Microsoft SC-900 *Cheat Sheets*

Good luck on your exam!

SC-900 CheatSheet

Zero-Trust Model operates on the principle of "**trust no one, verify everything.**"
Micosoft's Zero Trust Model has **3 Principles** and **6 Pillars**

- 3 Principles
  - **Verify Explicitly** - Always authenticate and authorize based on all available data points
  - **Least Privileged Access** - Limit user access with **Just-In-Time**, **Just-Enough-Access,** risk-based adaptive policies, and data protection
  - **Assume Breach** - Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses
- 6 Pillars
  - **Identities** - Verify and secure each identity with strong authentication across your entire digital estate
  - **Endpoints** - Gain visibility into devices accessing the network. Ensure compliance and health status before granting access.
  - **Apps** - Discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, and monitor and control user actions.
  - **Data** - Use intelligence to classify and label. Encrypt and restrict access via org policies from perimeter-based data protection to data-driven protection.
  - **Infrastructure** - Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior, and employ least privilege access principles.
  - **Networks** - Ensure devices and users aren't trusted just because they're on an internal network. Encrypt all internal communications, limit access by policy, and employ micro-segmentation and real-time threat detection

Zero Trust Assessment Tool - A free tool to assess your organization degree of adoption toward a Zero-Trust along with improvements
Microsoft Security Services Map (MSSM) – a tabular visualization to introduce you to security services in Azure
Shared Responsibility Model describes what the Customer and Azure is responsible for related to cloud resources

- **Software as a Service (SaaS)** — software that use in the cloud eg. Microsoft 365, Skype, Dynamics CRM
- **Platform as a Service (PaaS)** — deploy apps without worrying about underlying infrastructure. Azure App Services
- **Infrastructure as a Service (IaaS)** — basic building blocks of cloud IT eg. Storage, Compute, Databases, Networking
- **On-Premise** — datacenter owned, operated and maintained by customer
- Regardless of the type of deployment, the following responsibilities are always retained by Customer: **Data, Endpoints, Account, Access management**

SC-900 CheatSheet

Defense in Depth is 7 layers of security used by Microsoft:

1. **Data** - access to business and customer data, and encryption to protect data.
2. **Application** - applications are secure and free of security vulnerabilities.
3. **Compute** - Access to virtual machines (ports, on-premise, cloud)
4. **Network** - limit communication between resources using segmentation and access controls.
5. **Perimeter** - distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
6. **Identity and access** - controlling access to infrastructure and change control.
7. **Physical** - limiting access to a datacenter to only authorized personnel.

Confidentiality, Integrity, and Availability (CIA) triad is a model describing the foundation to security principles and their trade-off relationship.

- **Confidentiality -** protect our data from unauthorized viewer
- **Integrity -** maintaining and assuring the accuracy and completeness of data over its entire lifecycle
- **Availability -** information needs to be made be available when needed

Threat - potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application

4 Types of Common threats:

1. **Dictionary Attack** Attacker attempts to steal an identity by brute forcing into a target accounts by enumerating over a large number of known passwords.
2. **Disruptive attacks** An attack which attempts to disrupt a computer system or network for various reasons: DDoS, coin miners, rootkits, trojans, worms etc….
3. **Ransomware** A type of malicious software (malware) that when installed holds data, workstation or a network hostage until the ransom has been paid.
4. **Data Breach** When a malicious actor gains unauthorized access to a system in order to extract private data.

Vulnerability - a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

Cryptography - The practice and study of techniques for secure communication in the presence of third parties called adversaries

Encryption - The process of encoding (scrabbling) information **using a key** and a **cypher** to store sensitive data in an unintelligible format as a means of protection. An encryption takes in plaintext and produces **ciphertext**.

