Microsoft SC-900 Notes

Microsoft Security, Compliance, and Identity Fundamentals

Hassen Hannachi

December 10, 2025

Contents

List of Figures

Learn about core concepts that are foundational to security, compliance, and identity solutions, including shared responsibility, Zero Trust, data residency, the role of identity providers, and more.

1 Introduction to security, compliance, and identity concepts

1.1 Describe security and compliance concepts

Learn about common security and compliance concepts that are foundational to Microsoft solutions. Topics include the shared responsibility and Zero Trust models, encryption, data residency and data sovereignty, and more.

1.1.1 Unit 1: Describe Shared responsibility model

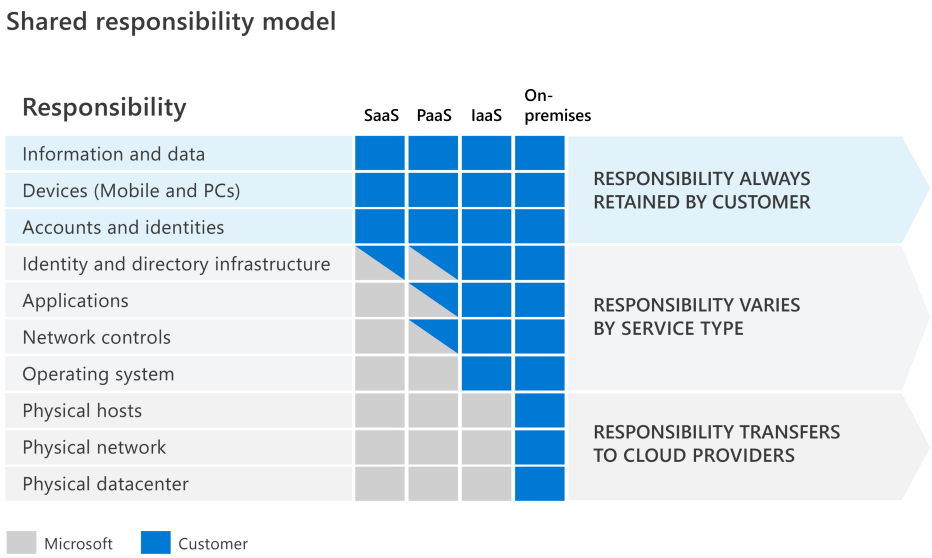

Figure 1: share responsibility model

- ***On-premises datacenters***: In an on-premises datacenter, hardware and software, the organization is 100 percent responsible for implementing security and compliance.
- ***Infrastructure as a Service (IaaS)***: Of all cloud services, IaaS requires the most management by the cloud customer. Customers still have responsibility for software components running on that computing infrastructure such as operating systems, network controls, applications, and protecting data.

- ***Platform as a Service (PaaS)***: PaaS provides an environment for building, testing, and deploying software applications. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

- ***Software as a Service (SaaS)***: SaaS is hosted and managed by the cloud provider, for the customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types, you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources including mobile devices, PCs, printers, and more. In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

1.1.2 Unit 2: Defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

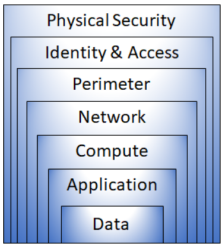

Figure 2: defense in depth

- ***Physical*** security such as limiting access to a datacenter to only authorized personnel.
- ***Identity and access*** security controls, such as multifactor authentication or condition-based access, to control access to infrastructure and change control.
- ***Perimeter*** security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- ***Network*** security, such as network segmentation and network access controls, to limit communication between resources.

- ***Compute*** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- ***Application*** layer security to ensure applications are secure and free of security vulnerabilities.
- ***Data*** layer security including controls to manage access to business and customer data and encryption to protect data.

Confidentiality, Integrity, Availability (CIA

Defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. All the different mechanisms (technologies, processes, and training) are elements of a cybersecurity strategy, whose goals include ensuring confidentiality, integrity, and availability; often referred to as CIA.

