Information Assurance

Domain 1

Information Security Governance

Part B

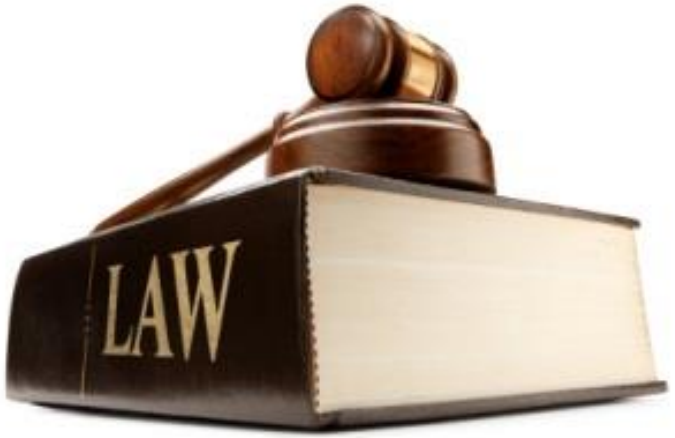
Information Security Strategy

Strategy Constraints

- Legal
- Physical
- Ethics
- Culture
- Costs
- Personnel
- Organizational structure
- Resources
- Capabilities
- Time
- Risk appetite

Legal and Regulatory Requirements

- Information security linked to privacy, Intellectual Property and law
- Security strategies for different regions may be required
- Retention requirements



Physical Constraints

- Include capacity, space, environmental hazards, etc.
- Safety of personnel should also be considered
- Often ignored and can lead to interruptions or breaches
- Disaster recovery should be considered

Ethics and Culture

- Ethics
  - Perception of the enterprise's behavior
  - Influenced by location and culture
- Culture
  - Internal culture
  - Local culture

Costs

- Justify spending based on a project's value.
- Cost-benefit/financial analysis most widely accepted
- Annual Loss Expectancy (ALE)
- Return On Investment (ROI)

Personnel and Organizational Structure

- Personnel
  - Resistance to changes can impact the success of strategy implementation
- Organizational structure
  - Impacts how a governance strategy can be implemented
  - Cooperation is needed
  - Senior management support ensures better collaboration across the organization.

Resources, Capabilities and Time

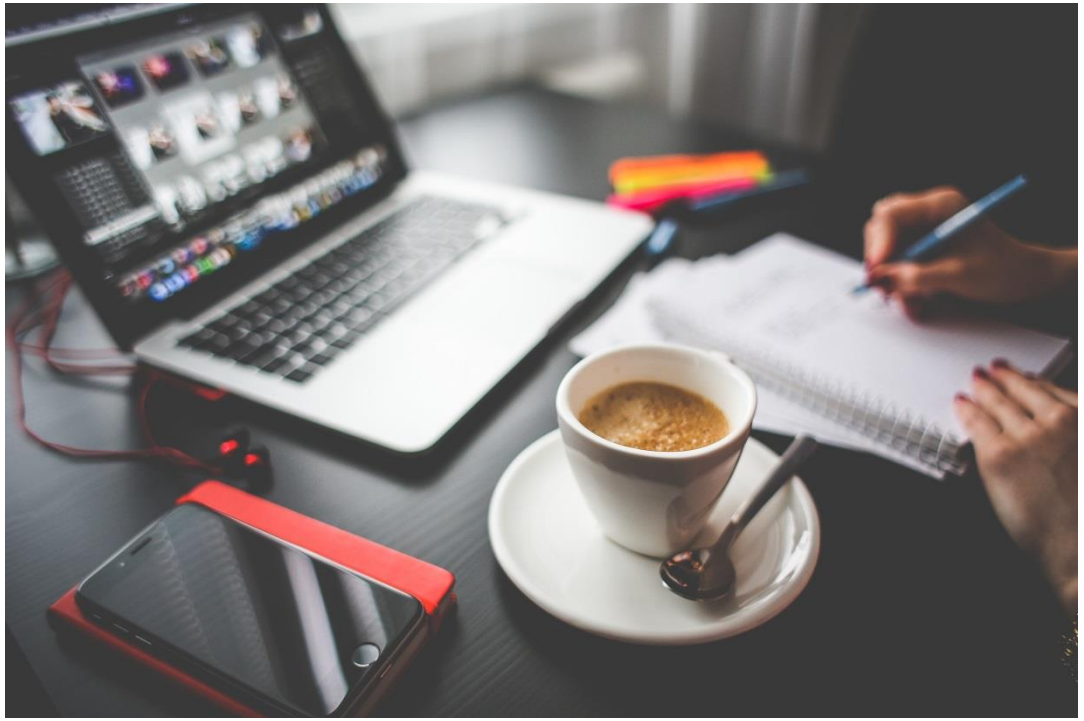
- Resources
  - Consider available budgets, Overall costs and personnel requirements
- Capabilities
  - Expertise and skills
- Time
  - Deadlines/Windows of opportunity

