Information security controls overview

Information Assurance (IA)

- Maintaining following of information during its use, storage, processing and transfer:
    - **Integrity**: No tampering of data from point A to point B, e.g. restraining physical access.
    - **Availability**: At all times data needs to be available to those who need it, e.g. stock market
    - **Confidentiality**: No leaks, e.g. ensuring policies are in-place
    - **Authenticity**: Only those who are authorized can access something
    - **Non-repudiation**: If you do something, you cannot say I did not do it, e.g. signatures, log files, camera videos.
- Processes to achieve information assurance are:
    - Security policies
    - Network and user authentication strategy
    - Identification of vulnerabilities and threats e.g. pen-testing
    - Identification of problems in the system and resource requirements
    - Plan design for the identified requirements
    - Certification and accreditation to find vulnerabilities and remove them
    - Training for employees

Types of control

- By type
    - **Physical controls**
        - E.g. fences, doors, locks and fire extinguishers
    - **Technical controls**
        - Also known as ***logical controls***
        - E.g. security tokens
    - **Administrative controls**

        - E.g. security policies and continuity of operations plans are administrative control

- By function
    - **Preventative controls**
        - Prevents the threat from coming in contact with the weakness
        - E.g. authentication, encryption (such as IPSec)
    - **Detective controls**
        - Used after a discretionary event.
        - E.g. audits, alarm bells, alerts
    - **Corrective controls**
        - Put in place after the detective internal controls discover a problem
        - E.g. backups and restore

Information Security Management Program

- All activities the organization takes to protect sensitive information
- E.g. security policies, rules, standards, business resilience, training and awareness, security metrics and reporting.

Enterprise Information Security Architecture (EISA)

- Regulates organizations structure and behavior in terms of security, processes and employees.
- Includes requirements, process, principles and models
- Goals:
    - Real time monitoring of organization's network
    - Security breach detection and recovery
    - Ensuring cost efficiency of security provisions
    - Helping the IT department to function properly
        - e.g. with policies and education
    - Risk assessment of IT assets

Security management framework

- To reduce risks of any system
    - Risks are never zero but you should reduce as much as u can
- Combination of policies, procedures, guidelines and standards

Defense in Depth

- Also known as **defence in depth**
- 📝 Using multiple layers for protection
- Like a tower defence game
- Provides redundancy in the event a security control fails or a vulnerability is exploited
- Layers:
    i. **Policies, Procedures, Awareness**: Data Classification, Risk Management, Code Reviews, Educations...
    ii. **Physical security**: ID cards, CCTV, fences...
        - Maintenance board should be protected in server room.
        - Not good in schools, universities etc.
    iii. **Perimeter**: Encryption, identities...
        - In front of the internal network where traffic in and out is filtered.
    iv. **Internal network**: Network zoning, firewalls...
    v. **Host**: Antivirus patches, security updates...
        - Individual devices with networking capability e.g. servers / PCs.
    vi. **Services**: Audit logs, authentication, authorization, coding practices.
        - Applications running on hosts
    vii. **Data**: Backups, encryption...