



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance Week 4 : Planning for Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- How governance turns Law and Ethics into actionable strategy.
- This lecture bridges compliance (week 3) to broader security management.

Key Concepts

- Governance: How organisations control security.
- Strategy: Planning to protect data long-term.
- Regulatory acts: Security to business

Introduction to the Management of Information Security

- InfoSec programs rely on policies, standards, and practices as the base for architecture and blueprints.
- Functions as part of the organisation's management team but with distinct objectives.
- While **Infosec** focuses on the Confidentiality, Integrity, Availability tenets (CIA) **IT** focuses on the effective and efficient information processing.

The 6 Ps in Infosec Management

- InfoSec management handles specialised responsibilities termed the "Six Ps"
 - Planning
 - Policy
 - Programs
 - Protection
 - People
 - Project management

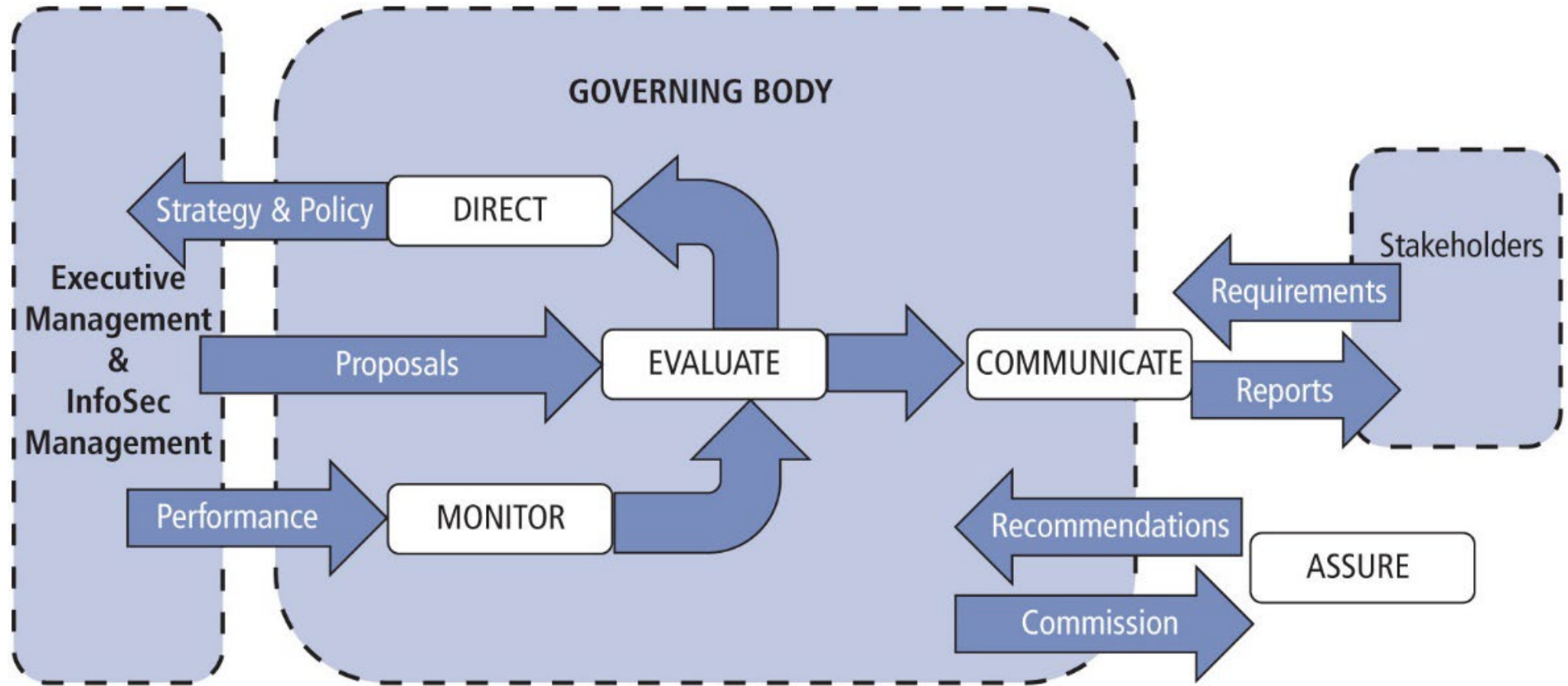
Information Security Planning and Governance

Governance in Organisations

- **Governance** refers to the responsibilities and practices of the board and executive management to:
 - Provide strategic direction
 - Ensure objectives are met
 - Manage risks effectively
 - Use organisational resources responsibly
- **GRC Approach:** Strategic planning and corporate responsibility are best managed through **Governance, Risk Management, and Compliance (GRC)**.

