



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

ACCA7028

Data Security and Compliance

Week 4 : Governance and Strategic Planning for Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Builds on Compliance: Law and Ethics—laws set the rules, ethics guide decisions, and now governance turns those into actionable strategy.
- Fits Data Security, Governance and Compliance—this lecture bridges compliance (week 3) to broader security management.

Key Concepts

- Governance: How organizations control security.
- Strategy: Planning to protect data long-term.
- Hook: “Compliance keeps you legal—governance keeps you alive.”

What is Security Governance?

Introduction to the Management of Information Security

- An information security program begins with policies, standards, and practices, which are the foundation for the information security architecture and blueprint.
- As part of the organisation's management team, the InfoSec management team operates like all other management units.
- The InfoSec management team's goals and objectives differ from those of the IT and general management communities in that the InfoSec management team is focused on the secure operation of the organization.
- Some of the InfoSec management team's goals and objectives may be contrary to or require resolution with the goals of the IT management team
- The primary focus of the IT group is to ensure the effective and efficient processing of information.
- The primary focus of the InfoSec group is to ensure the confidentiality, integrity, and availability of information.

Defining Governance

- Framework of policies, roles, and processes to manage security.
- Ensures compliance, aligns with business goals.
- Example: Board-level oversight after a breach.

Information Security Planning and Governance

- **Strategic planning** sets the long-term direction to be taken by the organization and each of its component parts.
- Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined **goals**.
- The leadership of the information security function that delivers strategic planning and corporate responsibility is best accomplished using an approach industry refers to as **governance, risk management, and compliance (GRC)**.

Information Security Planning and Governance

- InfoSec objectives must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach.
- In organizations with formal boards of directors, the boards should be the basis for **governance** review and oversight.
- **Information security governance** is the application of the principles and practices of corporate governance to the information security function, emphasizing the responsibility of the board of directors and/or senior management for the oversight of information security in the organization.

