.
        - Global Administrators do not have access to this.
    - Enable the audit log.
    - Set up groups if necessary for communication compliance
    - Create then test communication compliance policies.
    - If necessary, create notice templates.
    - Investigate issues using alerts and reports.
    - Examine the message basics.
        - It may be a False Positive.
    - Examine the message details.
    - Decide on a remediation action:
        - Resolve, false positive, use Power Automate, tag, notify user, escalate to another reviewer, escalate for investigation in Advanced eDiscovery, improve classification, remove message in Teams.

59. Describe information barriers

- Information barriers restrict communication/collaboration between two groups. This can avoid conflicts of interest. [Ethics wall]
    - Stop combination of banking, investing and insurance services (Gramm-Leach-Bliley Act of 1999).
    - Brokers talking to people who are planning a takeover of another company. (Do you want to buy shares in this beforehand?)
    - Legal firms representing both sides in ongoing legal disputes.
    - Stop people with trade secrets (product development team) from communicating with others (except, say, a research team).
- Information barriers are supported in:

    - Microsoft Teams (chats and channels), SharePoint Online and OneDrive.
- In Teams, it can stop:
    - Searching for users,
    - Adding a member to a team,
    - Starting a chat session, group chat or inviting someone to join a meeting, sharing a screen, sharing files with other users.
    - Placing a call.
- In SharePoint Online and OneDrive, it can stop:
    - adding a member to a site,
    - accessing site or content by a user,
    - sharing site or content with another user,
    - searching a site.
- It does not stop emails.
- You need to have:
    - Microsoft or Office 365 Global Admin,
    - Compliance Administrator,
    - IB [Information Barriers] Compliance Management.
- Barriers are defined and managed using PowerShell cmdlets.

Describe resource governance capabilities in Azure

-. Describe the use of Azure Resource locks

- This is to prevent accidental changes.
- Locks can be applied at:
    - The subscription level,
    - The resource group level
        - This includes all resources, existing or new,
    - Individual resources.
- There are two types of locks:
    - CanNotDelete – write and read are allowed (with permissions).
    - ReadOnly – no deletions or changes allowed.

- ReadOnly may have side-effects.
    - You cannot start/restart a VM, for instance.
- Even owners cannot do the forbidden activities.
- To do deletions (or writing, in the case of ReadOnly), you need to remove the lock.
- ReadOnly Locks to a Resource Group prevents resources from being added/taken away.
- A resource can have multiple locks.
    - Locks are inheritable, and uses the most restrictive lock.

60. Define Azure Policy and describe its use cases

- Policies allow you to control or audit resources:
    - Stop something from happening, or
    - Report on it.
    - Resource consistency (cost), regulatory compliance (security).
- They are evaluated:
    - A resource is created, updated, or deleted in a scope with a policy assignment.
    - A policy or initiative is newly assigned to a scope or is updated.
    - During the standard compliance evaluation cycle, every 24 hours.
- It is assigned to one or more “scopes” :
    - The “scope” could be management groups, subscriptions or resource groups.
    - Its location is either a subscription or management group. It can only be used there.
- Example policies are:
    - Restrict what types of VMs or storage accountscan be created.
        - SKUs, regions
    - Require tags to be inherited from resource groups to resources.
    - Prevent some resources from being deployed.
- Responses (or “effects”) to non-compliant resources include:
    - Deny the resource change,
    - Log the change,
    - Alter the resource before/after the change,
    - Deploy related compliant resources

- Policy Initiatives are a set of Policies.
    - Azure Policies restrict what can be created, and how it can be created – business rules.
    - Role-based access control (RBAC) is focused on user actions. It restricts who can access objects, and with what permissions. RBAC can be tenant-based, resource-based, object-based.
    - Just because you have RBAC access doesn't override Azure Policies.

61. Describe what Azure Blueprints is

- Azure Blueprints are orchestrated:
    - Resource groups.
    - Azure Resource Manager templates, and
    - Role and Policy assignments.
- Blueprints should be:
    - Drafted – each component in a blueprint definition is an "artifact",
        - Blueprint can have "fill in the gaps" – this are called "parameters".
    - Published,
    - Assigned to a subscription or management group,
        - Locks will then be enforced.
    - Versioned (comment on changes).
- When no longer needed, it can be:
    - Unassigned from a subscription or management group:
        - It does not delete previously created resources; they remain in place.
        - Locks, however, are removed.
    - Deleted:
        - All assignments must be deleted first.
- More details: https://azure.microsoft.com/en-us/services/blueprints

62. Describe the Microsoft Purview unified data governance solution

- Data can be anywhere on-premises or in the cloud.
    - It is hard to make sure data is compliance if you don't know where it is.
    - Others may not know what data your company has access to.