Governance in Information Security

- Strategic Importance
 - Information security governance is a key part of strategic planning.
 - Its significance has increased due to evolving security threats and regulatory demands.
- High-Level Management Involvement
 - InfoSec objectives must be addressed at the highest levels of management to ensure effectiveness and long-term sustainability.
 - Security programmes should not be limited to IT departments, as they must protect all organisational information assets, not just IT systems.



ISO 27014 Governance processes

Information Security Governance Roles And Responsibilities



Information Security Governance Goals

- Aligning information security with business goals to achieve organisational objectives.
- Managing and mitigating risks to protect information resources.
- Efficient use of security knowledge and infrastructure for resource management.
- Monitoring and reporting performance metrics to ensure goals are met.
- Optimising security investments to maximise value delivery.

Effective Planning in Information Security Management

- **Maximising Resources**
 - In environments with limited human and financial resources, strategic planning ensures optimal use of available materials.
- **Balancing Immediate and Long-Term Needs**
 - While CISOs and InfoSec managers must respond to urgent threats, they should also allocate resources to sustain the long-term success of the InfoSec programme.

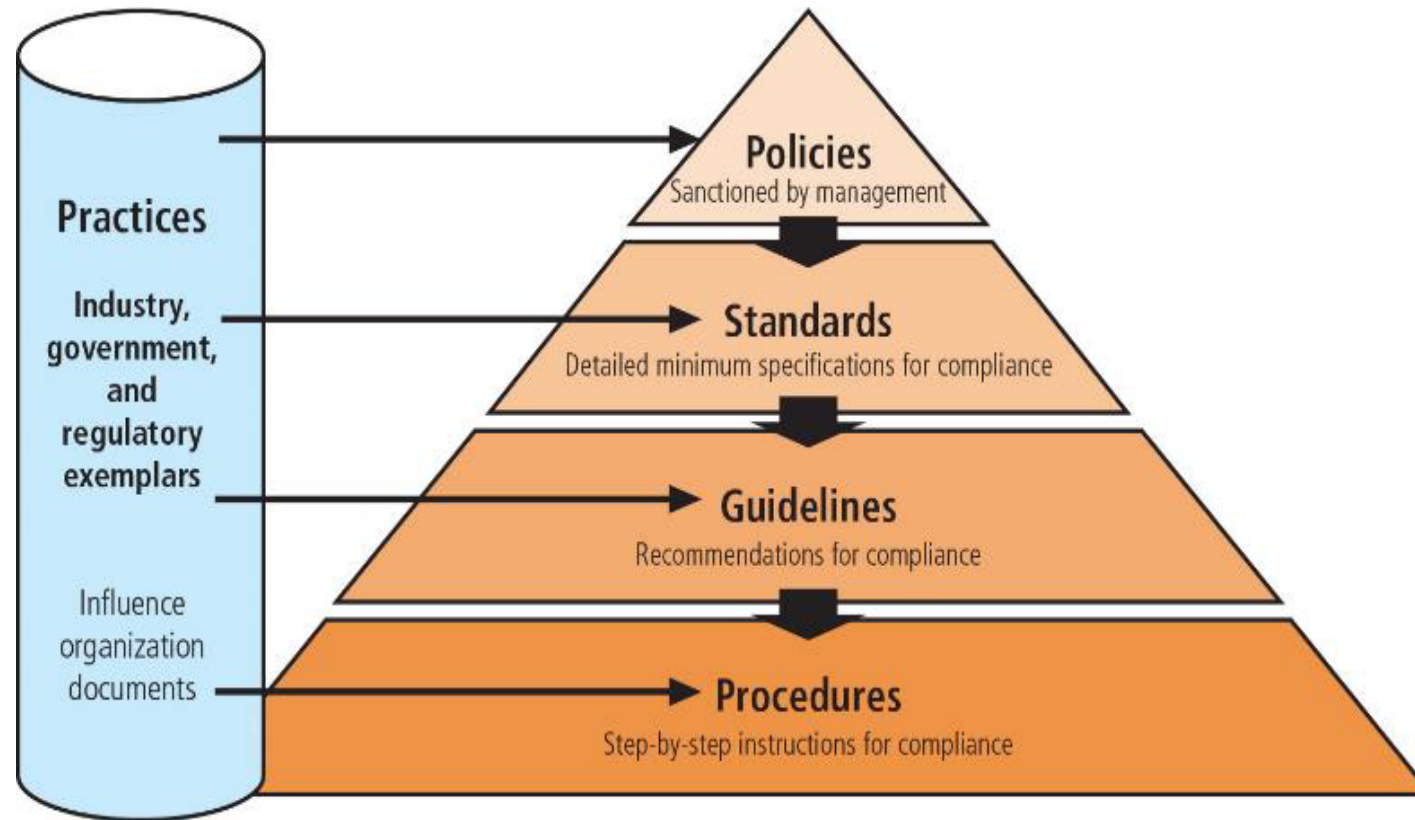
Information Security Policy, Standards, and Practices