Cyphers - An algorithm that performs encryption or decryption. Cipher is synonymous with “code”

Ciphertext - Ciphertext is the result of encryption performed on plaintext via an algorithm

SC-900 CheatSheet

Exam Pro

cryptographic key - A key is a variable used in conjunction with an encryption algorithm in order to encrypt or decrypt data.
symmetric encryption The same key is used for encoding and decoding. eg **Advanced Encryption Standard (AES)**
asymmetric encryption Two keys are used. One to encode and one to decode eg. **Rivest–Shamir–Adleman (RSA)**
hashing function A function that accepts arbitrary size value and maps it to a fixed-size data structure. Hashing is a **one-way process** and is **deterministic**
Hashing Passwords Hashing functions are used to store passwords in database so that a password does not reside in a plaintext format.

- Popular hashing functions are **MD5, SHA356 and Bcrypt**

Salting Passwords - A salt is a random string not known to the attacker that the hash function accepts to mitigate the deterministic nature of hashing functions
Digital signature - A mathematical scheme for verifying the authenticity of digital messages or documents.

- A Digital signature gives us **tamper-evidence** .
- There are three algorithms to digital signatures:
    1. **Key generation** – generates a public and private key.
    2. **Signing** - the process of generating a digital signature with a **private key** and inputted message
    3. **Signing verification –** verify the authenticity of the message with a **public key**
- ssh-keygen is a **well known command** to generate a public and private key
    - RSA algorthim is most commonly used with ssh-keygen

Code Signing - When you use a digital signature to ensure **computer code** has not been tampered
Encryption In-Transit Data that is secure when moving between locations Algorithms: **TLS, SSL**
Encryption At-Rest Data that is secure when residing on storage or within a database. Algorithms: **AES, RSA**
Multi-Factor Authentication (MFA) A security control where after you fill in your username/email and password **you use a second device** to confrm

- MFA **protects** against people who have stolen your password.

Log Management - Focus on simple collection and storage of log messages and **audit trails**
Event logs - systems and applications generate events which are kept in **event logs**.
Security information management (SIM) - Long-term storage as well as analysis and reporting of log data
Security event management (SEM) - Real-time monitoring, correlation of events, notifications and console views
Security information and event management (SIEM)?

- Combines SIM and SEM to **provides real-time analysis of security alerts** generated by network hardware and applications

SC-900 CheatSheet

Exam Pro

Security Orchestration Automated Response (SOAR) **collects data about security threats** and **respond to security events** without human assistance

- **Playbooks** (repeatable, automated processes to replace manual processes

Extended detection and response (XDR) **is cross-layered detection and response security system**

- uses a **holistic approach** to detect and respond to threats that would normally evade detection in a single-vector solution **by collaborating multiple data sources into a multi-vector solution**

Advanced Persist Threat (APT) will breach a security perimeter and take up residence within a network to steal as much data as it can over a long period of time. APT are threat actors that engineer malware engineered for a particular target. APTs are slow **acting and stealthy**

Endpoint detection and response (EDR) combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

Cloud access security broker (CASB) **sits between cloud service users and cloud applications**, and **monitors all activity and enforces security policies**

Malicious Actors *aka Threat Actor, Attacker*

- a person, machine or entity for an event or incident that impacts, or has the potential to impact, the safety or security of another entity

Inventory up-to-date list of assets (software and hardware) for your organization can be accompanied with additional metadata

Attack Vectors - The method that a malicious actor uses to breach or infiltrate your network. They could target infrastructure or a human for weakness

Attack Surface - The sum of the attack vectors.

Security Controls - safeguards or countermeasures to avoid, detect, counteract, or minimize security risks

Security Posture - A formula to determine the overall effectiveness of a companies security overall defense

- **Security Score** – the outputted result for a security posture. Often represented as a percentage (%)

Cloud Security Posture Management (CSPM) assesses your systems and **automatically alerts security staff** in your IT department when a vulnerability is found

Just-in-time (JIT) giving access to resources only during the time when needed reducing the surface attack based on range of time access

Just Enough Privilege (JeP) giving access to only the specific actions (API calls) reducing the surface attack by providing least-permissive permissions