Ongoing Assessment

- The information security strategy needs to be dynamic.
- Update assessments regularly.

Discussion Question

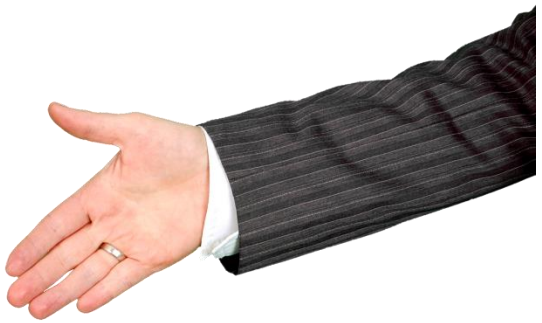
- What are some reasons that the information risk environment changes over time?



Gaining Management Support/Approval

Commitment is Key

- Senior management backing is essential to success
- Information security may need to educate senior managers to get them on board
- Use business language, not technical jargon



Lay the Foundation

- Workshops or briefings can set the stage for strategy implementation.
- Try to anticipate issues/concerns managers already have

Roles and Responsibilities

- Board of Directors
  - Need to be aware of information assets
  - Provided with high-level results of risk assessments and BIAs.
  - Exercise due care in protecting key assets
- Senior Management
  - Ensure needed functions/resources are available
  - Ensure resources are properly utilized
  - Promote cooperation, arbitrate when needed and set priorities

Roles and Responsibilities

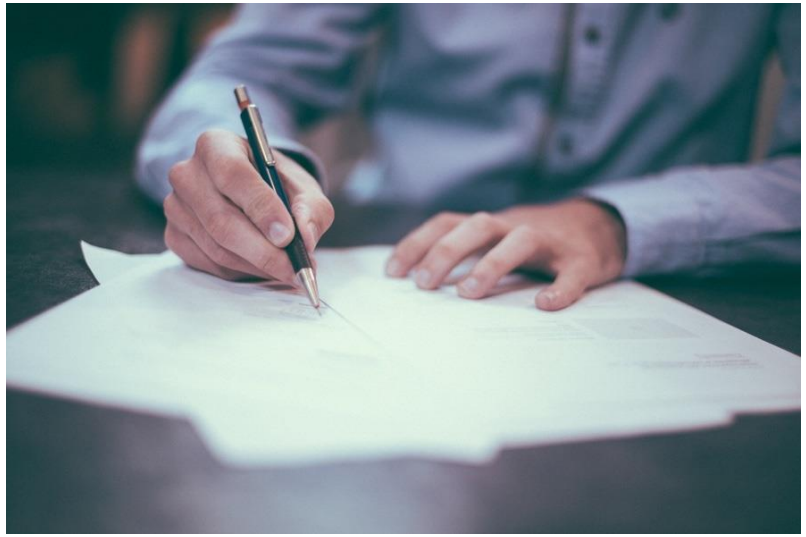
- Steering committee
  - Comprised of senior representatives of groups impacted by information security
  - Ensures alignment of security program with business objectives
- Common topics:
  - Security strategy and integration efforts
  - Specific actions and progress related to business unit support of information security program functions
  - Emerging risk, business unit security practices and compliance issues