- Azure Purview catalogs your data, whether it is on-premises, in a machine on the Internet, or in a cloud using Software-as-a-Service (SaaS).
    - It calls itself a Unified Data Governance solution. Cost from US$300 for 10 Gb of metadata.
- There are three main elements to the Azure Purview Studio:
    - Azure Purview Data Map captures metadata (information about data) from the various sources, by scanning and classifying it.
    - Azure Purview Data Catalog helps you to find data with classification or metadata filters. #Click on "Browse assets".
    - Azure Purview Data Insights allow you to see where sensitive data is and how it flows from one data source to another.
- Data can be classified into (for example):
    - Location (City, Country, Place),
    - Person First and Last Name,
    - Bank account, business, company, driver's license, medial accounts, passport, social security, tax file, and other identification numbers.
    - Date of Birth,
    - Email,
    - Ethnic group,
    - IP (Internet Protocol) Addresses.
- You can create scan rule sets which group together the classifications and file types.

Additional videos

These videos are no longer included in the current DP-900 exam.

-. Describe privileged access management

- Privileged Access Management is used in Microsoft 365 to limit access to admin functionality.
    - It is built on “zero standing privileges” to provide “just-in-time access”.
- It uses the Microsoft 365 Admin Center – https://admin.Microsoft.com
- You will need Microsoft 365 E5 or A5 subscription, or E3 or A3 subscription with the Microsoft compliance Add-on or Insider Risk Management add-on.
- First, you need to create an approver’s groups.

- go to Groups > Add a group

- Second – enable privileged access.
  - go to Settings > Org Settings > Security & Privacy > Privileged access
- Third – create an access policy.
  - Same place. Note the various tasks
    - This is the difference between PAM and PIM (Azure AD Privileged Identity Management).
      - PIM = access to Active Directory roles and groups.
      - PAM = task level.
- Fourth – Submit or approve Privileged access requests.
  - Same place.

-. Describe customer lockbox

- Not for scammers!
- Customer Lockbox ensures that Microsoft cannot access your content without your approval. You have to approve it.
- To turn this approval process on:
  - Go to https://admin.microsoft.com
  - Settings – Org Settings - Security & Privacy > Customer Lockbox > Edit,
- A several step process:
  - User experiences a problem.
  - They open a support request with Microsoft Support.
  - Microsoft needs to access your tenant to repair this issue.
  - Microsoft logs into the Customer Lockbox request tool.
  - Customer Lockbox sends the designated approver an email about this request.
  - User approves the request within 12 hours (or the request expires).
  - Microsoft receives the request approval, and now can fix the problem.
  - At the end of the time, the approval is revoked.
- Only for Microsoft for access to data.
  - PAM (Privileged Access Management) is for your organisation for tasks.

-. Describe the purpose of eDiscovery

- Electronic discovery, or eDiscovery, is for identifying electronic information for evidence in legal cases.
- eDiscovery tools in Microsoft 365 can be used to search through:
    - Exchange Online mailboxes,
    - Microsoft 365 Groups,
    - Microsoft Teams,
    - SharePoint Online
    - OneDrive for Business sites,
    - Skype for Business conversations,
    - Yammer teams.
- The Content Search tool is for searching mailboxes and sites.
- Core eDiscovery cases are used to identify, hold, and export content from mailboxes and sites.
    - add eDiscovery managers who can access the case
    - place an eDiscovery hold relevant content locations,
    - search for content, and export the search results from the case
- You can further manage custodians and analyze content by using the Advanced eDiscovery solution in Microsoft 365.
    - Workflow to preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations.
    - Allows legal teams manage custodians and the entire legal hold notification workflow to communicate with relevant custodians.
    - Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions) needed.

-. Describe the capabilities of the content search tool

- Content Search can search for emails, documents, and instant messaging conversations in your company in:
    - Exchange Online mailboxes
        - You can also preserve bcc recipients as well as to and cc.
    - SharePoint Online sites and OneDrive for Business accounts
    - Microsoft Teams

    - Microsoft 365 Groups
    - Yammer Groups
    - Skype for Business conversations.
- You search by going to Solutions – Content search.
    - You can choose a guided search (wizard),
    - New search, or
    - Search by Exchange ID List.
- You search:
    - Keywords to search
        - Message properties, such as sent/received dates,
        - Document properties like filenames,
        - A date a document was changed.
        - “Show keyword list” allows you to type a keyword in each row (using an OR).
        - You can get statistics about each keyword.
    - Conditions
        - Date, Sender/Author, Size, Subject/Title, Compliance Label
        - Can use After/Before/Between/Contains/Equals/ Greater/Less (and NOT).
    - Locations
        - All locations, or specific locations.
    - Add app content for on-premises users
        - This adds Teams content.
- Once the search has been done, you can open the query and see:
    - Summary – statistics for each type of content locations searched.
    - Queries – statistics about the search query:
        - the type of content location the query statistics are applicable to,
        - part of the search query the statistics are applicable to,
        - the number of the content locations that contain items that match the search query,