- Management from communities of interest must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and how technologies should be used.
- Policies should never contradict law, must be able to stand up in court, and must be properly administered.
- Security policies are the least expensive controls to execute but most difficult to implement properly.

Policy as the Foundation for Planning

- Policy functions as organizational law that dictates acceptable and unacceptable behaviour
- Standards: more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy.
- For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of the organization, and uniformly enforced.

Policies, Standards, Guidelines, And Procedures



Developing and Implementing Effective Security Policy

- For policies to be effective and legally defensible, the following must be done properly:
 - **Development**—They must be written using industry-accepted practices and formally approved by management.
 - **Dissemination**—They must be distributed using all appropriate methods.
 - **Reading**—They must be reviewed by all employees.
 - **Comprehension**—They must be understood by all employees.
 - **Compliance**—They must be formally agreed to by act or affirmation.
 - **Enforcement**—They must be uniformly applied to all employees.

Precursors to Planning

Foundations for Effective Planning

- To implement effective planning, organisational leaders build on existing frameworks that define the organisation's:
 - Ethical stance
 - Entrepreneurial approach
 - Philosophical perspective
- A **key precursor document** is an essential element or document that helps shape and guide the planning process. It includes:
 - A Mission statement
 - A Vision statement
 - A values statement.

The Mission Statement

- Purpose and Scope

- Clearly states what the organisation does and for whom
- Defines its core business activities and operational areas
- Example – GreenCup Ltd

"GreenCup Ltd designs and manufactures high-quality reusable coffee cups and accessories for eco-conscious consumers and businesses across the UK."

The Mission Statement

- Purpose and Scope

- Clearly states what the organisation does and for whom
- Defines its core business activities and operational areas
- Example – GreenCup Ltd

"GreenCup Ltd will be the leading provider of sustainable drinkware, ensuring every café, office, and household in the UK chooses reusable over disposable."

The Vision Statement

- Looking to the Future
 - Expresses the organisation's long-term aspirations
 - Defines where the organisation aims to be in the future
 - Should be ambitious and inspiring
 - Example – GreenCup Ltd

"GreenCup Ltd values sustainability, innovation, integrity, and social responsibility, ensuring our products support a greener future while maintaining the highest ethical and environmental standards."

The Values Statement

- Guiding Principles
- Defines the organisation's fundamental beliefs and standards
- Sets benchmarks for behaviour and decision-making
- Provides a foundation for corporate ethics and accountability
- Example – Random Widget Works

"Random Widget Works values commitment, honesty, integrity, and social responsibility among its employees and is committed to providing its services in harmony with its corporate, social, legal, and natural environments."

Strategic Planning for Security

Strategic Planning

Definition

- Strategic planning defines the long-term direction of an organisation and determines how resources will be allocated to achieve its goals.