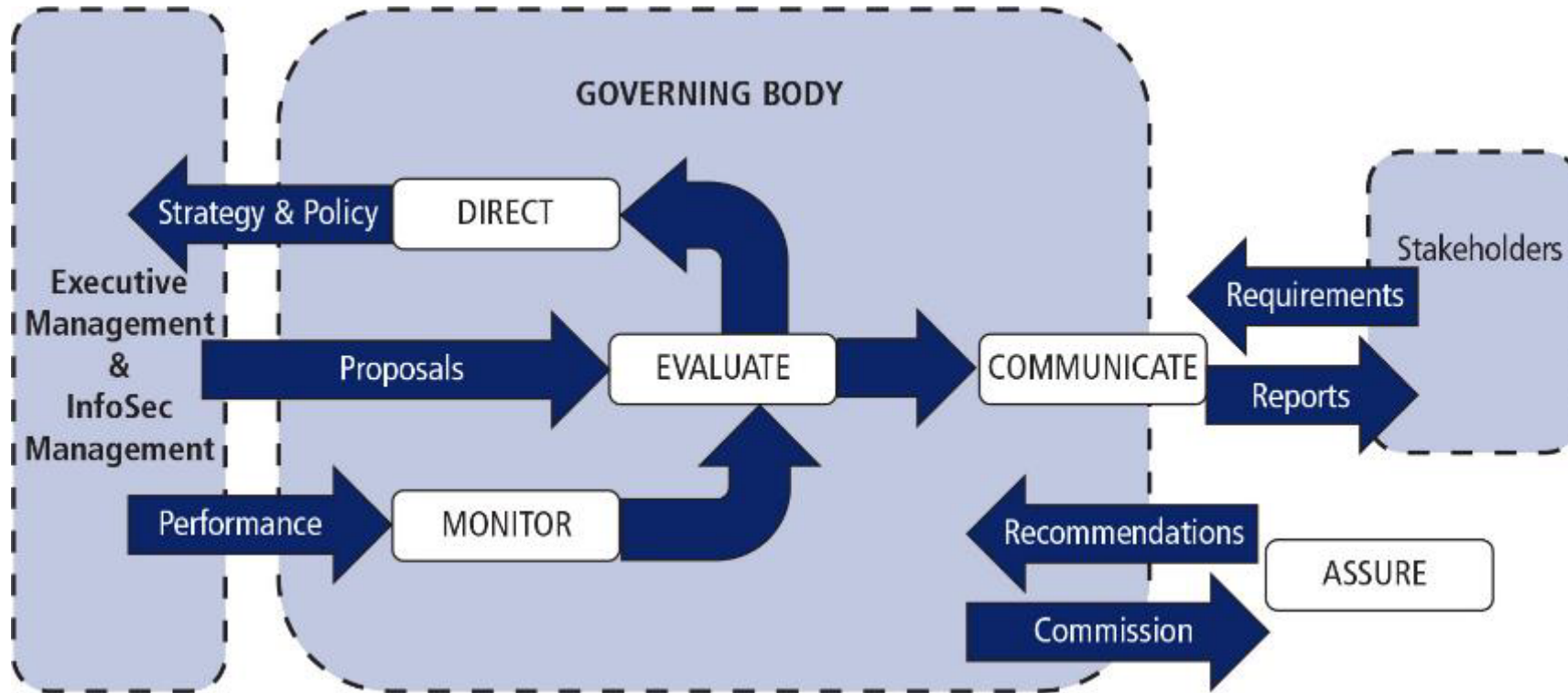
Governance vs. Management

- Governance: Sets direction (e.g., “We prioritise GDPR”).
- Management: Executes it (e.g., “Encrypt all drives”).
- Visual: Hierarchy—Board → CISO → IT team.

Information Security Governance

- ISO 27014:2013: the ISO 27000 series standard for Governance of Information Security—specifies six high-level “action-oriented” information security governance principles:
 1. Establish organization-wide information security.
 2. Adopt a risk-based approach.
 3. Set the direction of investment decisions.
 4. Ensure conformance with internal and external requirements.
 5. Foster a security-positive environment.
 6. Review performance in relation to business outcomes.

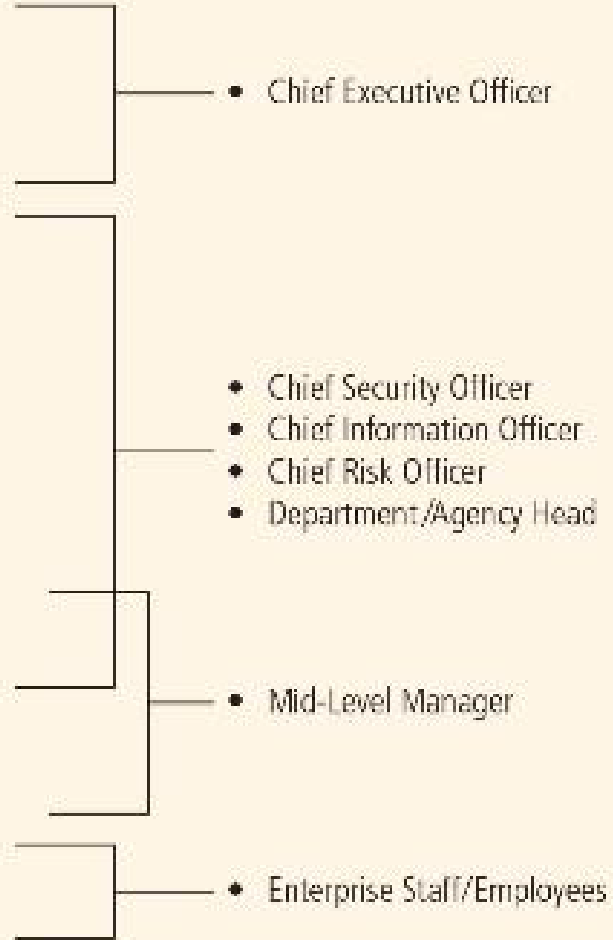
ISO/IEC 27014:2013 Governance Processes



Responsibilities

- Oversee overall corporate security posture (accountable to board)
- Brief board, customers, public
- Set security policy, procedures, program, training for company
- Respond to security breaches (investigate, mitigate, litigate)
- Responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement policy; report security vulnerabilities and breaches

Functional Role Examples



Information Security Governance Roles & Responsibilities

Information security governance goals

1. Strategic alignment of information security with business strategy to support organizational objectives
2. Risk management by executing appropriate measures to manage and mitigate threats to information resources
3. Resource management by using information security knowledge and infrastructure efficiently and effectively
4. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved
5. Value delivery by optimizing information security investments in support of organizational objectives