        - the total number and size and items that were found that match the search query.
    - Top locations
        - The top 1,000 locations are shown.
- Other actions:
    - You can also export the search results to csv.
    - You can search for and delete email messages.
    - "Save as" the search and change this second search.
- 1,000 mailboxes can be searched in around 1 minute, and 10,000 mailboxes in about 4minutes.
- With multiple searches selected, you can get the Search Statistics for the searches combined.
- For more advanced/repetitive searches, you can use PowerShell scripts.

-. Describe the core eDiscovery workflow

- Core eDiscovery allows you to search and export content in Microsoft 365 and Office 365.
- You can also place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams.
- You require a Microsoft/Office 365 E3 subscription or higher, or a E1 license with an add-on license.
- You will also need to add a eDiscovery Manager/Administrator.
    - The Manager can view and manage their cases.
    - The Administrator can view all cases, access and export case data for all cases, and manage any case after they add themselves as a member.
- You start a Core eDiscovery case by going to Solutions – eDiscovery – Core – Create a case.
    - You can subsequently add members and role groups and update the status (closed – deleted).
- You can also Open Case:
    - You can create an eDiscovery hold, preserving all content based on the location/query.
        - It may take up to 24 hours for it to take effect.
        - The query may specify locations, dates etc.
    - You can then search all "on hold" content (in addition to other locations).
    - Export and download search results.
        - Mailbox items are downloaded in PST or MSG files.

- SharePoint and OneDrive are downloaded in native format.
- A results.csv file and a Manifest file in XML format contains a catalog.

- Updating status.
    - eDiscovery holds are turned off for closed cases (but still held for 30 days).
    - Deleted cases cannot be reopened, and all searches and exports are also deleted.
    - Cases with holds cannot be deleted.

-. Describe the advanced eDiscovery workflow

- Advanced eDiscovery expands Core eDiscovery.
    - Identify persons of interest (“custodians”).
    - Apply holds to preserve data
    - Manage the process.
- Native search and collection for:
    - Teams, Yammer, SharePoint Online, OneDrive for Business, and Exchange Online
    - Reconstructs Teams conversations (instead of individual messages),
    - Collects cloud-based contents from email and Teams chats links.
    - Collects data from third-party sources (Facebook, Zoom) that has been imported and archived in Microsoft 365 using Data Connectors.
- Requires:
    - The organization to have:
        - Microsoft/Office 365 E5 subscription, or
        - Microsoft 365 E3 subscription with a E5 add-on.
    - Custodians must also have a E5 license.
    - Users of Advanced eDiscovery don’t need the E5 license.
- Add eDiscovery permissions:
    - Needs an eDiscovery Manager/Administrator.
- Create a case:
    - Add custodians and non-custodial data.
    - A custodian is someone who has administrative control of a relevant document or electronic file.

- Custodian data is reindexed.
- You can place a hold on custodian data.

- Collect relevant content from data sources.
  - Build search queries.
  - View collection statistics.
- Save the collection to a review set.
- Review and analyze data in a review set.
  - View documents.
  - Create queries and filters.
  - Create and use tags.
  - Annotate and redact documents.
  - Analyze case data.
- Export and download case data.

-. Describe the core audit capabilities of M365

- You need a E3/G3 or E5/G5 license to use the audit log.
- The audit log may need to be turned on before you can use it.
- It may take up to 30 minutes or 24 hours (depending on the service) after an event occurs for there to be an audit log record.
- The core audit capabilities in Microsoft 365 include:
  - User activity in:
    - SharePoint Online and OneDrive for Business
    - Exchange Online (Exchange mailbox audit logging)
  - Admin activity in:
    - SharePoint Online
    - Azure Active Directory (the directory service for Microsoft 365)
    - Exchange Online (Exchange admin audit logging)
    - Briefing email and MyAnalytics
  - User and admin activity in:
    - Power BI

        - Microsoft Teams
        - Dynamics 365
        - Yammer
        - Microsoft Power Automate
        - Microsoft Stream
        - Microsoft Power Apps
        - Microsoft Forms
        - for sensitivity labels for sites that use SharePoint Online or Microsoft Teams
    - Analyst and admin activity in Microsoft Workplace Analytics
- To run an audit log search:
    - Go to Solutions – Audit.
    - Configure the activities.
    - Start date and end date.
        - You can specify up to 90 days.
        - If you don't have a Microsoft/Office E5 license or a suitable E5 add-on license, audit records are only retained for 90 days.
    - Users
    - File, folder or site
        - If you specify a URL, use the full URL path.
    - Click search
- You will see the latest 5,000 results.
- You will see:
    - Date
    - IP Address
    - User or service account
    - Activity
    - Item, and
    - Detail.
- You can then filter or export this list.

