CSIT988/CSIT488

Security, Ethics and Professionalism

Week 10: Risk Management: Controlling Risk

Subject Coordinator: *Dr Khoa Nguyen*

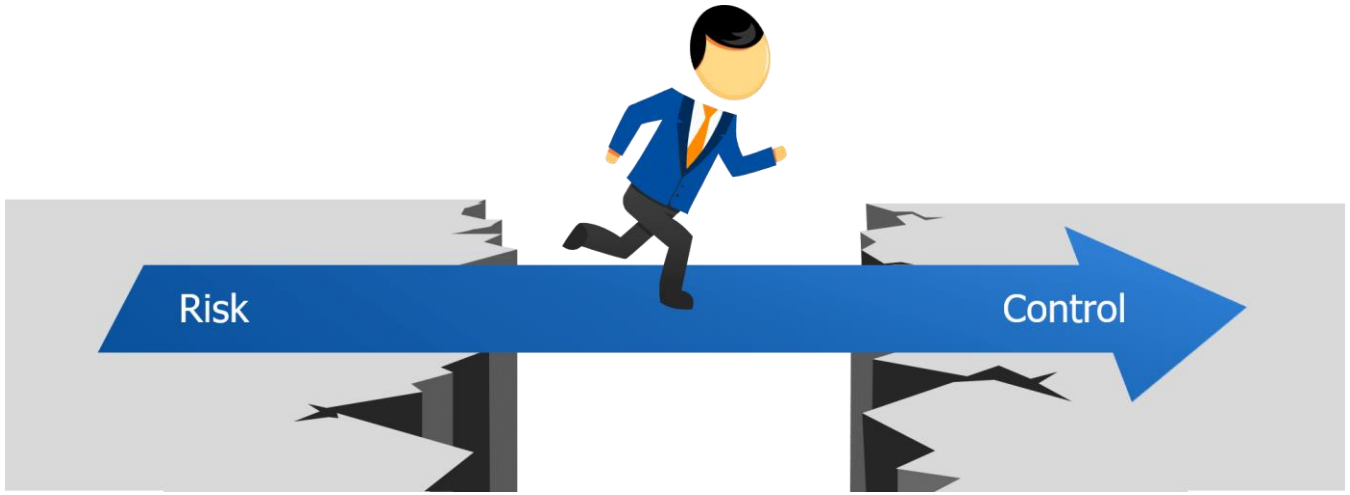
School of Computing and Information Technology

Autumn 2025

Learning Objectives

- Recognize the strategy options used to control risk and be prepared to select from them when given background information
- Evaluate risk controls and formulate a cost-benefit analysis (CBA) using existing conceptual frameworks
- Explain how to maintain and perpetuate risk controls

Reference: Chapter 9 of the textbook



- The concept of “competitive disadvantage” has emerged as a critical factor for organizations nowadays.
- To keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function
  - This environment must maintain confidentiality and privacy and assure the integrity and availability of organizational data
  - These objectives are met by applying risk management principles
- Controlling risk begins with an understanding of what risk mitigation strategies are and how to formulate them.

Risk Control Strategies

- After creating the ranked vulnerability worksheet, an organization must choose one of five basic strategies to control risks
  - **Defense:** Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
  - **Transference:** Shifting the risk to other areas or to outside entities
  - **Mitigation:** Reducing the impact if the vulnerability is exploited
  - **Acceptance:** Understanding the consequences and accepting the risk without control or mitigation
  - **Termination:** Removing or discontinuing the information asset

Risk Defense

- The defense risk control strategy attempts to prevent the exploitation of the vulnerability
- Preferred approach since it seeks to avoid risk rather than deal with it after it has been realized.
- Defense is accomplished through:
  - Application of policy
  - Application of training and education
  - Implementation of technical security controls and safeguards
- Risk can be avoided by countering the threats facing an asset or by eliminating the exposure of a particular asset.

Risk Transference

- The transference control approach attempts to shift the risk to other assets, other processes, or other organizations

- May be accomplished by
  - Rethinking how services are offered
  - Revising deployment models
  - Outsourcing to other organizations
  - Purchasing insurance
  - Implementing service contracts with providers

Risk Mitigation

- The mitigation control approach attempts to reduce the damage caused by the exploitation of vulnerability
  - Using planning and preparation
  - Depends upon the ability to detect and respond to an attack as quickly as possible
- Types of mitigation plans
  - Disaster recovery plan (DRP)
  - Incident response plan (IRP)
  - Business continuity plan (BCP)

Plan	Description	Example	When Deployed	Time Frame
Incident response (IR) plan	Actions an organization takes during incidents (attacks or accidental data loss)	• List of steps to be taken during an incident • Intelligence gathering • Information analysis	As an incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery (DR) plan	• Preparations for recovery should a disaster occur • Strategies to limit losses before and during a disaster • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost technology infrastructure and services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business continuity (BC) plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DR plan's ability to quickly restore operations	• Preparation steps for activation of alternate data centers • Establishment of critical business functions in an alternate location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organizational stability

Risk Acceptance

- The choice to do nothing to protect an information asset, to accept the loss when it occurs
- Before using the acceptance strategy, the organization must:
  - Determine the level of risk to the information asset
  - Assess the attack probability and the likelihood of a successful exploitation
  - Estimate the potential loss from attacks
  - Perform a thorough cost benefit analysis
  - Evaluate controls using each appropriate type of feasibility
  - Decide that the particular asset did not justify the cost of protection
- This control, or lack of control, assumes that it may be a prudent business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure.