Purpose

- It helps focus organisational efforts and resources on clear objectives in a constantly changing environment.

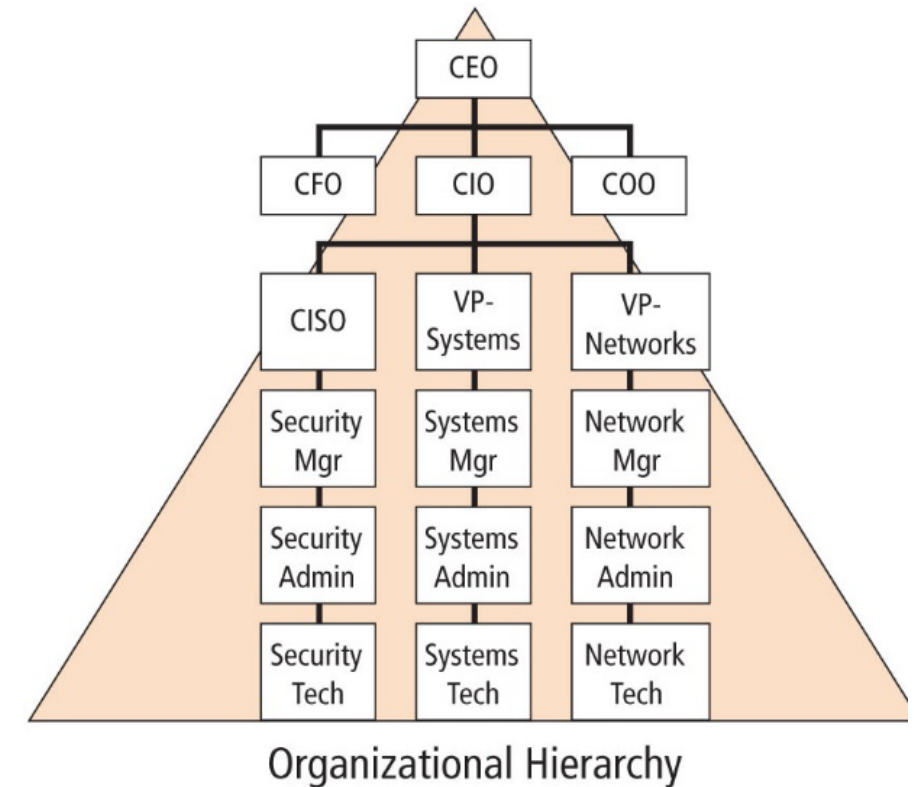
Process

1. General strategy is refined into specific strategies.
2. Strategic planning is further developed into tactical and operational plans.

Top-down strategic Planning

Information Security's Role

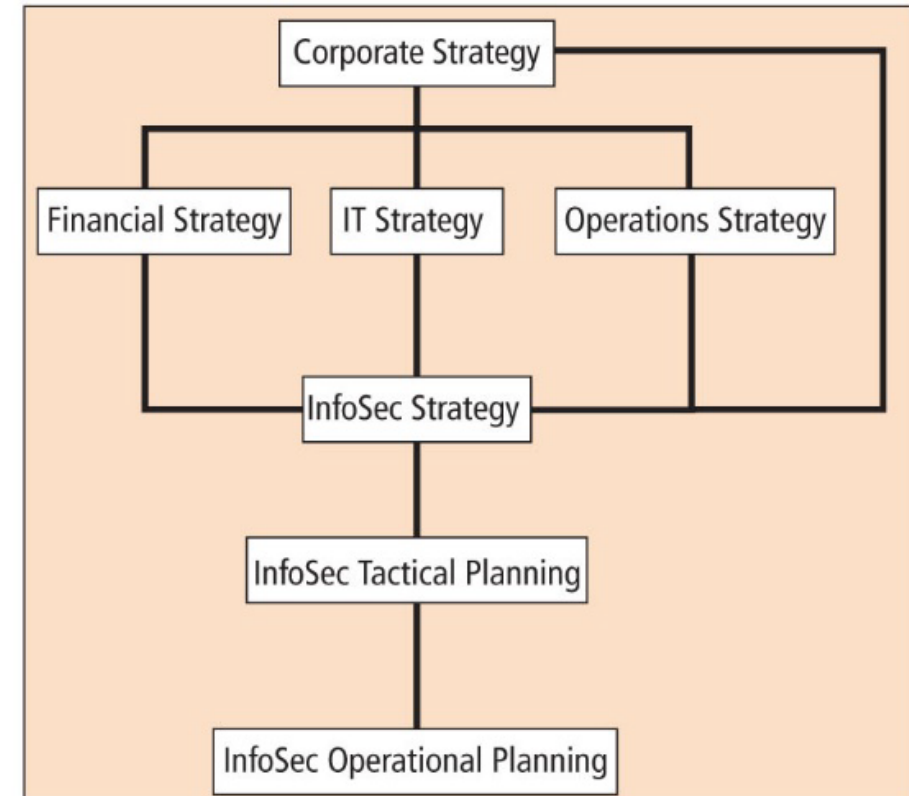
- InfoSec must align with the strategic plans of all business units, not just IT.
- A potential conflict exists between IT (focused on efficiency) and InfoSec (focused on protecting information assets).