Roles and Responsibilities

- Chief Risk Officer
  - Generally responsible for all non-information risk and overall ERM
- Chief Information Officer
  - Responsible for IT planning, budgeting and performance
- Chief Information Security Officer
  - Similar functions as information security manager with more strategic and management elements; IT strategy

The Business Case

- Provides a formal proposal for a project/strategy
  - Likely costs
  - Benefits
- Should have enough detail to explain the why of a project/strategy and what it will deliver back

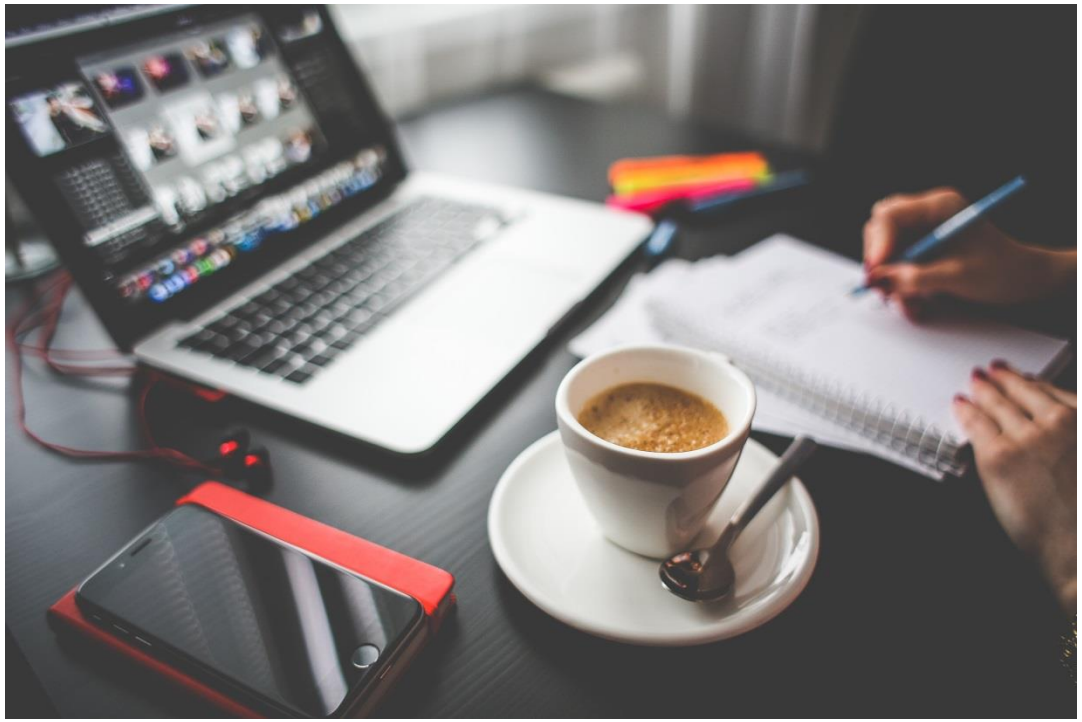


Preparing a Business Case

- Starts with a clear statement of what problem or opportunity a project seeks to address
- Elements of a feasibility study
  - Project scope
  - Current analysis
  - Requirements
  - Recommended approach
  - Evaluation
  - Formal review
- **Note:** The feasibility study focuses on direct, up-front costs, while the business case should focus on total cost of ownership.

Discussion Question

- Who are some of the stakeholders in an organization's information security strategy?



Presenting the Strategy

- Can be used to educate and communicate
- Common factors for acceptance:
  - Aligning security with business objectives
  - Identifying potential consequences
  - Identifying budget items
  - Using common risk/benefit or financial models
  - Defining monitoring and auditing measures

Presenting the Strategy

- Remember: You are the subject matter expert!
  - Be concise, but be honest
  - Senior management may not realize the impact of reputational damage
- Alignment is key: If the strategy is aligned with the business, it is more likely to be approved.

Thanks a lot