Security & Identity Concepts

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

LAYERED CLOUD SECURITY

- **Responsibility** — Shared
- **Zero Trust** — Verify
- **Defense** — Layers
- **Cryptography** — Protect

01 Describe the concepts of security, compliance, and identity 10–15%

Shared responsibility and cloud adoption

- **Shared responsibility** divides security work between provider and customer. Microsoft protects cloud datacenters, physical hardware and the underlying infrastructure; customers remain responsible for their data, identities, access decisions and device security.
- **IaaS** leaves customers managing guest operating systems, applications and configurations. **PaaS** transfers operating-system and platform management to the provider. **SaaS** also transfers application operation; customers still configure access and protect their information.
- Customer management responsibility generally decreases from **IaaS** → **PaaS** → **SaaS**. A cloud service does not automatically make customer permissions, accounts or data handling compliant.
- The **Cloud Adoption Framework** starts with business strategy and planning before preparing the environment. **Ready** establishes foundations; adoption implements workloads, with governance, security and management supporting ongoing operation.

Zero Trust and defense in depth

- **Zero Trust** has three guiding principles: **verify explicitly**, **use least privilege**, and **assume breach**. A corporate network location alone is insufficient evidence of trust.
- **Verify explicitly** uses identity, device health, location, workload and risk signals. **Least privilege** limits access scope and duration. **Assume breach** encourages segmentation, encryption, monitoring and rapid containment.
- **Defense in depth** places complementary controls across physical security, identity and access, the perimeter, networks, compute, applications and data. Failure of one control should leave other protective layers.
- **Identity** is a primary security perimeter for cloud access. Protect identities, devices, applications, data, infrastructure and networks together; regular patching, MFA and reduced exposure address different attack paths.

Encryption, hashing and signatures

- **Encryption** converts readable data into ciphertext recoverable with the appropriate key. **At rest** protects stored data such as disks; **in transit** protects communications such as TLS/HTTPS or encrypted VPN traffic.
- **Symmetric encryption** uses a shared secret key. **Asymmetric cryptography** uses a public/private key pair. Keep private keys secret; public keys may be distributed to other parties.

Security & Identity Concepts / Microsoft Entra

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

LAYERED CLOUD SECURITY

- **Responsibility** Shared
- **Zero Trust** Verify
- **Defense** Layers
- **Cryptography** Protect

- **Hashing** produces a one-way digest used for integrity checks and password verification. It does not provide a decryption operation; password storage also needs salts and a suitable password-hashing algorithm.
- A **digital signature** is created with the signer's private key and verified with the corresponding public key. It supports integrity and signer authenticity; signing alone does not hide the content.

Identity vocabulary and GRC

- **Authentication** establishes who an identity is. **Authorization** determines what it can do. **Auditing** records activity; **administration** manages accounts, roles and their lifecycle.
- An **identity provider** authenticates users and issues trusted identity assertions or tokens. A **directory service** stores identities and related information; **federation** establishes trust so one identity system accepts another's authentication.
- **Governance** defines policies, ownership and accountability. **Risk management** evaluates likelihood and impact, then selects treatments. **Compliance** assesses whether required rules, standards and obligations are met.
- **Preventive** controls reduce the chance of an incident, such as encryption or separation of duties. **Detective** controls reveal problems through monitoring or audits. **Corrective** controls limit damage and restore operation after an incident.

02 Describe the capabilities of Microsoft Entra 25–30%

Directories, hybrid identity and external access

- **Microsoft Entra ID** is a cloud identity and access service used by Microsoft 365, Azure and connected applications. A **tenant** is an organization's directory boundary for identities, applications and policies.
- **Active Directory Domain Services (AD DS)** supports domain controllers, computer accounts, domain join, Group Policy and protocols such as Kerberos and LDAP. Entra ID serves cloud identity needs and is not a domain controller.
- **Hybrid identity** connects on-premises AD DS with Entra ID. **Microsoft Entra Connect Sync** or **Cloud Sync** synchronizes supported identity information; synchronization and federation are different functions.
- **Password hash synchronization** supports cloud password validation. **Pass-through authentication** validates through on-premises agents. **Federation** delegates authentication to a trusted system such as AD FS.
- **B2B collaboration** supports partner and guest access using external identities. **Single sign-on (SSO)** lets users access connected applications after signing in, subject to applicable authorization and access policies.