- Exports to a csv file.
- This will export up to 50,000 results, not just 5,000 results.

-. Describe purpose and value of Advanced Auditing

- This needs:
  - an Office/Microsoft 365 E5 license, or
  - Microsoft 365 E5 Compliance or Microsoft 365 E5 eDiscovery and Audit add-on license.
- Advanced Audit keeps:
  - All Exchange, SharePoint, and Azure Active Directory audit records for one year.
  - Additionally, you can expand this to 10 years.
  - This could help with long-running investigations and respond to regulatory, legal, and internal obligations.
  - Retaining audit logs for 10 years requires an additional add-on license.
- Advanced Audit adds the additional events:
  - MailItemsAccessed
    - When is mail data accessed? Can help identify data breaches and determine the scope of messages that may have been compromised. Doesn't track whether emails were actually read.
  - Send
    - When you send, reply or forward an email.
    - Includes the metadata (when, subject line, message ID, are there attachments), but not the email itself.
  - SearchQueryInitiatedExchange
    - Some used the Outlook search bar to search for items
      - Outlook (desktop client)
      - Outlook on the web (OWA)
      - Outlook for iOS
      - Outlook for Android
      - Mail app for Windows 10
  - SearchQueryInitiatedSharePoint
    - SharePoint to search for items.

- Home sites
- Communication sites
- Hub sites
- Sites associated with Microsoft Teams

- Has better speeds using Office 365 Management Activity API (Application Programming Interface)
    - Previously restricted (throttled) per publisher.
    - Now restricted by tenant- 2,000 requests minimum per minute. More licenses and an E5 license will get better speed.
    - Caps are needed to protect the service health.

Additional videos – Describe endpoint security with Microsoft Intune

-. Describe what Intune is

- Microsoft Intune focuses on:
    - Mobile Device Management (MDM) and
    - Mobile Application Management (MAM).
- You can control settings for your organisation's iPhone, iPads and Android devices, and Windows and Mac computers.
    - It is part of Microsoft's Enterprise Mobility + Security (EMS) suite.
    - It integrates with Azure Active Directory (Azure AD) to control access, and Azure Information Protection for data protection.
    - You can specify specific policies.
    - You can also deploy Microsoft 365 Apps such as Teams and OneNote to devices.
    - Control how users access and share devices.
    - Impose security requirements, and install apps.
- For company devices:
    - Organisations could have full control of settings, features and security.
    - See what devices are enrolled.
    - Push certificates for WiFi or VPN.
    - See reports on compliance.
    - Wipe devices in full or in part if needed.

- For personal devices (Bring Your Own Device) and company devices:
    - Use Azure AD to isolate organization data from personal data.
    - Restriction actions, such as copy/paste, save, view.

-. Describe endpoint security with Intune

- Microsoft Endpoint Manager admin center:
    - https://endpoint.microsoft.com
- Intune for Education:
    - https://intuneeducation.portal.azure.com
- Home
- Dashboard
- Devices
    - You can enroll Windows, iOS, macOS and Android devices.
    - Show how to enroll Windows, iOS (macOS is similar) and Android devices.
    - Create a new compliance policy, then a configuration policy for Windows and iOS users.
- Apps
    - Windows – Add – Windows 10 Microsoft 365 Apps
- App selective wipe
- Reports
    - Device compliance
    - Group policy analytics
    - Windows updates
    - Cloud attached devices
- Users
- Groups
- Tenant administration (advanced)

-. Describe the endpoint security with the Microsoft Endpoint Manager admin center

- Antivirus
    - Antivirus policies help security admins focus on managing antivirus settings for managed devices. Uses Microsoft Defender for Endpoint.
        - Real-time protection

        - Scan

- Disk encryption
    - Endpoint security Disk encryption profiles focus on only the settings that are relevant for a devices built-in encryption method, like FileVault or BitLocker.
        - Demo
- Firewall
    - Configure a device's firewall for devices that run macOS and Windows 10.
        - No need to demo.
- Endpoint detection and response
    - If you integrate Microsoft Defender for Endpoint with Intune, manage the endpoint detection and response settings.
        - No demo
- Attack surface reduction
    - When Defender antivirus is in use on your Windows 10 devices, use Intune endpoint security policies for Attack surface reduction to manage those settings for your devices.
        - Demo Attack surface reduction rules.
- Account protection
    - Account protection policies help you protect the identity and accounts of your users.
        - quick demo
- Conditional Access
    - As seen before.
        - Click on "Grant".