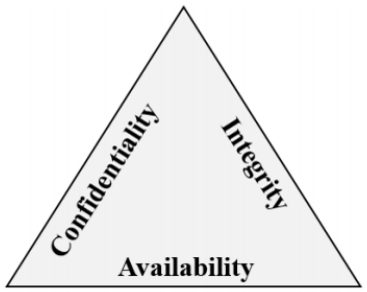

Figure 3: Confidentiality, Integrity, Availability (CIA

- ***Confidentiality*** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential. but then you also need to keep the encryption keys confidential.
- ***Integrity*** refers to keeping data or messages correct. Integrity is about having confidence that data hasn't been tampered with or altered.
- ***Availability*** refers to making data available to those who need it, when they need it.

1.1.3 Unit 3: Describe the Zero Trust model

The Zero Trust model operates on the principle of "trust no one, verify everything."

Trust Guiding Principles

The Zero Trust model has three principles which guide how security is implemented:

- ***Verify explicitly***. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.

- ***Least privileged access***. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- ***Assume breach***. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

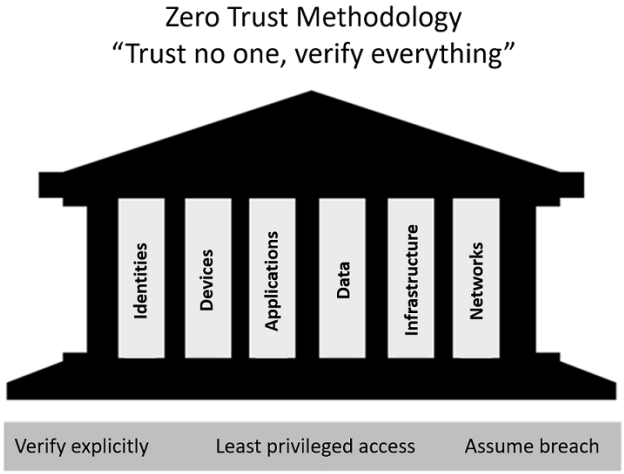

Figure 4: six foundational pillars

Six Foundational Pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- ***Identities*** may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication and follow least privilege access principles.
- ***Devices*** create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- ***Applications*** are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- ***Data*** should be classified, labeled, and encrypted based on its attributes.
- ***Infrastructure***, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies.

- ***Networks*** should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

1.1.4 Unit 4: Describe encryption and hashing

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

- Symmetric encryption uses the same key to encrypt and decrypt data.
- Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but the key used to encrypt can't be used to decrypt encrypted data.
- Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions.
- Encryption may protect data at rest, or in transit.

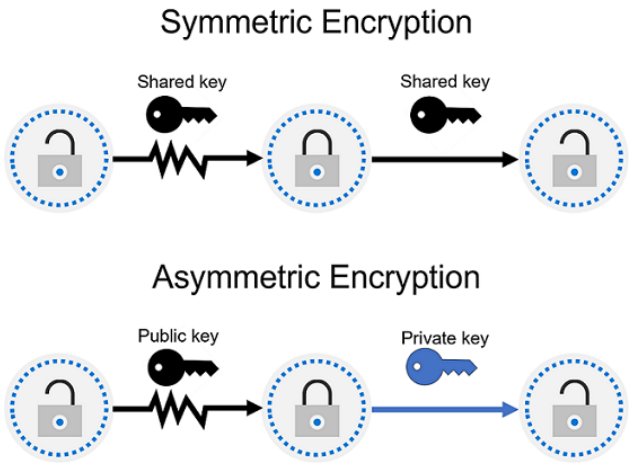

Figure 5: encryption

Encryption for data at rest

Data at rest is the data that's stored on a physical device, such as a server (or stored in a database or a storage account), encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

Encryption for data in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encryption for data in use

A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

Hashing

uses an algorithm to convert text to a unique fixed-length value called a hash. Each time the same text is hashed using the same algorithm, the same hash value is produced.

- Hashing is different to encryption in that it doesn't use keys
- Hashed value isn't subsequently decrypted back to the original.
- Hashing is often used to store passwords.

Figure 6: hashing

1.1.5 Unit 5: Describe governance, risk, and compliance (GRC) concepts

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managing governance, risk, and compliance (GRC).

As organizations establish GRC competency they can establish a framework that includes implementing specific policies, operational processes, and technologies.