Microsoft Entra

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

IDENTITY AND ACCESS DECISIONS

Identity Authenticate → **Signals** Evaluate → **Access** Authorize → **Governance** Review

Users, applications and managed identities

- **User identities** represent people. **Workload identities** represent applications, services and automation; they also need explicit permissions and lifecycle management.
- An **application registration** defines an application object. A **service principal** is its local representation in a tenant and receives access assignments. Registering an application in its home tenant normally creates both.
- A **managed identity** is a workload identity whose credentials Azure manages. Supported resources can obtain tokens without embedding passwords or client secrets in code; permission grants are still required.
- A **system-assigned managed identity** belongs to one resource and is deleted with it. A **user-assigned managed identity** has its own lifecycle and can be attached to multiple supported resources.

MFA, passwordless sign-in and password care

- **MFA** combines at least two distinct factor types: something you **know**, something you **have**, and something you **are**. Two passwords are still one factor type.
- **Microsoft Authenticator**, phone calls and SMS are familiar verification methods. Available methods depend on policy and context; **FIDO2/passkeys** and **Windows Hello for Business** provide phishing-resistant options.
- **Windows Hello for Business** uses a device-bound key unlocked by a PIN, fingerprint or facial recognition. The PIN is local to that device; biometric templates remain on the device.
- **Passwordless sign-in** authenticates without a reusable account password. Authenticator phone sign-in uses an approval and number-matching experience; passkeys and Hello use cryptographic credentials.
- **Password Protection** blocks known weak passwords and variants using a global banned list and supported custom terms. **Self-service password reset (SSPR)** lets registered users recover access with approved verification methods.
- **SSPR methods** and **MFA methods** are different sets: alternate email and security questions can support eligible password-reset scenarios, but are not general Entra MFA sign-in factors. Method policy and user role affect availability.

Conditional Access and identity risk

- **Conditional Access** evaluates signals such as user or group, target resource, device state, location and risk. It makes policy decisions during access evaluation after initial authentication.
- **Grant controls** can block access or require MFA, an authentication strength or a compliant device. **Session controls** constrain an allowed session, such as sign-in frequency or supported download restrictions.

Microsoft Entra / Microsoft Security

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

IDENTITY AND ACCESS DECISIONS

Identity Authenticate → **Signals** Evaluate → **Access** Authorize → **Governance** Review

- **Microsoft Intune** manages devices and apps and evaluates device compliance. Conditional Access can use that compliance signal to control resource access; management enrollment alone is not proof of compliance.
- **Microsoft Entra ID Protection** detects and investigates identity-based risks. **User risk** concerns possible compromise of an account; **sign-in risk** concerns a particular authentication attempt. Leaked credentials are an account-compromise signal.
- **Risk-based policies** can require remediation such as MFA or a secure password change. **Security defaults** provide a preconfigured baseline including MFA registration, privileged-account protection and blocking legacy authentication; Conditional Access enables tailored policies.

Roles, PIM and access governance

- **Role-based access control (RBAC)** grants permissions through roles at a defined scope. Use the least powerful suitable role; built-in and supported custom roles avoid unnecessary broad administration.
- **Microsoft Entra roles** manage directory resources. **Azure RBAC roles** manage Azure resources at management-group, subscription, resource-group or resource scope. A directory administrator role does not automatically grant all Azure resource access.
- **Privileged Identity Management (PIM)** provides eligible, just-in-time and time-bound privileged access. Activation can require approval, MFA, justification and a limited duration; eligibility differs from an active assignment.
- **Access reviews** periodically reassess group memberships, application access and supported role assignments. Review decisions can remove access that is no longer needed.
- **Microsoft Entra ID Governance** combines access lifecycle controls such as PIM, access reviews and entitlement management. **Access packages** bundle resources with request, approval and expiration rules.