Ingress traffic traffic that is entering a network boundary

Egress traffic traffic that is exiting a network boundary

Shadow IT is a **business agility process** where **departments can purchase and provision their own IT resources** *without the approval* of the organization centralized IT department

SC-900 CheatSheet

Investigation is the act **of** gathering evidence from digital systems to **uncover malicious intent** or reduction in a security posture
Remediation the action of remedying something **to prevent or revert a disaster**

- the act of changing a resource back to the desired state or a state that does not causes problems

Automated Investigation - a service which uses an inspection algorithms that **triggers an alert** which in turn creates an incident
Automated Remediation - a service which **watches for types of incidents and matches it with a remediation action** eg. shut off server
Automated Investigation and Remediation (AIR) - a unified service that does both Automated Investigation and Remediation
Threat analysis is the **practice of mitigating possible threats** via threat modeling
threat modelling is a structured process for identifying attackers and cataloging possible threats

- STRIDE — is that threa model developed by Microsoft in 1999
  - **S**poofing — illegally accessing and then using another user's authentication information
  - **T**ampering — malicious modification of data
  - **R**epudiation — llegal operation in a system that lacks the ability to trace the prohibited operation
  - **I**nformation Disclosure — exposure of information to individuals who are not supposed to have access to it
  - **D**enial of Service — deny service to valid users
  - **E**levation of Privilege — unprivileged user gains privileged access
- **Microsoft Threat Modeling Tool** makes threat modeling easier for all developers through a standard notation for visualizing system components, data flows, and security boundaries

Intrusion Detection System (IDS) **monitors** a network or system for malicious activity or policy violations
Intrusion Protection System (IPS) **restricts** access to a network or systems mitigate malicious activity or policy violations
Intrusion Detection System and Intrusion Protection System (IDS/IPS) is the combination of an IDS and IPS.
MITRE ATT&CK - globally-accessible **knowledge base of adversary tactics and techniques** based on real-world observations

- a foundation for the **development of specific threat models and methodologies** in the private sector, in government, and in the cybersecurity product and service community

SC-900 CheatSheet

Microsoft has 6 privacy principles

1. **Control -** We will put you in control of your privacy with easy-to-use tools and clear choices.
2. **Transparency -** We will be transparent about data collection and use so you can make informed decisions.
3. **Security -** We will protect the data you entrust to us through strong security and encryption.
4. **Strong legal protections -** We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.
5. **No content-based targeting -** We will not use your email, chat, files or other personal content to target ads to you.
6. **Benefits to you -** When we do collect data, we will use it to benefit you and to make your experiences better.

Security perimeters are barriers or built fortifications to either keep intruders out or to keep captives contained within the area the boundary surrounds.

- A cloud network would have a protocol, software and or hardware as its security perimeter

Entrypoint is the point of entry to cross a security perimeter

Access Controls (AC) is security mechanism at the point of access that that allows or denies access

Authorization is permission to access a resource

Primary Security Perimeter – the idea of treating Identity as the first security perimeter influenced by the Zero-Trust model

- Azure Active Directory would be Microsoft's tool of defense for the Primary Security Perimeter

Identity Provider (IdP) a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to applications within a **federation** or distributed network

Federated identity is a method of linking a user's identity across multiple separate identity management systems

OpenID open standard and decentralized authentication protocol. Eg be able to login into a different social media platform using a Google or Facebook account

- *OpenID is about providing who are you*

OAuth2.0 industry-standard protocol for authorization OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers.

- *Oauth is about granting access to functionality*

SAML is an open standard for exchanging authentication and authorization between an identity provider and a service provider.

- An important use case for SAML is Single-Sign-On via web browser.

SC-900 CheatSheet

Exam Pro

Azure Active Directory (Azure AD) is Microsoft's cloud-based **identity and access management service**, which helps your employees sign in and access resources

Azure Active Directory comes in four editions

1. **Free** MFA, SSO, Basic Security and Usage Reports, User Management
2. **Office 365 Apps** Company Branding, SLA, Two-Sync between On-Premise and Cloud
3. **Premium 1** Hybrid Architecture, Advanced Group Access, Conditional Access
4. **Premium 2** Identity Protection, Identity Governance

Azure AD can **authorize** and **authenticate** to multiple sources.

