



SC-900: Security, Compliance and Identity Concepts

SC-900 domain 1, Describe the concepts of security, compliance and identity (10-15 %, as of 2026) | Shared responsibility, defence in depth, zero trust, encryption and hashing, GRC, authentication vs authorisation, identity providers, federation

SC-900 Domain 1 Zero Trust GRC

Who secures what

	On-premises	IaaS	PaaS	SaaS
Information and data	Customer	Customer	Customer	Customer
Devices (mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Shared	Shared
Applications	Customer	Customer	Shared	Microsoft
Network controls	Customer	Customer	Shared	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts, network, datacenter	Customer	Microsoft	Microsoft	Microsoft

Customer Shared Microsoft responsibility shifts

EXAM TIP

Whatever the model, the **customer** always owns information and data, devices, and accounts and identities. Physical security moves to Microsoft as soon as you leave on-premises.

Identity concepts

Authentication (who are you?)	Authorisation (what can you do?)
something you know: password, PIN	roles (RBAC) and group membership
something you have: phone, FIDO2 key	permissions granted by app or resource
something you are: fingerprint, face	Conditional Access adds conditions
MFA = two or more different categories	checked after authentication, on every request

Identity as the primary security perimeter — With cloud and remote work, the identity (user, device, workload) replaces the network edge as the main control point.

Four pillars of identity — Administration (create and manage identities), authentication, authorisation, auditing (track who did what).

Modern authentication — Token-based protocols (OpenID Connect, OAuth 2.0, SAML) between client, IdP and app, instead of passwords sent to every app.

MYTH

❌ In SaaS the provider is responsible for everything

❌ Zero Trust means trusting nothing inside the company network, outside is fine

❌ Hashing is encryption

❌ Data residency and sovereignty are the same

FACT

✅ **Data, devices, accounts and identities stay with the customer**
Microsoft runs the service; you configure access and protect your data.

✅ **No network location is trusted**
Every request is verified with identity, device and context signals.

✅ **Hashing is one-way, encryption is reversible with a key**
Hashes verify integrity and passwords; encryption protects confidentiality.

✅ **Residency = where data sits; sovereignty = whose laws apply**
Data stored in an EU region can still face foreign legal requests.

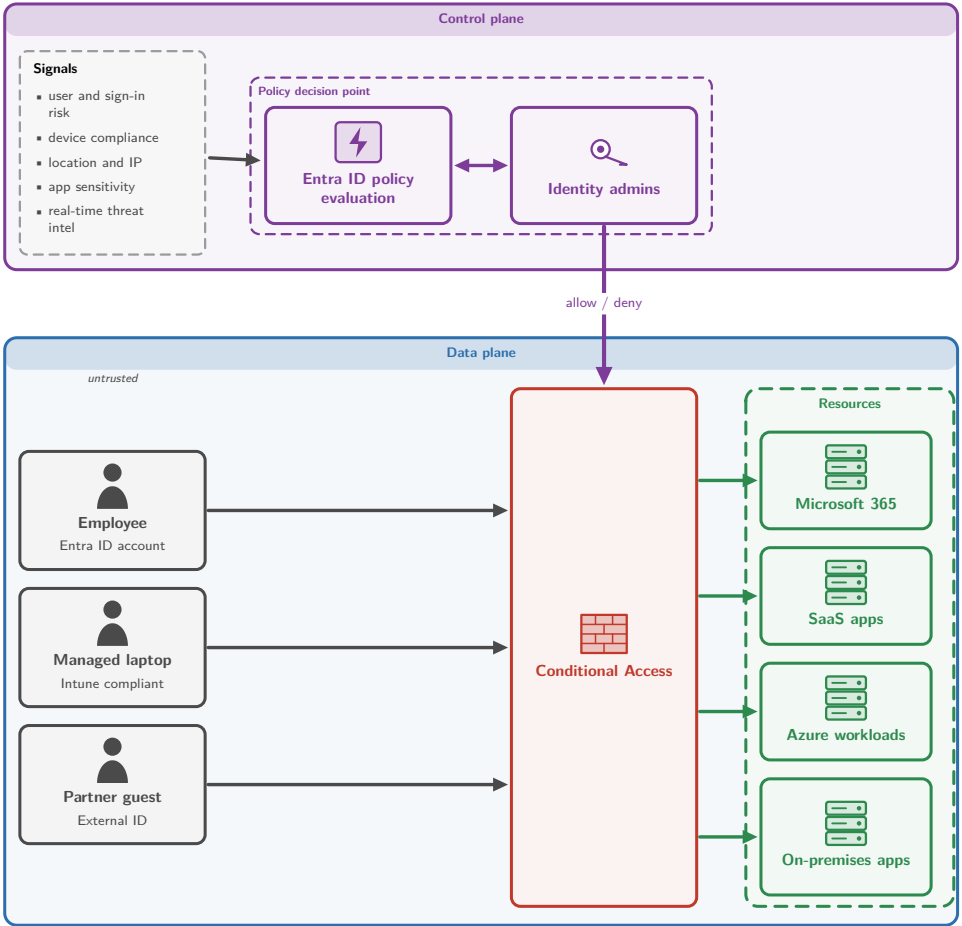
🔒 Defence in depth and Zero Trust

Physical security	datacenter access, guards, cameras (Microsoft's job in the cloud)
Identity and access	MFA, Conditional Access, SSO, auditing of sign-ins
Perimeter	DDoS Protection, Azure Firewall at the edge
Network	segmentation, NSGs, deny by default, private endpoints
Compute	patching, endpoint protection, Bastion instead of open RDP/SSH
Application	secure development, secrets in Key Vault, WAF
Data	encryption, classification, DLP, backups

- Mnemonic: **VLA**
- V Verify explicitly** authenticate and authorise on every available data point: identity, location, device, service, data, anomalies
 - L Least-privilege access** just-in-time and just-enough access, risk-based policies, data protection
 - A Assume breach** segment access, encrypt end to end, use analytics to detect threats and limit blast radius

Identities Devices Applications Data Infrastructure Networks

Microsoft's **six foundational pillars** of Zero Trust above are where signals come from and controls apply; identity is the control plane that ties them together.



