Introduction to the class

Enabling you to manage and reduce cybersecurity risks effectively, regardless of the organisation’s size or maturity level.

Our Target Audiences

Security Newcomers

Professionals relatively new to information security who are unsure where the business value lies in an Information Security Management System (ISMS).

- Early-career professionals
- Business-focused learners
- Those seeking to understand ISMS value

Security Experts

Experienced security professionals and leaders seeking traction and funding for strategic solutions like an ISMS.

- Security professionals
- Leadership teams
- Those requiring executive buy-in

Core Objectives

Five strategic areas that form the foundation of our comprehensive security curriculum, designed to transform the organisation's approach to cybersecurity risk management.

1. Establish Security as a Strategic Investment

Return on Investment Focus

A key objective is to help organisations understand that security, particularly implementing robust practices such as an ISMS, delivers a positive return on investment (ROI).

The lessons demonstrate the *why, what, and how* an organisation can realise ROI that aligns with its specific business needs.

2. Develop Robust Security Governance

The curriculum focuses on establishing high-level strategy, expectations, and policy for cybersecurity risk management, aligned with the GOVERN Function.

01

Mission Alignment

Understanding the organisation's mission and stakeholder expectations to create meaningful security strategies.

02

Strategic Integration

Aligning the security function with the organisation's strategy, goals, mission, and objectives.

03

Due Diligence Implementation

Establishing and practising formal plans and policies to demonstrate **due diligence and due care**.

04

Documentation Framework

Defining security documentation including policies, standards, procedures, and guidelines.

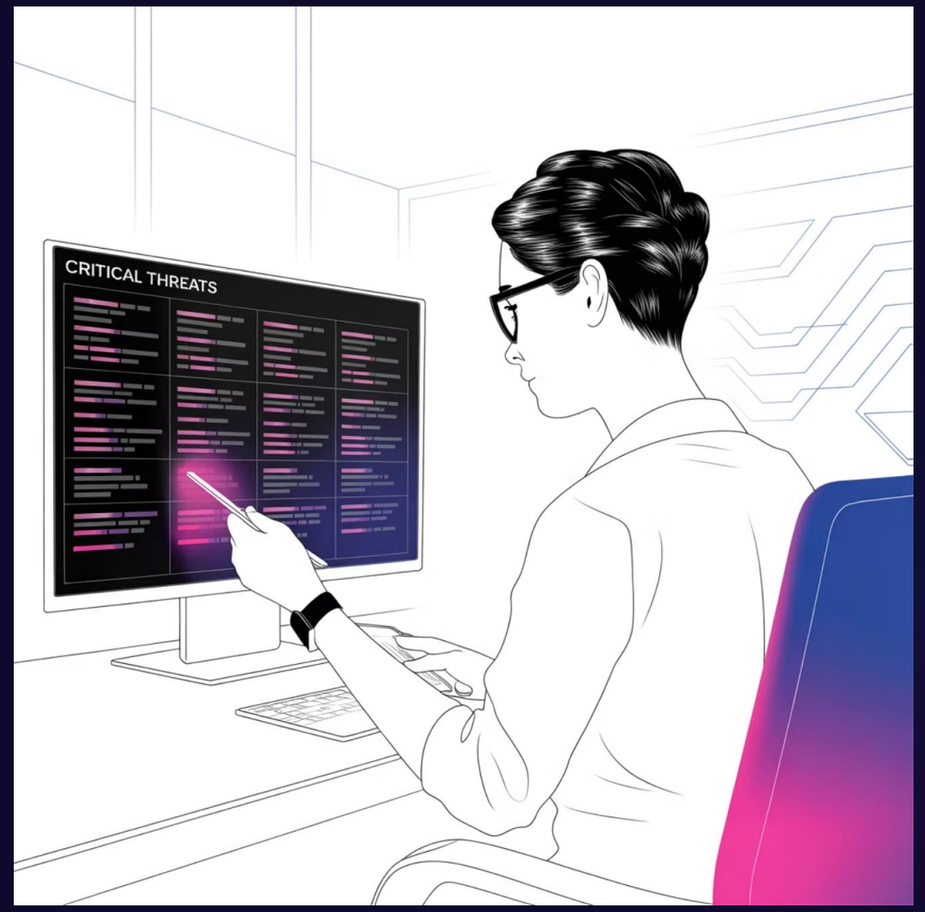
05

Organisational Structure

Establishing clear roles, responsibilities, and authorities (GV.RR) throughout the organisation.

3. Risk Management & Asset Protection

A significant portion of the lessons addresses identifying and managing internal and external cybersecurity risks through systematic approaches.



Risk Management Process

Learning qualitative and quantitative analysis to identify threats, vulnerabilities, and prioritise responses effectively.