- To your on-premise AD (Azure AD Connect)
- To your web-application (App Registrations)
- Allow users to login with their IpD eg. Facebook or Google (External Identities)
- To Microsoft 365 or **Microsoft Azure**

App Registrations allows developers to integrate web-applications to use Azure AD authenticate users and request access to user resources such as email, calendar, and documents

External Identities in Azure AD, allow people outside your organization to access your apps and resources, while letting them sign in using whatever identity they prefer.

- Your partners, distributors, suppliers, vendors, and other guest users can **"bring their own identities"**.
- There are two types of External Identities for Azure AD
    - **B2B** allows external businesses to authenticate with your app
    - **B2C** allows customers to authenticate with your app
        - customer identity access management (CIAM) solution.

Most popular IpD support: Microsoft account, LinkedIn, Twitter, Github, SalesForce

Service principal is a **security identity** used by applications or services to **access specific Azure resource**

Managed identities are used to manage the credentials for authenticating a cloud application with an Azure service

- Using a managed identity, you can **authenticate to any service** that supports Azure AD authentication **without having credentials in your code**.
- There are two types of managed Identities
    1. **System-assigned** An identity in tied to the lifecycle of a service instance. Deleting the resource also deletes the identity
    2. **Used-Assigned** An identity assigned to one or more instances of services. The identity needs to be separately deleted

SC-900 CheatSheet

Exam Pro

Device identity management is the management of **physical devices** such as **phones, tablets, laptops and desktop** computers, that are granted access to company resources such as Printers, Cloud Resources via **device-based Conditional Access**.

There are **3 ways** to get devices into Azure AD

1. Azure AD Registered **personally** owned or mobile devices,And signed in with a **personal** Microsoft or local account

2. Azure AD Joined owned by an **org,** And signed in with an Azure AD account belonging to the organization. They exist **only in the cloud**.

3. Hybrid Azure AD Joined owned by an **org,** signed in with an Active Directory Domain Services account. They exist **in the cloud and on-premises**

Microsoft Authenticator is a mobile application for **secure sign-ins** for all your online accounts using: MFA, Passwordless, password autofill

Mobile Device Management (MDM) - control the entire device, can wipe data from it, and also reset it to factory settings

Mobile Application Management (MAM)- Publish, push, configure, secure, monitor, and update mobile apps for your users

MDM and MAM is managed via **Microsoft Intune**

- To use Microsoft Intune you have to upgrade to **Azure AD Premium 2**
- Microsoft Intune is part of **Microsoft Endpoint Manager**

Windows Hello Gives Windows 10 users **an alternative way** to log into their devices and applications using: fingerprint, iris scan, facial recognition

- Windows Hello uses a PIN backed by hashing
- Windows Hello for Business uses a PIN backed by asymmetric (public/private key) or certificate-based authentication

Azure AD Connect is a **hybrid service** to **connect your on-premise Active Directory to your Azure Account**

- Azure AD Connect allows for seamless **Single Sign On** from your on-premise workstation to Microsoft Azure
- Three methods of authentication
    - **Password hash synchronization** — sign-in method, synchronizes a hash of a users on-premises AD password with Azure AD
    - **Pass-through authentication** — sign-in method, allows users to use the same password on-premises and in the cloud
    - **Federation integration** — hybrid environment using an on-premises AD FS infrastructure, for certificate renewal

Self-service password reset (SSPR) allows users to **change or reset their password, without the help from an administrator**,

- Self-service password scenarios: **Password change** , **Password reset, Account unlock**

SC-900 CheatSheet

Password Spraying - A type of brute force dictionary attack. Avoids password lockout cooldowns by spreading passwords across multiple accounts before enumerating

Azure AD Password Protection is a feature of Azure AD to protect your passwords from identity attacks such as **password spray attacks**.