03 Describe the capabilities of Microsoft security solutions 35–40%

Network segmentation and traffic controls

- **Virtual networks (VNets)** create logical network boundaries. Separate VNets and subnets support segmentation and governance; connectivity between them must be designed explicitly.
- A **network security group (NSG)** filters inbound and outbound traffic using source, destination, protocol and port rules. Associate an NSG with a **subnet** or **network interface**.
- NSG rules run in **priority order**, with lower numbers evaluated first. Custom rules use priorities **100–4096**; default rules have higher numbers. NSGs are stateful and do not inspect web payloads like a WAF.

Microsoft Security

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

SECURITY OPERATIONS

Posture Assess → **Telemetry** Collect → **Detection** Correlate → **Response** Contain

- **Azure Firewall** centrally filters network and application traffic and supports NAT. It protects network resources; it is distinct from identity controls or mailbox protection.
- **Web Application Firewall (WAF)** filters HTTP(S) requests for common web attacks such as SQL injection and cross-site scripting. **Azure DDoS Protection** mitigates supported network-layer denial-of-service attacks.

Secure administration, secrets and standards

- **Azure Bastion** provides managed RDP/SSH connectivity to VMs over their private IP addresses. Browser connections use TLS through the Azure portal; supported configurations also offer native-client access.
- **Azure Key Vault** safeguards **secrets**, **cryptographic keys** and **certificates**. Control access to each operation; use managed identities where possible instead of storing application credentials in source code.
- **Azure Policy** evaluates resource configurations against organizational standards. Effects can audit, deny, modify or deploy supported settings; remediation can address existing resources. An **initiative** groups related policy definitions.
- **RBAC** governs who can perform operations; **Policy** governs acceptable resource configuration. **ARM templates/Bicep** provide repeatable infrastructure deployments; governance definitions can group deployment templates, policies and role assignments.

Defender for Cloud and security posture

- **Microsoft Defender for Cloud** combines **cloud security posture management (CSPM)** with **cloud workload protection** across supported Azure, multicloud and hybrid environments.
- **CSPM** assesses configuration, exposes weaknesses and recommends improvements. Policies and standards organize expected controls; recommendations identify actions for affected resources.
- **Secure score in Defender for Cloud** summarizes posture improvement against assessed recommendations. It is distinct from Microsoft Secure Score and the Purview compliance score; a high score does not prove that breaches are impossible.
- **Cloud workload protection (CWPP)** provides threat detection and protection for supported servers, databases, storage, containers and other workloads. Defender for SQL covers supported SQL services, including SQL Managed Instance.
- Foundational posture assessment and enhanced protection have different plan requirements. **Just-in-time VM access** restricts management-port exposure for a requested time window; **PIM** controls privileged identity role activation.

Microsoft Security

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

SECURITY OPERATIONS

Posture Assess → **Telemetry** Collect → **Detection** Correlate → **Response** Contain

Microsoft Sentinel: collect, detect and respond

- **SIEM** centralizes and analyzes security logs, correlates events and generates alerts or incidents. **SOAR** orchestrates response workflows and automation. **Microsoft Sentinel** provides cloud-native SIEM and SOAR capabilities.
- For a workspace-based deployment, enable Sentinel on a **Log Analytics workspace** and connect security data sources. **Data connectors** ingest supported Microsoft, third-party and multicloud telemetry.
- **Analytics rules** detect suspicious patterns. **Incidents** group related alerts for investigation; entity relationships help analysts understand affected users, hosts and other resources.
- **Workbooks** visualize security data and trends. **Hunting** uses proactive queries, commonly in **Kusto Query Language (KQL)**, to investigate activity that existing detections may have missed.
- **Automation rules** streamline incident handling. **Playbooks**, built on Azure Logic Apps, execute response workflows such as enrichment, notification or containment. Sentinel can integrate Defender XDR incidents and other security sources.