CIA Triad Foundation

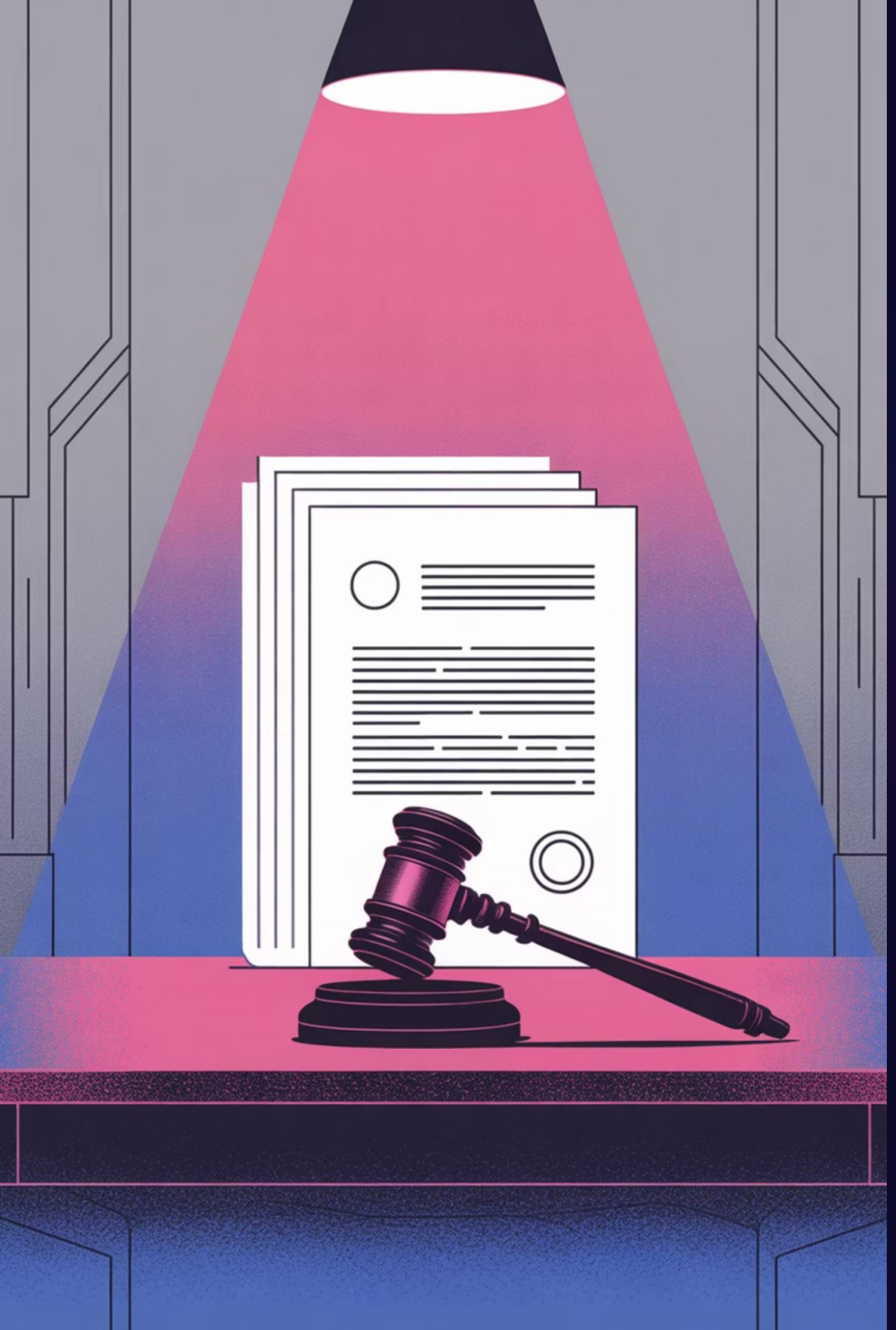
Understanding Confidentiality, Integrity, and Availability as foundational goals of security infrastructure.

Asset Classification

Protecting assets by correctly identifying and classifying information and assets through Data Classification.

Security Controls

Applying control baselines and secure design principles, including **Defence in Depth** and **Zero Trust**.



4. Ensure Legal & Regulatory Compliance

The lessons cover the critical area of compliance, ensuring organisations understand their obligations to legal, regulatory, and contractual requirements.

Privacy & Data Laws

Specific considerations for privacy and data handling laws and compliance frameworks.

Third-Party Risk

Contracting and managing third-party risks through Supply Chain Risk Management (SCRM) and Service Provider Management.

Compliance Programmes

The importance of formal compliance programmes to avoid legal and administrative penalties whilst maintaining business operations.

5. Cultivate Human Capital & Resilience

Security Awareness Programmes

Developing and maintaining comprehensive security awareness, education, and training programmes (PR.AT) tailored to organisational needs.

Social Engineering Defence

Training personnel on recognising social engineering attacks and implementing data handling best practices across all departments.

Incident Response Planning

Establishing and maintaining **incident response (IR) and business continuity planning (BCP)** capabilities for preparation, detection, analysis, response, and recovery.

> By covering these strategic areas, the lessons aim to simplify information security and equip both newcomers and experts with the essential knowledge needed to build, implement, manage, and continuously improve robust security programmes.