- **Global banned password list** password list with known weak passwords is automatically updated and enforced by Microsoft.
- **Custom banned password lists** Admins can also create custom banned password lists to support specific business security needs.
- Banned password lists are a feature of **Azure AD Premium 1 or 2.**
- Azure AD Password Protection can be integrated to on-premise Active Directory environments

Emergency access **accounts prevent admins from being accidentally locked** out of Azure AD

- You can mitigate the impact of accidental lack of administrative access by creating **two or more** emergency access accounts in your organization

Azure Active Directory MFA methods:

- **SMS -** A text message is sent to your phone with a PIN
- **Voice call -** A phone call from a synthesized voice speaks a PIN
- **Microsoft Authenticator app-** You press a button in the app and it authorizes you
- **OATH Hardware token -** You touch your security key and it authorize you by generating and entering a PIN

Biometrics are body measurements and calculations related to human characteristics e.g. Fingerprint, Iris recognition, typing rythmn, voice

Fast Identity Online (FIDO) Alliance An open industry association whose mission is to **develop and promote authentication standards** that **help reduce the world's over-reliance on passwords**

- FIDO Universal Second Factor (FIDO U2F)
- FIDO Universal Authentication Framework (FIDO UAF)
- Client to Authenticator Protocols (CTAP)
- CTAP is complementary to the W3C's Web Authentication (WebAuthn) specification; together, they are known as **FIDO2**

What is a Security Key? A secondary device used as second step in authentication process to gain access to a device, workstation or application.

Open Authentication (OATH) *not to be confused with Oauth* is an open standard that specifies how time-based, one-time password (TOTP) codes are generated

Time-based One-time Password (TOTP) is a computer algorithm that generates a one-time password (OTP) which uses the current time as a source of uniqueness

SC-900 CheatSheet

Exam Pro

Passwordless authentication is **something you have** + **something you are** or **something you know**

- Something you have: Windows 10 Device, Phone, Security Key
- Something you are: Biometric, Fingerprint
- Something you know: PIN
- Solutions for Passwordless Authentication include: Windows Hello for business, Microsoft Authenticator App, FIDO2 Security Keys

Azure AD Conditional Access provides an extra layer of security before allowing authenticated users to access data or other assets.

- Conditional Access is implemented through **Conditional Access policies**
    - **Conditional Access policy** analyses uses Signals and Common Decisions:
        - Signals: user, location, device, application …
        - Common Decisions: Block Access, Grant Access

Security Principal represents the identities requesting access to an Azure resource such as:

- **User** An individual who has a profile in Azure Active Directory
- **Group** A set of users created in Azure Active Directory.
- **Service Principal** A security identity used by applications or services to access specific Azure resources.
- **Managed identity** An identity in Azure Active Directory that is automatically managed by Azure.

Scope is the **set of resources** that access for the Role Assignment applies to Scope Access Controls at the Management, Subscription or Resource Group level.

A Role Definition is a collection of permissions.

- A role definition lists the operations that can be performed, such as **read, write, and delete**.
- Roles can be high-level, like owner, or specific, like virtual machine reader.

Azure AD roles are used to **manage Azure AD resources** in a directory such as:

- create or edit users
- assign administrative roles to others
- reset user passwords
- manage user licenses
- manage domains.

SC-900 CheatSheet

Exam Pro

Human capital management (HCM) - The practice of managing people as resources within an organization
HCM system - An application that provide **administrative** and **strategic** support around human resources
Identity lifecycle management is the **foundation** for Identity Governance The goal is to achieve a balance between **productivity** and **security**

- Microsoft Identity Manager

Access lifecycle is the process of managing user access throughout their lifecycle in an organization

- Dynamic Groups, Access Reviews, Entitlement Management

Privileged Access Lifecycle is the management of fine-grade permissions over the life-cycle of a user within an organization

- Privileged Identity Management (PIM)