Defender XDR, endpoints and identity threats

- **Microsoft Defender XDR** correlates threats across endpoints, identities, email and cloud apps. **XDR** joins signals and response across these protection domains; Sentinel can bring in a broader set of enterprise logs.
- The **Microsoft Defender portal** provides incidents, alerts, investigation, hunting and reports. An **alert** flags suspicious activity; an **incident** connects related alerts into an attack story.
- **Defender for Endpoint** includes attack surface reduction, endpoint detection and response, and automated investigation and remediation. **Network protection** helps block access to dangerous internet destinations.
- **Defender Vulnerability Management** discovers and prioritizes endpoint weaknesses and remediation work. **Secure Score for Devices** tracks device security configuration; it differs from a count of active malware incidents.
- **Defender for Identity** analyzes identity signals, especially from on-premises Active Directory, to detect compromised identities, lateral movement and other suspicious behavior.
- **Microsoft Secure Score** measures recommended security improvements across supported organizational services. **Threat analytics** and **threat intelligence** help explain threats, indicators and exposure so teams can prioritize defenses.

Microsoft Security / Microsoft Purview

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

PROTECT AND GOVERN INFORMATION

- **Classify** — Identify
- **Labels & DLP** — Protect
- **Retention** — Preserve
- **Audit** — Investigate

Email, collaboration and cloud apps

- **Defender for Office 365** protects email and supported collaboration workloads from phishing, malicious attachments and unsafe links. **Safe Attachments** analyzes attachments in a virtual environment before normal delivery under supported policies.
- **Safe Links** checks URLs and provides time-of-click protection in supported email and collaboration experiences, including Teams. Link protection and attachment detonation address different attack paths.
- **Attack simulation training** runs benign phishing simulations and education to improve user awareness. It is a **Defender for Office 365 Plan 2** capability.
- **Defender for Cloud Apps** is a cloud access security broker (**CASB**). It discovers **shadow IT**, evaluates cloud-app risk, helps protect sensitive information and can control supported app sessions.
- **SaaS security posture management (SSPM)** in Defender for Cloud Apps identifies risky SaaS configurations. **Intune MDM** manages device settings; **MAM** protects organizational app data, including supported scenarios without full device enrollment.

04 Describe the capabilities of Microsoft compliance solutions 20–25%

Trust, privacy and compliance assessments

- The **Service Trust Portal** provides information about Microsoft cloud security, privacy and compliance, including audit reports and certifications. The **Microsoft Purview portal** is used to operate an organization's compliance and data-protection solutions.
- Microsoft privacy principles emphasize **control**, **transparency**, **security**, **strong legal protections**, **no content-based targeting**, and benefits to customers. Privacy information explains how data is collected and used and how customers exercise choices.
- **Customer Lockbox** adds customer approval to eligible Microsoft support access requests for customer content. It governs a support-access workflow; it does not replace normal user permissions or data protection.
- **Compliance Manager** organizes **assessments**, controls, improvement actions and supporting evidence. An assessment groups requirements from a regulation, standard or policy; responsibility may be Microsoft-managed, customer-managed or shared.
- **Compliance score** tracks progress on risk-reducing improvement actions. Preventive, detective and corrective actions serve different purposes; a score is guidance for improvement, not a legal compliance certification.

Microsoft Purview

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

PROTECT AND GOVERN INFORMATION

- **Classify** — Identify
- **Labels & DLP** — Protect
- **Retention** — Preserve
- **Audit** — Investigate

Discover and classify sensitive information

- **Sensitive information types (SITs)** recognize patterns such as credit card numbers using regular expressions, supporting evidence and confidence requirements. **Exact data match (EDM)** identifies matches to a prepared sensitive dataset.
- **Trainable classifiers** use examples and machine learning to recognize categories such as resumes or contracts. Pretrained classifiers are ready-made categories; custom classifiers learn an organization's content patterns.
- **Document fingerprinting** recognizes content based on a standard form or template. Choose the classification method for the content structure; pattern matching and semantic classification solve different detection problems.
- **Content explorer** shows where classified sensitive content is found, subject to permissions. **Activity explorer** shows relevant data activity, such as labeling actions and policy-related events.

