ISEC Test 2

Access controls (AC) – sec. features that control how users and systems communicate + interact w other systems/resources

AC Concepts:

- **Identity –** set of attributes related to entity used by computer system.
  - **Must be –** unique (identifiers are specific to individual), non-descriptive (credential set should not reveal purpose of account e.g. role), issuance (provided by another authority as means of proving identity)
- **Identification –** assurance the user requesting access is accurately associated with role defined in system
  - First step in applying access controls
  - Common methods – IP address, user ID, email
- **Authentication –** process of verifying user identity
  - User provides something only they can know – establishes trust between user and system
  - 3 main forms: smth person knows (password), smth person has (mobile code), smth person is (biometrics, FaceID)
  - **Strong/multi authentication –** has 2 out of 3 methods above
- **Authorization –** allocating appropriate controls/privileges based on identity in system
  - **3 AC models** use to determine how user is authorized:
  - Discretionary AC – resource owner specifies what users access what resources
  - Mandatory AC – users and data are given clearance/classification lvls, access determined by org. policy
  - Role-based AC – centrally administered set of roles that have privileges, role defined in terms of what operations and tasks it will carry out
- **Accountability –** process of ensuring users are accountable for actions and sec. policies are enforced
  - Tracked by recording user, system and app. Activity
  - Recorded via audits – audit trails can show performance and errors which can be used to trace causes of disruptions
  - Audits: stored securely, manageable size, protected from unauth. Changes, trained personnel to review, only delete-able by admins, show activity of all high privilege accounts
- **Password management –** pw is protected string of characters used to authenticate a user
  - **PW security –** generation (user or system made), strength (length + complexity), rotation (not re-using), limited log-in attempts
  - **PW management –** synchronization (copy user PW to accounts on diff system), self-service pw reset (less tickets to help desk), assisted pw reset (involved another auth. Mechanism to reset pw)

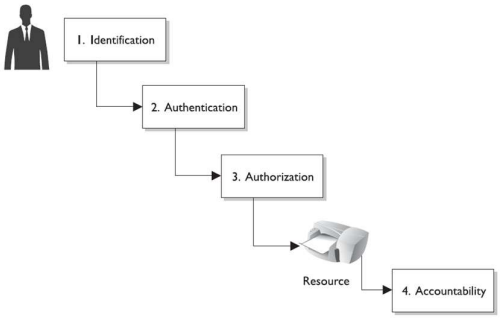

Figure 3-2 Four steps must happen for a subject to access an object: identification, authentication, authorization, and accountability.

Security Controls – safeguards to prevent, detect, correct or minimise security risks

3 types of controls:

Administrative – process of developing and ensuring compliance with policy and procedures

Technical – controls managed or carried out by computer systems

Physical – physical controls that exist

5 purposes of controls:

Deterrent – discourage attacks from happening

Preventative – reduce chance attacks are successful

Detective – detect if attacked has occurred

Corrective – undo damage done by attacks/incidents

Recovery – bring back system after disruption

AC Practices:

Deny system access to undefined/anonymous users

Limit + monitor usage of administrator accounts

Suspend access after specific amount of failed logins

Remove obsolete user accounts as soon as they leave company

Suspend inactive accounts after 30 or 60 days

Enforce strict access criteria.

Enforce the need-to-know and least-privilege practices.

Disable unneeded system features, services, and ports.

Replace default password settings on accounts.
Limit and monitor global access rules.
Remove redundant resource rules from accounts and group memberships.
Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
Enforce password rotation.
Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
Audit system and user events and actions, and review reports periodically.
Protect audit logs.

Security Methods:
Least privilege - only give users the minimum privilege required to do their job
Defense-in-depth - multiple layers of defense
Minimisation - system should not run apps that are not required to complete assigned tasks
Keep things simple - sec. system over-complexity can lead to insecurities
Compartmentalisation - split system into parts so that damage doesn't spread in the case of a vulnerability exploit
Choke points - 'narrow channels' are easy to monitor and control
Fail securely/safely - e.g. if a firewall fails, it defaults to 'deny all'
Secure weakest link - self explanatory
Leverage unpredictability - specific detail about what types of sec. controls are implemented should not be disclosed publicly, a deterrent would simply announce the controls existence but not reveal their nature
Separation of duties - helps to avoid the possibility of a single person being responsible for multiple different function within an org and reduces chance of authorisation abuse

	DETERRENT	PREVENTIVE	DETECTIVE	CORRECTIVE	RECOVERY/COMPENSATORY
Administrative	Penalty & termination policy Publication of previous incidents	Security awareness & training Separation of duties Password policy ICT guidelines Recruitment checks Supervision User registration to access data/resources Change control procedure	Security reviews Performance evaluations Required vacations Background investigations Rotation of duties	Incident handling procedures	Disaster recovery and contingency plans
Technical	Pop-up window Log-on screen Welcome message Display deterrent information on websites	Access control software Library control systems System configuration Antivirus software Passwords Smartcards Biometrics Encryption Firewall (packet filtering) Network architecture Software patching OS hardening	Intrusion detection system Honeypot Firewall (application proxy) Antivirus software Audit trails Penetration testing software Check-sum Signature (MD5, hashes) Integrity validation Task/process manager Advanced CPU features	Recycle bin Undo feature Version control Error correction methods RAID arrays File recovery software Safe-mode booting	Redundant server Recovery technologies
Physical	Warning signs Lights/flashing strobes	Fences Barriers & bollards Locks & keys Double door systems Site selection HVAC Security guards Badge system	Motion detectors Smoke and fire detectors CCTV cameras Security alarms & sensors (heat, moisture, etc.)	Fire extinguishers	Hot/cold/warm sites Backup power/generator

<u>Business Continuity:</u>
Risk – potential event that may have positive or negative effects on business objectives
Risk management – proactive attempt to ID and manage internal events + external threats
Risk management plan:

1. Plan – ID team, scope, methods, tools and acceptable risk level
2. Collect info/risk analysis – ID assets + assign asset value, ID vulnerabilities + threats, calculate risks, cost/benefit analysis, uncertainty analysis
3. Define recommendations – defend/mitigate/transfer/avoid/accept risk

Risk = likelihood * value – (%risk alr controlled) + uncertainty
Likelihood – chance a vuln is target of successful attack – 0.1-1 or 1-100
Residual risk = total risk * control gap
Residual risks is the risk that remains after controls have been implemented
Risk plan 4 goals:

1. Eliminate risks
2. Reduce risks that cannot be eliminated to an acceptable level
3. Accept risks, implementing controls that keep them at acceptable level
4. Transfer risks to another org. (insurance)