Information Security Policy, Standards, and Practices

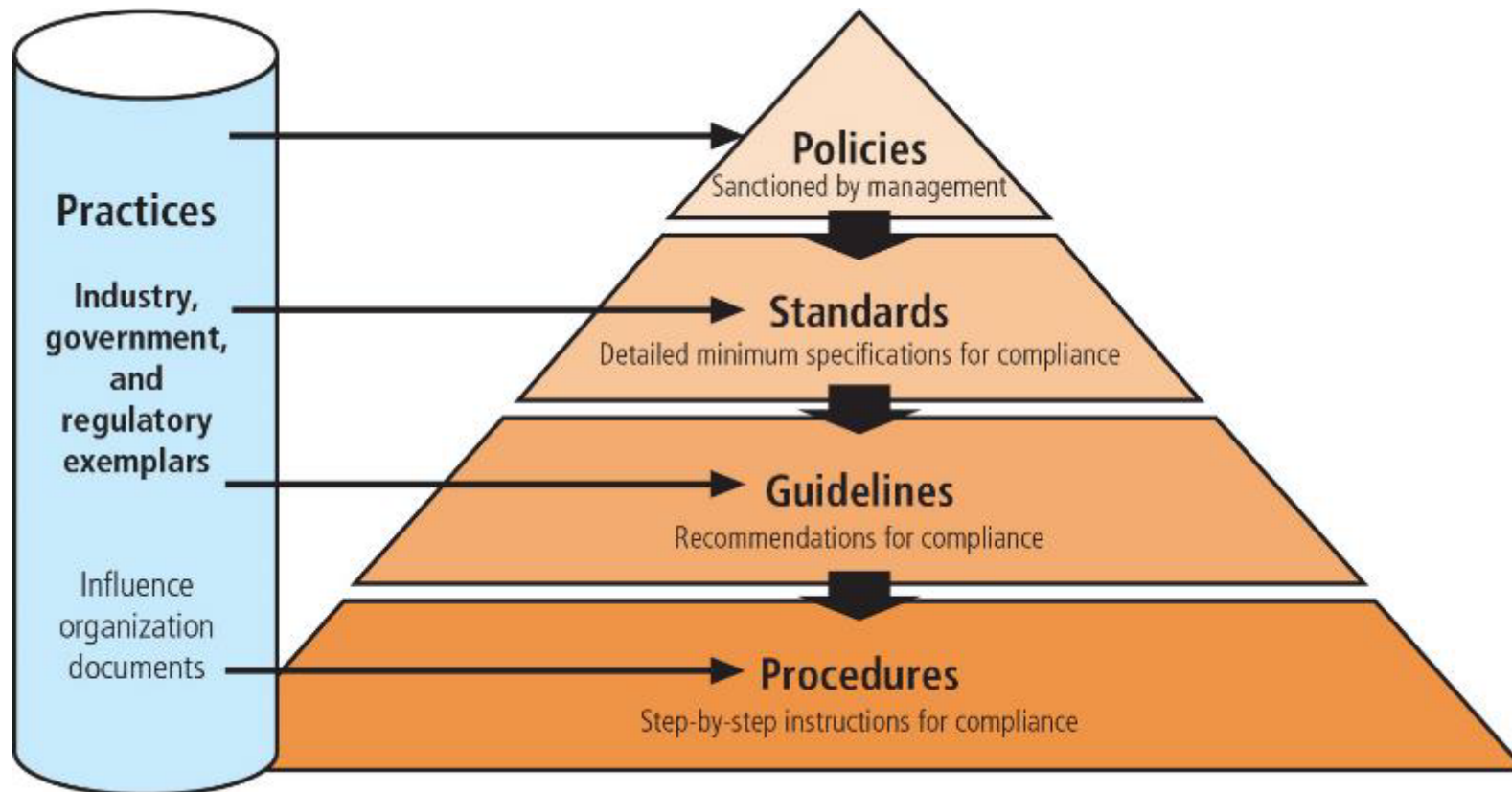
Information Security Policy, Standards, and Practices

- 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 behavior
- 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



Relationship between Policies, Standards, Practices, Procedures, and Guidelines

Policy	"Use strong passwords, frequently changed."
Standard	"The password must be at least 10 characters with at least one of each of these: uppercase letter, lowercase letter, number, and special character."
Practice	"According to <i>Passwords Today</i> , most organizations require employees to change passwords at least every six months."
Procedure	"In order to change your password, first click the Windows Start button; then ... "
Guideline	"We recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password."

Why It Matters

- Mitigates risks, avoids fines (e.g., £20M GDPR hit).
- Case: Equifax 2017—weak governance delayed breach response.