Azure AD Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating: **access request workflows, access assignments, reviews, expiration**
Azure AD Privileged Identity Management (PIM) is an Azure AD service enabling you to **manage, control, and monitor access to** important resources in your org
Azure AD Identity Protection is an Azure AD that's you to **detect, investigate, remediate and export** for future analysis **identity-based risks**.
Network security group (NSG) **filter network traffic** to and from Azure resources in a VNet
DDoS (Distributed Denial of Service) Attack - A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic

- Most frequent types of DDoS attack: Volumetric, Protocol and Application Layer attacks

Azure offers **two tiers** of DDoS Protection

- **Basic:** Free, Already turned on protect Azure's global network
- **Standard** Starting at $2,994/month, Metrics, Alerts, Reporting, DDoS Expert Support, Application and Cost Protection SLAs

Azure Firewall is a managed, **cloud-based network security service** that protects your Azure Virtual Network (vNETs) resources.
Azure Bastion is an **intermediate harden instance** you use to connect to your target server via SSH or RDP It will provision a web-based RDP client or SSH Terminal
Web Application Firewall (WAF) is a service that protects web-applications communication on the application layer (layer 7) by **analyzing incoming HTTP requests**.
Azure WAF is a WAF offering that can be can be attached to:

- Azure Application Gateway (an application load balancer)
- Azure Front Door (CDN)
- Azure Content Delivery Network (CDN)

SC-900 CheatSheet

Azure provides a variety of encryption methods:

- **Azure Storage Service Encryption (SSE)**
  - protect data at rest by automatically encrypting before persisting it to: Azure-managed disks, Azure Blob Storage, Azure Files, Azure Queue Storage
  - It also is used to decrypt data on retrieval
- **Azure Disk Encryption (ADE)**
  - encrypt Windows and Linux IaaS virtual machine disks
  - Uses BitLocker feature on Windows or DM-Crypt on Linux

Transparent data encryption (TDE) **encrypts data-at-rest** for Microsoft Databases. can be applied to: SQL Server, Azure SQL Database, Azure Synapse Analytics

Azure Key Vault helps you **safeguard** **cryptographic keys and other secrets** used by cloud apps and services

- **Secrets Management** store and tightly control access to **tokens, passwords, certificates, API keys, and other secrets**
- **Key Management** create and control the **encryption keys** used to encrypt your data
- **Certificate Management** easily provision, manage, and deploy public and private **SSL certificates** for use with Azure and internal connected resources.
- **Hardware Security Module** secrets and keys can be protected either by software or **FIPS 140-2 Level 2** validated HSMs

Azure Security Benchmark includes a collection of high-impact security recommendations you can use to help secure the services you use in Azure.

- It includes **Security Controls** and **Service Baselines**

Security controls recommendations are generally applicable across your Azure tenant and Azure services

Service baselines apply the controls to individual Azure services to provide recommendations on that service's security configuration

Azure Security Center is a **unified infrastructure security management system** It strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud.

- **Regulatory Compliance Dashboard** shows you your **compliance posture** for a set of supported standards and regulations, based on continuous assessments of your Azure environment
- **Security Score** - continually assesses your resources, subscriptions, and organization for security issues and produces a single aggerated value
- **Recommendations –** a grouping of security controls to improve your security score

SC-900 CheatSheet

Azure Defender provides **advanced protection** for your Azure and on-premise workloads

- **Azure Defender** can be found in the **Azure Security Center**
- **Coverage** lets **see the resources types** that are in your subscription and eligible for protection by Azure Defender
- **Security Alerts** describe **details of the affected resources**, suggested **remediation** steps, and in some cases an option to trigger a logic app in response
- **Insights** is a **rolling pane of news**, suggested reading, and **high priority alerts**
- **Network map** provides a graphical view with security overlays giving you recommendations and insights for hardening your network resources

Advanced Protection within Defender are additional security features that is driven by analytics

Azure Defender has **Hybrid Support:** can protect virtual machines residing in other cloud service providers e.g. Amazon Web Services (AWS) and Google Cloud Platform (GCP) via **Azure Arc**

Azure Sentinel is a scalable, cloud-native:

- **security information event management (SIEM)**
- **security orchestration automated response (SOAR)**
- alert detection, threat visibility, proactive hunting, threat response

Microsoft 365 *(formally Office 365) e.g. M365* is a **suite of business software** packaged a as SaaS offering

Microsoft 365 Defender is a **unified pre- and post-breach enterprise defense suite** that natively coordinates

- responses: **detection, prevention, investigation**
- across: **endpoints, identities, email, applications**

to provide integrated protection against sophisticated attacks

SC-900 CheatSheet

Exam Pro

Microsoft Defender is composed of the following services:

- Microsoft Secure Score
  - a representation of your organization's **security posture**, and your opportunity to improve it via **Improvement Actions**
- **Microsoft Defender for Endpoint**
  - **M365 Endpoints** are the set of destination IP addresses, DNS domain names, and URLs for Microsoft 365 traffic on the Internet
  - an enterprise endpoint security platform designed to help enterprise networks **prevent, detect, investigate, and respond** to **advanced threats**
- **Microsoft Defender for Office 365**
  - protects against advanced threats by email messages, links (URLs), and Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients
  - **Exchange Online Protection (EOP)** is cloud-based filtering service that protects your organization **against spam, malware, and other email threats**
- **Microsoft Defender for Identity**
  - a cloud-based security solution that leverages your on-premises Active Directory signals **to identify, detect, and investigate** advanced threats, compromised identities, and malicious insider actions directed at your organization
- **Microsoft Cloud App Security**
  - **a Cloud Access Security Broker (CASB)** that sits **between the user and the cloud service provider** to gatekeep access in real-time to cloud resources
  - MCAS is built on-top of the **4 principles** of the **Microsoft Cloud App Security Framework**:
    1. **Discover and control the use of Shadow IT**
    2. **Protect your sensitive information anywhere in the cloud**
    3. **Protect against cyberthreats and anomalies**
    4. **Assess the compliance of your cloud apps**

SC-900 CheatSheet

Exam Pro

Microsoft Intune and **Configuration Manager** was merged into a single service called **Microsoft Endpoint Manager**

- **Microsoft Intune** Used for managing the security of mobile devices
- **Configuration Manager** Used to manage desktops, servers and laptops

Compliance - conforming to a rule, such as a **specification, policy, standard or law**

Regulatory compliance - an organization that take effort to comply with relevant **laws, policies, and regulations**

Compliance controls - internal control mechanisms that need to be in place to detect, prevent, and correct compliance issues

Azure Trust Center - A public-facing website portal providing easy access to **privacy** and **security** and **regulatory compliance** information.

- **Audit Reports** independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements

Compliance Manager At-a-glance summary of the shared responsibility model for Microsoft and your Organization

- Microsoft Trust Center – Compliance Manager (Classic)
- M365 Compliance Center – Compliance Manger

SC-900 CheatSheet

Exam Pro

Microsoft 365 compliance center provides easy access to the data and tools you need to manage to your organization's compliance needs.

- Sensitive Information Types - **classifications (categories) of data by sensitivity, hundreds of built-in information types e.g. EU passport number**
- Trainable Classifier
  - **Pre-Trained Classifiers** Ready to use classifiers **with five pretrained classifiers**. (Resumes, Source Code, Harassment, Profanity, Threat)
  - **Custom Trainable Classifiers** When you have your own kind of documents. specific business documents. You'll have to provide training data.
- Compliance Manager
- Audits
- Activity Alerts
- Data Classification
  - **Microsoft Information Protection (MIP)** is a collection of concepts to help **you discover, classify, and protect** sensitive information wherever it lives or travels eg: (Know your data, Protect your data, Prevent Data Loss, Govern your Data)
  - **Content Explorer** - Drill down to find emails (Microsoft Exchange) and documents (OneDrive and SharePoint) that's been labeled based on
    - Sensitive info types, labels, Retention labels
  - **Activity Explorer** Helps discover **which file labels were changed**, and **which files were modified**.