Sensitivity labels and data loss prevention

- **Sensitivity labels** classify content and can apply protection such as encryption, access restrictions and visual markings. Labels persist with supported files and email; the label's configured settings determine the protection.
- **Sensitivity label policies** publish labels to selected users and configure defaults, mandatory labeling or justification requirements. Supported automatic labeling applies labels based on detected sensitive content or classifiers.
- **Data loss prevention (DLP)** detects sensitive content and risky sharing or use. Rules can warn, block, restrict or allow an action with justification; **policy tips** explain the issue to users.
- DLP can target supported **Exchange Online**, **SharePoint**, **OneDrive**, **Teams chats and channels**, endpoint devices and other locations. Match each policy's location and action support to the intended protection.
- **Endpoint DLP** monitors and restricts supported sensitive-file activities on onboarded **Windows and macOS** devices, such as copying to removable media, printing or uploading. It is separate from mobile device management.
- **Sensitivity labels** describe and protect data; **DLP** controls risky handling; **retention** governs preservation and deletion. These controls can complement one another on the same content.

Microsoft Purview

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

PROTECT AND GOVERN INFORMATION

- **Classify** — Identify
- **Labels & DLP** — Protect
- **Retention** — Preserve
- **Audit** — Investigate

Retention, deletion and records

- **Retention policies** apply preservation and deletion settings across selected locations or scopes. A retain setting can preserve a protected copy even when a user edits or deletes an item.
- **Retention labels** apply item-level lifecycle rules; **retention label policies** publish or automatically apply them. Retain-only, delete-only, and retain-then-delete meet different lifecycle requirements.
- **Records management** uses labels, record declarations, retention and disposition processes to manage business records. Regulatory records apply stronger restrictions than ordinary labeled content.
- An **eDiscovery hold** preserves relevant content for an investigation or legal matter. Retention and holds can prevent permanent deletion even when another policy requests deletion.

Insider risk and communication boundaries

- **Insider Risk Management** correlates activity signals to identify potentially harmful behavior such as data leakage or intellectual-property theft. Risk scores and alerts help analysts prioritize investigation; signals do not establish guilt.
- The insider-risk workflow moves from **policy configuration** through **alerts**, **triage**, **investigation** and **action**. Cases organize investigation; privacy controls and role separation limit unnecessary exposure of user details.
- **Communication Compliance** detects potentially inappropriate or policy-violating communications for review. **Information barriers** restrict communication and collaboration between defined groups in supported Teams, SharePoint and OneDrive scenarios.
- Use **DLP** for sensitive-data sharing rules, **information barriers** for group separation, and **insider risk** for behavioral risk investigation. Each addresses a different compliance requirement.

Microsoft Purview

Microsoft Security, Compliance, and Identity Fundamentals

KNOWLEDGE CHEATSHEET

PROTECT AND GOVERN INFORMATION

- **Classify** — Identify
- **Labels & DLP** — Protect
- **Retention** — Preserve
- **Audit** — Investigate

eDiscovery and audit evidence

- **Microsoft Purview eDiscovery** finds, preserves, collects, reviews and exports content for legal, regulatory or internal investigations. A **case** organizes permissions, searches, holds and related work.
- **Content searches** use keywords, conditions and selected locations to find items such as SharePoint documents or Exchange messages. A search finds content; a hold preserves it. A hold is not required for every search.
- Advanced eDiscovery capabilities can add **custodian management**, review sets and analysis to reduce the volume requiring review. Use the case workflow suited to the investigation's legal and review requirements.
- **Audit** records user and administrator activity for investigation. **Audit Standard** provides baseline search; **Audit Premium** adds capabilities such as eligible longer retention and higher-bandwidth access. Retention depends on licensing, workload and policy.
- **MailItemsAccessed** records supported mailbox-item access events for investigations. **Audit** answers what activity occurred; **eDiscovery** searches and preserves the underlying content.