Every request is verified with all available signals, whatever its network

🔍 Encryption, hashing and GRC

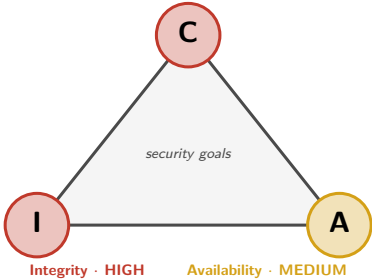
		REVERSIBLE? · NEEDS A SECRET?
Text	Pa55word!	
Hex (UTF-8 bytes)	50 61 35 35 77 6f 72 64 21	yes, by anyone · no
Base64	UGE1NXdvcnQh	yes, by anyone · no
URL-encoded	Pa55word%21	yes, by anyone · no
SHA-256	40a4b7590a7061dfeac26ea3d3153b5802a4f003941e412c7f5699ebfac39a6	no (one-way) · no
HMAC-SHA256 (key 'demo-key')	3b792be939013b4fb7c1933349b58ad72ed48eebf5ea855ef2486dee6f60b568	no (one-way) · yes, the key
AES-GCM encryption	different every time: depends on the key and a random nonce	yes, with the key only · yes, the key

Encoding changes the form, anyone can undo it. Hashing gives a fixed-size fingerprint, nobody can undo it. A MAC is a hash that needs a secret key, so it proves who made it. Encryption hides the content from anyone without the key.

Encoding is reversible without a key; hashing is one-way; only encryption needs a key to reverse

Concept	What it is	Microsoft example
Encryption at rest	data stored encrypted on disk	Azure Storage service encryption, TDE in Azure SQL, BitLocker
Encryption in transit	data encrypted while moving	TLS 1.2+ to Azure endpoints, VPN, ExpressRoute with MACsec
Symmetric	one secret key (AES-256)	bulk data encryption
Asymmetric	public / private key pair (RSA, ECC)	TLS certificates, digital signatures
Hashing + salt	one-way digest of a password	Entra ID stores password hash derivatives, never passwords
Key management	generate, store, rotate keys	Azure Key Vault, Managed HSM, customer-managed keys

Scenario: Customer database of an online shop Confidentiality · HIGH



Confidentiality HIGH only the right people can read it IF BROKEN card and address data leaked PROTECT encryption, least privilege, DLP	Integrity HIGH nobody can change it unnoticed IF BROKEN prices or orders altered PROTECT hashing, signing, audit logs	Availability MEDIUM it works when it is needed IF BROKEN DDoS stops checkout PROTECT zone redundancy, backups, DDoS Protection
---	--	---

Governance — Rules, policies and processes an organisation sets to meet its objectives and obligations.

Risk management — Identify, assess and treat risks (accept, mitigate, transfer, avoid).

Compliance — Proving that you meet laws, regulations and standards (GDPR, ISO 27001, NIS2).

Quantity	Formula
Single loss expectancy	$SLE = AV \times EF$

Annualised loss expectancy $ALE = SLE \times ARO$

where AV = asset value (EUR); EF = exposure factor: share of the asset lost in one event (0-1); ARO = annualised rate of occurrence (events per year); SLE = loss from one event (EUR); ALE = expected loss per year (EUR per year)

Quantifying a risk for GRC decisions

📄 **Worked example: account takeover**

A customer database is valued AV = 500,000 EUR; one takeover of an admin account exposes EF = 0.4 of it: SLE = **200,000 EUR**. Without MFA you expect ARO = 0.5 per year: ALE = **100,000 EUR**. If MFA cuts ARO to 0.01 (Microsoft reports MFA blocks over 99 % of account-compromise attacks), ALE = **2,000 EUR**: a control costing less than 98,000 EUR a year is justified.

Self-test and recap

Q1 Three Zero Trust principles?

A Verify explicitly, use least-privilege access, assume breach.

Q2 Which responsibilities stay with the customer in every model?

A Information and data, devices, accounts and identities.

Q3 Proving who you are vs what you may do?

A Authentication vs authorisation.

Q4 One key to encrypt and decrypt?

A Symmetric encryption (AES).

Q5 One-way fixed-length digest?

A A hash (salted for passwords).

Q6 Laws of the country where data is stored apply?

A Data sovereignty.

Q7 Trust between two organisations' identity providers?

A Federation.

Q8 Innermost layer of defence in depth?

A Data.

Q9 Four pillars of identity?

A Administration, authentication, authorisation, auditing.

Shared responsibility shifts
but data, devices, identities stay
yours

Seven layers of defence
physical to data

Zero Trust = V, L, A
verify, least privilege, assume
breach

Encrypt vs hash vs encode
key, one-way, no secret

GRC
governance, risk, compliance;
residency $\neq$ sovereignty

AuthN then AuthZ
identity is the new perimeter