Policies for planning

Policy as the Foundation for Planning

- **An information security policy** provides rules for protection of the organization's information assets.
- Management must define three types of security policy:
 1. Enterprise information security policies
 2. Issue-specific security policies
 3. Systems-specific security policies

Enterprise Information Security Policy

- Sets strategic direction, scope, and tone for all security efforts within the organization
- Executive-level document, usually drafted by or with chief information officer (CIO) of the organization
- Typically addresses compliance in two areas:
 - Ensure meeting of requirements to establish program and assigning responsibilities therein to various organizational components
 - Use of specified penalties and disciplinary action
- EISP elements should include:
 - Overview of corporate philosophy on security
 - Information on the structure of the organization and people in information security roles
 - Fully articulated responsibilities for security shared by all members of the organization
 - Fully articulated responsibilities for security unique to each role in the organization

Issue-Specific Security Policy (ISSP)

1. Addresses specific areas of technology
 2. Requires frequent updates
 3. Contains statement on the organization's position on a specific issue
- Three common approaches when creating and managing ISSPs:
 - Independent ISSP documents, each tailored to a specific issue
 - A single comprehensive ISSP document that covers all issues
 - A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

Systems-Specific Policy (SysSP)

- SysSPs often function as standards or procedures used when configuring or maintaining systems.
- Systems-specific policies fall into two groups:
 - Managerial guidance
 - Technical specifications
- Access control lists (ACLs) can restrict access for a particular user, computer, time, duration—even a particular file.
- Configuration rule policies govern how security system reacts to received data.
- Combination SysSPs combine managerial guidance and technical specifications.

Developing policies

Developing and Implementing Effective Security Policy

For policies to be effective and legally defensible, the following must be done properly:

1. Development—They must be written using industry-accepted practices and formally approved by management.
2. Dissemination—They must be distributed using all appropriate methods.
3. Reading—They must be reviewed by all employees.
4. Comprehension—They must be understood by all employees.
5. Compliance—They must be formally agreed to by act or affirmation.
6. Enforcement—They must be uniformly applied to all employees.

Policy Management

- Policies must be managed, as they constantly change.
- To remain viable, security policies must have:
 - Responsible manager/policy administrator
 - Schedule of reviews
 - Review procedures and practices
 - Policy and revision dates
 - Automated policy management

Strategic Planning

Strategic Planning

- Information security, like information technology, must support more than its immediate parent in the organizational chart
- As all organizational units will be using information, not just IT-based information, the information security group must understand and support the strategic plans (a.k.a strategies) of all business units
- This role may at times conflict with that of the IT department as IT's role is the efficient and effective *delivery* of information and information resources, while InfoSec's role is the *protection* of all information assets

Creating a strategic plan

- After an organization develops a general strategy, it must create an overall strategic plan by extending that general strategy into specific strategic plans for major divisions
- Each level of each division translates those objectives into more specific objectives for the level below
- The conversion of goals from the strategic level to the next lower level relies on the executive's ability to know and understand the strategic goals of the entire organization, to know and appreciate the strategic and tactical abilities of each unit within the organization, and to negotiate with peers, superiors, and subordinates

Planning levels

- Once the organization's overall strategic plan is translated into strategic goals for each major division or operation, the next step is to translate these strategies into objectives that are specific, measurable, achievable, and time-bound
- Strategic plans are used to create tactical plans, which are in turn used to develop operational plans

Basic Components of a Typical Strategic Plan

1. Executive Summary
2. Mission, Vision, and Values Statements
3. Organizational Profile and History
4. Strategic Issues and Challenges
5. Organizational 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)

Security Education, Training, and Awareness Program

Security Education, Training, and Awareness Program

- Once general security policy exists, implement a **security education, training, and awareness (SETA)** program.
- SETA is a control measure designed to reduce accidental security breaches.
- The SETA program consists of security education, security training, and security awareness.
- SETA enhances security by improving awareness, developing skills and knowledge, and building in-depth knowledge.

Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs a formal degree or certificate in security.
- When formal education is deemed appropriate, an employee can investigate degree programs or courses in continuing education from local institutions of higher learning.
- Resources, such as the DHS/NSA-designated National Centers of Academic Excellence program (www.iad.gov/NIETP/index.cfm), can provide additional information on security curriculum.

Security Training

- Training provides members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
- Management of information security can develop customized in-house training or outsource the training program.
- Alternatives to formal training include conferences and programs offered through professional organizations.
- Massive Open Online Courses (MOOCs) are available from vendors such as Coursera (www.coursera.org), with free courses and completion certificates for a nominal fee.

Security Awareness

- Security awareness program: one of the least frequently implemented but most beneficial programs
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to neglect security matters, and risk of employee accidents and failures are likely to increase

References

- Slides are devised from the recommended books:
 - Whitman, M.E., Mattord, H.J., Principles of Information Security . Cengage Learning 658.
 - Management of Information Security 6th Ed by Whitman & Herbert Chapter 4: Governance and Strategic Planning for Security



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