Information Assurance

Part A

Enterprise Governance

Governance

- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Governance

- Governance describes the entire function of **controlling**, or governing, the **processes** used by a **group** to accomplish some **objective**.
- It represents the **strategic controlling function** of an organization's senior management, which is designed to ensure **informed**, prudent **strategic decisions** made in the **best interest** of the organization.

Governance vs. Management

Governance

- Purpose is to set goals
- "*Do the right thing*"

Management

- Purpose is plan, build, execute and monitor activities to achieve goals
- "*Do the thing right*"

Why Does Governance Matter?

- Information is critical to our lives.
- Protecting information is key, but costs and benefits vary.
- How can we be sure we are choosing the appropriate option?

Governance helps align information security with business goals and objectives

Effective Information Security

An effective information security program:

- Supports what the organization is trying to do
- Keeps risk within acceptable levels
- Tracks success and areas of improvement
- Changes with the organization

Goals of Information Security Governance

Six basic goals of a information security governance:

- Strategic alignment
- Risk management
- Value delivery
- Resource optimization
- Performance measurement
- Assurance process integration

Strategic alignment

- Process of ensuring that an organization's goals, objectives, and strategies are integrated and consistent across all levels of the organization.
- Security requirements driven by enterprise requirements that are thoroughly developed to provide guidance on what must be done and a measure of when it has been achieved

Risk Management

- Executing appropriate measures to mitigate risk and reduce potential impacts on information resources to an acceptable level such as:
  - Collective understanding of the organization's threat, vulnerability and risk profile
  - Understanding of risk exposure and potential consequences of compromise
  - Risk mitigation sufficient to achieve acceptable consequences from residual risk
  - Risk acceptance based on an understanding of the potential consequences of residual risk

Value delivery

- Process of ensuring that information security investments, initiatives, and activities contribute to the organization's overall objectives and goals.
- It involves identifying and implementing strategies and practices that enable the organization to maximize the value of its information assets while minimizing the associated risks.

Resource Optimization

- Ensuring that adequate resources (including financial, human, and technical resources) are allocated to support information security initiatives and activities.

Performance measurement

- *Measure how well security is working.*
- Monitoring and reporting on information security processes to ensure that objectives are achieved, including:
  - A defined, agreed-upon and meaningful set of metrics that are properly aligned with strategic objectives and provides the information needed for effective decisions at the strategic, management and operational levels.
  - Measurement process that helps identify shortcomings and provides feedback on progress made resolving issues.
  - Independent assurance provided by external assessments and audits.

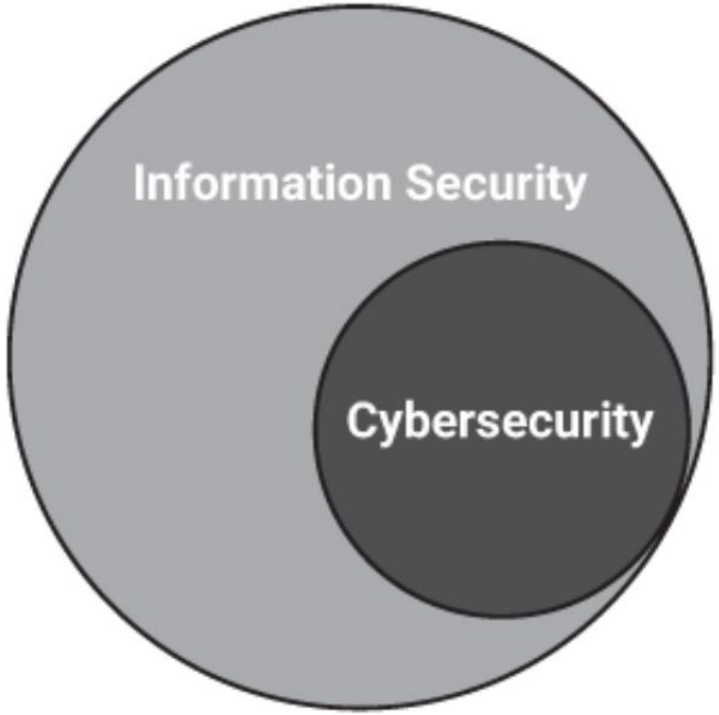
Assurance Process Integration

- *Make security part of regular audits and compliance, not a one-time thing*.
- Integration is important because it ensures that information security is not treated as a separate or standalone function, but rather as an integral part of the organization's overall business operations.
- This helps to ensure that information security risks are identified and managed in a manner that is consistent with the organization's overall risk management framework, and that information security initiatives are aligned with the organization's overall goals and objectives

Scope of IS Governance

- Information Security deals with all aspects of information in any medium (written, spoken, electronic) regardless of whether it is being created, viewed, transported, stored or destroyed.

Information Security and Cyber Security



Organizational Culture aspects in IS Governance

- General Rules of Use / Acceptable use policy
- Ethics
- Legal, Regulatory and Contractual Requirements
- Requirement of content and retention of business records
- Organizational structure, roles and responsibilities
- Board of Director / Senior Management / Steering Committee / CISO

Roles and Responsibilities

Responsibilities	Functional Role Examples
• Oversee overall corporate security posture (accountable to board) • Brief board, customers, public	• Chief Executive Officer
• 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	• Chief Security Officer • Chief Information Officer • Chief Risk Officer • Department/Agency Head
• Communicate policies, program (training)	• Mid-Level Manager
• Implement policy; report security vulnerabilities and breaches	• Enterprise Staff/Employees

Thought Experiment

- A staff member installs free gaming software on the office computer, which later causes a malware infection.
  - Violates: Acceptable Use Policy (AUP)
- An employee finds sensitive salary data of colleagues and decides to leak it on social media.
  - Violates: Ethics
- A hospital fails to protect patient medical records, leading to a data privacy law violation.
  - Violates: Legal/Regulatory Requirements

Thought Experiment

- An accountant deletes financial records after one year, even though the law requires them to be kept for seven years.
  - Violates: Record Retention
- IT staff assume HR will handle background checks for new hires, but HR assumes IT will do it,so the task is missed.
  - Violates: Roles & Responsibilities
- The Board of Directors announces a new security policy but they themselves do not follow it, sending a message that rules are optional.
  - Violates: Leadership Roles (Board/Senior Management)

Thanks a lot