Planning hierarchy

Hierarchy of Planning

- General strategy is expanded into strategic plans for major divisions.
- Each division further refines these into more specific objectives at different levels.
- Executives must balance organisational goals with the capabilities and needs of each unit.



Planning Levels

Process of Translating Strategy into Action

Strategic Plans →

- Define high-level organisational goals.

Tactical Plans →

- Develop strategies to achieve these goals within business units.

Operational Plans →

- Outline specific actions that are measurable, achievable, and time-bound.

Basic Components of a Typical Strategic Plan

1. Executive Summary
2. Mission, Vision, and Values Statements
3. Organisational Profile and History
4. Strategic Issues and Challenges
5. Organisational Goals and Objectives
6. Major Business Units (or Product/Service) Goals and Objectives
7. Appendices (as applicable, including market analyses, internal/external surveys, budgets, and R&D projections)

Key Regulatory Acts

ISO 27000 series

- One of the most widely referenced security models
- Standard framework for information security that states organizational security policy is needed to provide management direction and support
- Purpose is to give recommendations for information security management with the goal of certification
- Provides a starting point for developing organizational security

The Sections of ISO/IEC 27002- What it covers

- Foreword
- 0. Introduction
- 1. Scope
- 2. Normative references
- 3. Terms and definitions
- 4. Structure of this standard
- 5. Information security policies
- 6. Organization of information security
- 7. Human resource security
- 8. Asset management
- 9. Access control
- 10. Cryptography
- 11. Physical and environmental security
- 12. Operations security
- 13. Communication security
- 14. System acquisition, development, and maintenance
- 15. Supplier relationships
- 16. Information security incident management
- 17. Information security aspects of business continuity management
- 18. Compliance

NIST

- NIST's approach to managing risk in the organisation, titled the Risk Management Framework (RMF), emphasises on:
 - Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
 - Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes
 - Providing essential information to help senior leaders make decisions about accepting risk to an organization's operations and assets, individuals, and other organizations arising from the use of information systems

NIST Cybersecurity Framework

- Consists of three fundamental components:
 1. **Framework core:** set of information security activities an organization is expected to perform and their desired results:
 - Identify
 - Protect
 - Detect
 - Respond
 - Recovery
 2. **Framework tiers:** help relate the maturity of security programs and implement corresponding measures and functions
 - Tier 1: Partial
 - Tier 2: Risk Informed
 - Tier 3: Repeatable
 - Tier 4: Adaptive
 3. **Framework profile:** used to perform a gap analysis between the current state and a desired state of information security/risk management

NIST Cybersecurity Framework

- Seven-step approach to implementing/improving programs:
 1. Prioritize and scope
 2. Orient
 3. Create current profile
 4. Conduct risk assessment
 5. Create target profile
 6. Determine, analyze, prioritize gaps
 7. Implement action plan

References

- Slides are devised from the recommended books:
 - Whitman, M.E., Mattord, H.J., Principles of Information Security . Cengage Learning 658.
 - Whitman, ME., Mattord H.J., Readings and Cases in Information Security Law and Ethics. Cengage
- Some of the slides are devised from my own notes



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk