TOPIC 3: LEGISLATION DETAILS

Lecturer: Mark Gillan

ISO/IEC 27001 (INFORMATION SECURITY MANAGEMENT SYSTEM - ISMS)

- Establishes a framework for managing sensitive company information.
- Risk assessment and mitigation strategies.
- Policies on data protection, confidentiality, and integrity.
- Incident response and business continuity planning.
- Regular audits and compliance monitoring.
- Employee training on cybersecurity best practices.
- Certification requires regular audits and compliance checks.

Summary & Legal Details:

- ISO/IEC 27001 is an internationally recognised standard that provides a systematic approach to managing information security risks. Organisations can achieve certification by implementing an Information Security Management System (ISMS) with policies, risk assessments, and controls. Compliance is voluntary but often required for business contracts, especially in finance, healthcare, and IT.

ISO/IEC 27035 (INFORMATION SECURITY INCIDENT MANAGEMENT)

- Guidelines for detecting, reporting, and responding to security incidents.
- Defines roles and responsibilities for incident management.
- Incident categorisation and prioritisation framework.
- Root cause analysis and lessons learned for continuous improvement.
- Communication protocols for internal and external stakeholders.
- Integration with business continuity and disaster recovery planning.

Summary & Legal Details:

- ISO/IEC 27035 provides a framework for identifying and responding to security incidents, including cyberattacks, breaches, and insider threats. It ensures that organisations have a structured incident response plan. Though not legally binding, organisations adopting it improve security compliance with GDPR, ISO 27001, and regulatory frameworks.

INVESTIGATORY POWERS (SCOTLAND)

- Regulates law enforcement access to communications data.
- Covers surveillance, interception of communications, and equipment interference.
- Defines lawful access and oversight mechanisms.
- Data retention policies for telecommunications providers.
- Protection of personal privacy versus national security interests.
- Role of judicial and regulatory oversight bodies.

Summary & Legal Details:

- The **Investigatory Powers Act 2016** (UK-wide, with specific provisions for Scotland) allows government agencies to monitor digital communications for law enforcement, national security, and crime prevention. Authorities can access metadata and stored communications under strict oversight. Penalties for unlawful interception include imprisonment (up to **2 years**) and unlimited fines.

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

- Provides public access to information held by Scottish public authorities.
- Ensures transparency and accountability in government and public services.
- Outlines exemptions for national security, personal data, and confidentiality.
- Defines timeframes for responding to FOI requests.
- Enforcement mechanisms and appeal processes.
- Responsibilities of organisations handling requests.

Summary & Legal Details:

- The law requires Scottish public authorities to disclose requested information unless it falls under exemptions (e.g., personal data, law enforcement). Organisations must respond within **20 working days**, or risk enforcement by the **Scottish Information Commissioner**. Non-compliance can result in legal action and reputational damage.

PROTECTION OF INTERNET OF THINGS (IOT) DEVICES

- Security by design principles for IoT manufacturers.
- Default password restrictions and mandatory security updates.
- User authentication and encryption requirements.
- Secure data transmission and storage standards.
- Continuous monitoring for vulnerabilities and threats.
- Consumer awareness and regulatory compliance obligations.

Summary & Legal Details:

- The **Product Security and Telecommunications Infrastructure Act 2022 (UK)** mandates security features in smart devices, such as unique passwords and disclosure of vulnerabilities. Companies failing to comply can face **fines of up to £10 million or 4% of global turnover**.

INTELLECTUAL PROPERTY RIGHTS (IPR)

- Protection of digital assets and creative works.
- Legal frameworks for copyright, patents, and trademarks.
- Licensing and fair use considerations.
- Consequences of IP infringement and enforcement measures.
- Employee and organisational obligations regarding IP.
- Cybersecurity measures to prevent IP theft.

Summary & Legal Details:

- IPR laws protect original works from unauthorised use. **Copyright lasts:**
  - **Literary, artistic, music, and dramatic works**: **70 years after the author's death**.
  - **Sound recordings**: **70 years from publication**.
  - **Broadcasts**: **50 years**.
  - **Published editions**: **25 years**.
- Infringement can result in **civil lawsuits** and **criminal penalties** including **fines or imprisonment**.

COPYRIGHT, DESIGNS AND PATENTS ACT 1988

- Protects original works (text, images, software, etc.).
- Defines copyright duration and ownership rights.
- Criminal offences for copyright infringement (e.g., software piracy).
- Fair use exceptions for research, education, and criticism.
- Protection for software developers and digital content creators.
- Digital Rights Management (DRM) enforcement mechanisms.

Summary & Legal Details:

- This Act protects intellectual property and grants rights to creators. Copyright infringement can result in:

- **Up to 10 years in prison**.
- **Unlimited fines** for large-scale infringement.
- Seizure of infringing materials.

SOFTWARE LICENSING

- Types of software licences (proprietary, open-source, freeware).
- Compliance with terms and conditions of software usage.
- Risks of unlicensed or pirated software.
- Software asset management strategies.
- Vendor and third-party software contract agreements.
- Security implications of unpatched or outdated software.

Summary & Legal Details:

- Using unlicensed software breaches copyright law and can result in **civil lawsuits**, financial penalties, and loss of business credibility.

END USER LICENCE AGREEMENTS (EULAS)

- Legal contracts between software providers and users.
- Outlines permitted and prohibited software usage.
- Liability disclaimers and limitations of warranty.
- Data collection, privacy, and user consent considerations.
- Dispute resolution and termination clauses.
- Compliance obligations for organisations using third-party software.

Summary & Legal Details:

- EULAs establish user rights and limitations. Breaching an EULA may lead to **legal action, termination of service, and financial damages**.

COMPUTER MISUSE ACT 1990

- Defines offences related to unauthorised access to computer systems.
- Covers hacking, malware deployment, and data theft.
- Criminal penalties for cybercrimes.
- Protection against Denial of Service (DoS) attacks.
- Corporate responsibilities for preventing misuse.
- Enforcement and investigative powers of authorities.

Summary & Legal Details:

- This Act criminalises hacking and cybercrime:
- **Unauthorised access**: **Up to 2 years in prison and fines**.
- **Intent to commit further offences**: **Up to 5 years**.
- **Serious offences (e.g., major cyberattacks)**: **Up to life imprisonment**.

ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (USA)

- Regulates interception and access to electronic communications.
- Governs email privacy, mobile data, and cloud storage protections.
- Restrictions on government and corporate surveillance.
- User consent requirements for data collection and monitoring.
- Jurisdictional challenges for international organisations.
- Legal obligations for businesses handling US-based user data.

Summary & Legal Details:

- The ECPA restricts unauthorised surveillance but allows law enforcement access under warrants. Violations can result in **fines and imprisonment of up to 5 years**. This law affects UK companies dealing with US data.