Governance

is the set of rules and processes an organization uses to direct and control its operations. Many of these come from external standards and requirements. For example, organizations define who can access resources, what they can do, where and when they can do it, and who gets administrative privileges and for how long.

Risk management

is the process of identifying, assessing, and addressing threats that could impact company or customer goals. Risks come from both external and internal sources. External risks include political or economic changes, weather events, pandemics, and security breaches. Internal risks arise within the organization, such as data leaks, intellectual property theft, fraud, or insider threats.

Compliance

refers to the laws and regulations—local, national, or international—that an organization must follow. These rules define what data must be protected, what processes are required, and the penalties for failing to comply.

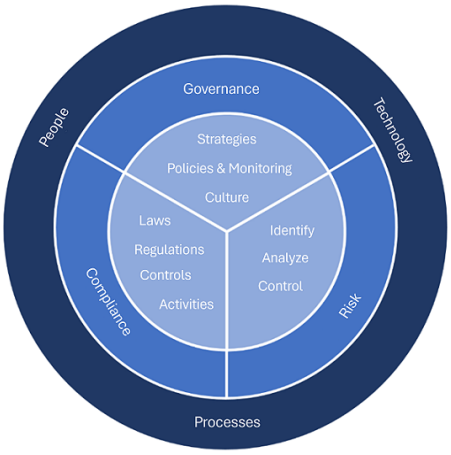

Figure 7: governance, risk, and compliance (GRC)

Compliance is not the same as security. Compliance focuses on meeting legal minimum standards, while security involves all the practices and technologies used to protect sensitive data and prevent breaches. However, strong security is often essential for meeting compliance requirements. Some compliance-related concepts include:

- ***Data residency*** in compliance, data residency rules define where data can be physically stored and how/when it can be transferred, processed, or accessed across borders. These requirements vary widely by jurisdiction.
- ***Data sovereignty*** is the principle that data—especially personal data—is governed by the laws of the country or region where it's collected, stored, or processed. This creates complexity because a single piece of data may be collected in one place, stored in another, and processed in a third, making it subject to multiple legal jurisdictions.
- ***Data privacy*** Providing clear notice and being transparent about how personal data is collected, used, processed, and shared are core principles of privacy laws. Personal data includes any information that identifies or can be linked to an individual. Organizations must follow numerous laws, regulations, codes of conduct, and industry standards that govern how this data is protected and managed.

All organizations manage data so understanding terminology and concepts related to compliance is important as they work to meet the minimum, mandated laws and/or regulations.

1.2 Describe identity concepts

Identity is the way in which people and things are identified on your corporate network, and in the cloud. Being certain about who or what is accessing your organization's data and other resources is a fundamental part of securing your environment.

1.2.1 Unit 1: Define authentication and authorization

Authentication

is the process of proving that a person is who they say they are.

When you want to access a computer or device, you may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password, together, are a form of authentication. Authentication is sometimes shortened to AuthN.

Authorization

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization. In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to **`AuthZ`**.

1.2.2 Unit 2: Define identity as the primary security perimeter

Digital collaboration has evolved. Employees and partners now need to access resources from anywhere, on any device, without losing productivity. Remote work has also increased significantly, accelerating this shift.

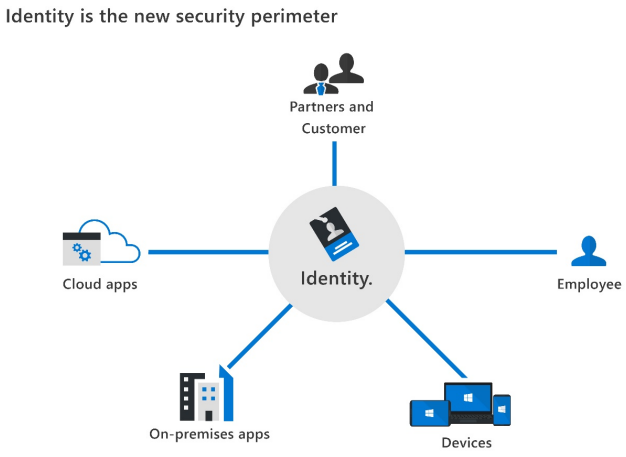

Figure 8: security perimeter

The security perimeter can no longer be viewed as the on-premises network. It now extends to:

- SaaS applications for business-critical workloads that might be hosted outside the corporate network.
- The personal devices that employees are using to access corporate resources (BYOD, or bring your own device) while working from home.
- The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees
- Internet of things, referred to as IoT devices, installed throughout your corporate network and inside customer locations.