  Sensitivity Labels allow you to **apply a label to your documents or emails**, The most common way is via built-in dropdown within Office 365 products
    - **Content markings** watermarks, warnings are applied to the header and footer of a document e.g. "Highly Confidential"
    - **Encryption** Apply encryption and specific which users and groups may decrypt and other fine-tune permissions
    - In order to use Sensitivity labels they need to be **published** along with a **label policy**
  - **Retention Labels** ensures **data is held for a specific duration** to meet a regulatory compliance or industry best practices.
    - **Retention Policies** are used to **assign the same retention settings to content at a site level or mailbox level**
- **Insider Risk Management** - minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization
- **Records Management** - helps organization meeting regulatory compliance (legal requirements) by managing information throughouts it lifecycle
- **Data Loss Protection (DLP)** policies prevent data loss via DLP policies
- **Communication Compliance** that helps **minimize communication risks** by helping you detect, capture, and act on inappropriate messages in your organization.
- **Information Barriers** are policies that admins can configure to **prevent individuals or groups from communicating with each other**

SC-900 CheatSheet

M365 Privileged Access Management protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration setting

- **just-in-time access rules** are implemented for tasks that need elevated permissions and lets an organization operate with **zero standing access**

Customer Lockbox **protects sensitive data when working with Microsoft Support Engineers** by enforcing a **request system** to view custom private information to resolve a M365 related issue.

M365 Electronic discovery (eDiscovery) the process of identifying and delivering electronic information that can be used as evidence in legal cases.

Microsoft 365 provides the following eDiscovery tools:

- **Content search** – running a search across content
- Holds – holds onto data as long as the hold our data source exists
- **Core eDiscovery** – A workflow to search and export content
- **Advanced eDiscovery** - end-to-end workflow to preserve, collect, review, analyze, and export content for internal or external investigation

M365 audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention required to conduct an investigation

Resource Locks: As an admin, you may need to **lock a subscription, resource group, or resource** to **prevent other users from accidentally deleting or modifying critical resources.**

- **ReadOnly (Read-only)** authorized users can read a resource, but they can't delete or update the resource
- **CanNotDelete (Delete)** authorized users can still read and modify a resource, but they can't delete the resource.

Resource tag is a **key and value pair** that you can assign to azure resources.

Azure Blueprints enable **quick creation** of **governed subscriptions**.

- Compose artifacts based on common or organization-based patterns into re-usable blueprints.
- The service is designed to help with *environment setup*

Azure Policy enforce organizational standards and to assess **compliance** at-scale

- Policies do not restrict access, they only observe for compliance.
- **policy definition** is a **JSON** file used to describe business rules to control access to resources.
- **Policy Assignment** scope of a policy can effect. Assigned to a user, a resource group or management group.
- **Initiative definition** is a collection of policy definitions, that you can assign. eg. A group of policies to enforce **PCI-DSS compliance**

SC-900 CheatSheet

Cloud Adoption Framework is a whitepaper that is a **step by step process** to help organizations plan and migrate their workloads to Azure
Azure Well-Architected Framework describe **best practices for building workloads** on Azure **categorized into 5 pillars**

- **Cost Optimization** — Managing costs to maximize the value delivered.
- **Operational Excellence** — Operations processes that keep a system running in production.
- **Performance Efficiency** — The ability of a system to adapt to changes in load.
- **Reliability** — The ability of a system to recover from failures and continue to function.
- **Security** — Protecting applications and data from threats.
- **Microsoft Security Best Practices** is a collection of best practices that provide clear actionable guidance for security related decisions.
    - *Previously known as Azure Security Compass*

Shared access signature (SAS) is a temporary URI that grants restricted access rights to **Azure Storage** resources.
Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any other origins (domain, scheme, or port) than its own from which a browser should permit loading of resources
Microsoft Security Development Lifecycle (SDL) is an **industry-leading software security assurance process**.

- Building security into each **SDL phase** of the development lifecycle helps you catch issues early, and it helps you reduce your development costs.