An identity may be associated with a user, an application, a device, or something else.

1.2.3 Unit 3: Describe the role of the identity provider

Modern authentication relies on a central identity provider. The identity provider creates, manages, and maintains identity information, and delivers authentication, authorization, and auditing services.

- With this model, all authentication flows through a single provider, which centrally stores and manages the information used to verify users.
- This centralization allows organizations to enforce consistent authentication and authorization policies, monitor user behavior, detect suspicious activity, and reduce malicious attacks.
- With modern authentication, the client provides an identity to the identity provider, which verifies it. Once verified, the identity provider issues a security token that the client presents to the server.
- The server validates the token through its trust relationship with the identity provider. Using the token and its contained information, the user or application gains access to server resources. The identity provider centrally manages both the token and authentication service.

Examples of cloud-based identity providers include Microsoft Entra ID, Google, Amazon, LinkedIn, and GitHub.

Single sign-on

Another fundamental capability of an identity provider and "modern authentication" is the support for single sign-on (SSO). With SSO, the user logs in once and that credential is used to access multiple applications or resources. When you set up SSO between multiple identity providers, it's called federation.

1.2.4 Unit 4: Describe the concept of directory services and Active Directory

In computer networks, a directory is a hierarchical structure that stores information about network objects. A directory service manages this data and makes it accessible to users, administrators, services, and applications.

Microsoft's Active Directory (AD), introduced with Windows 2000, is a set of directory services for on-premises, domain-based networks. Its primary service, Active Directory Domain Services (AD DS), stores information about domain members, verifies credentials, and defines access rights. Servers running AD DS are called domain controllers (DCs). AD DS allows organizations to manage multiple on-premises systems using a single user identity. However, it does not natively support mobile devices, SaaS applications, or modern authentication methods.

The rise of cloud services, SaaS, and personal devices has driven the evolution of AD-based identity solutions. Microsoft Entra ID (formerly Azure Active Directory) is an example, offering Identity as a Service (IDaaS) for both cloud and on-premises applications.

1.2.5 Unit 5: Describe the concept of federation

Federation allows access to services across organizational or domain boundaries by creating trust between their identity providers. It eliminates the need for users to have separate usernames and passwords for different domains.

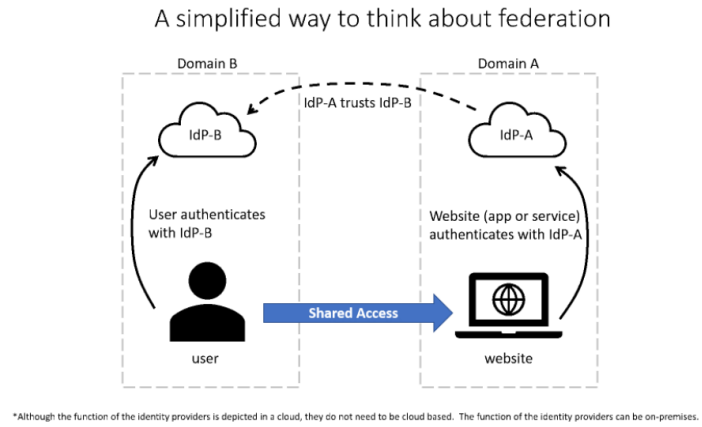

Figure 9: federation

A simplified view of federation works like this:

- A website in domain A uses Identity Provider A (IdP-A) for authentication.
- A user in domain B authenticates with Identity Provider B (IdP-B).
- IdP-A trusts IdP-B, so when the user provides credentials, the website grants access based on this trust.

Federation trust isn't always bidirectional; access from domain A to B only works if the trust is explicitly configured.

A common example is logging into a third-party site using a social media account. Here, the social media platform acts as the identity provider, and the third-party site (e.g., using Microsoft Entra ID) trusts it, allowing access without separate credentials.