Risk Termination

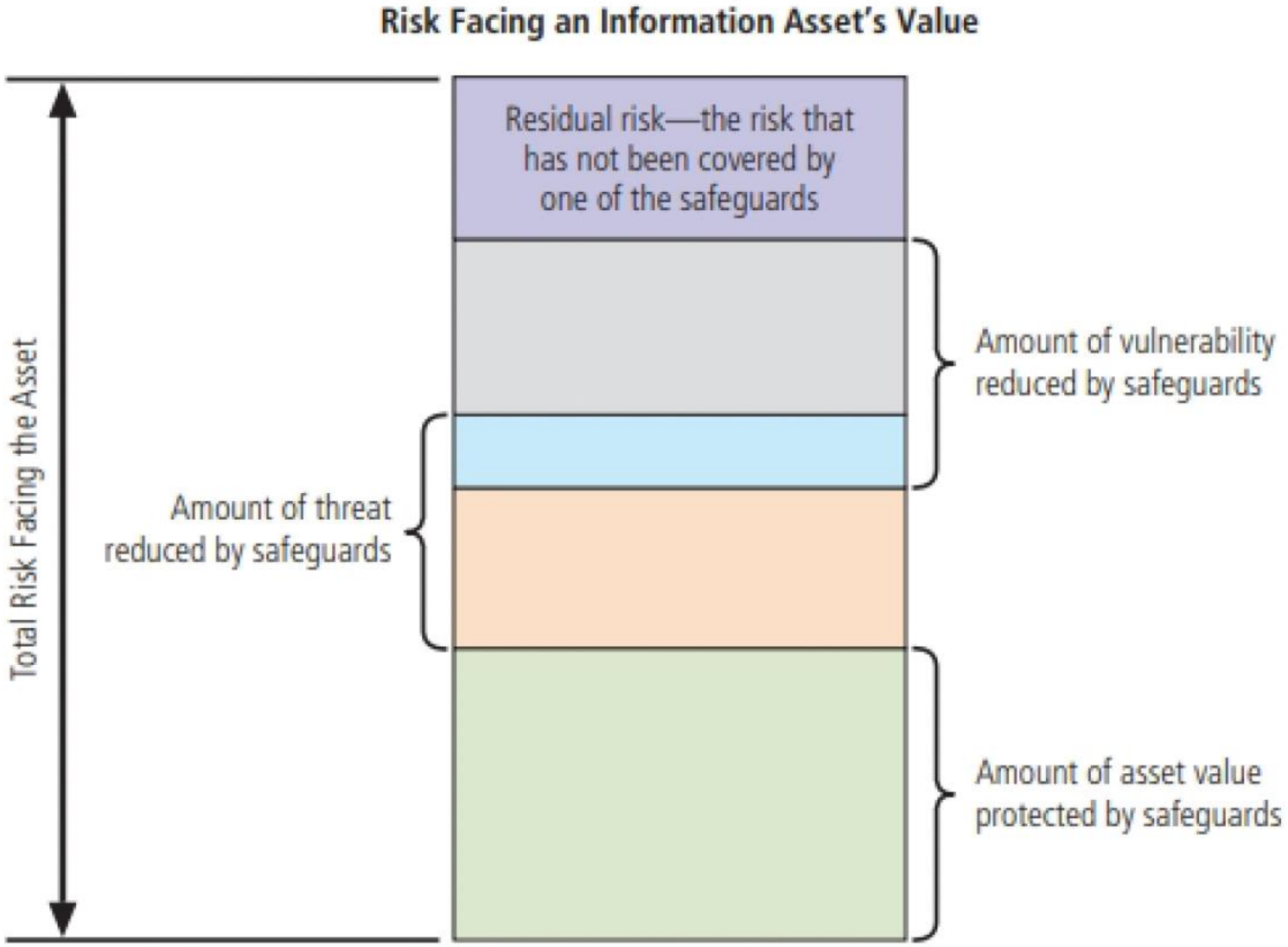
- The termination risk control strategy is based on the organization's need or choice not to protect an asset. Here, organization does not wish the information asset to remain at risk and so removes it from the environment that represent risks.
- Sometimes, the cost of protecting an asset outweighs its value, or it may be too difficult/expensive to protect an asset. Then termination is a conscious business decision.

Managing Risk

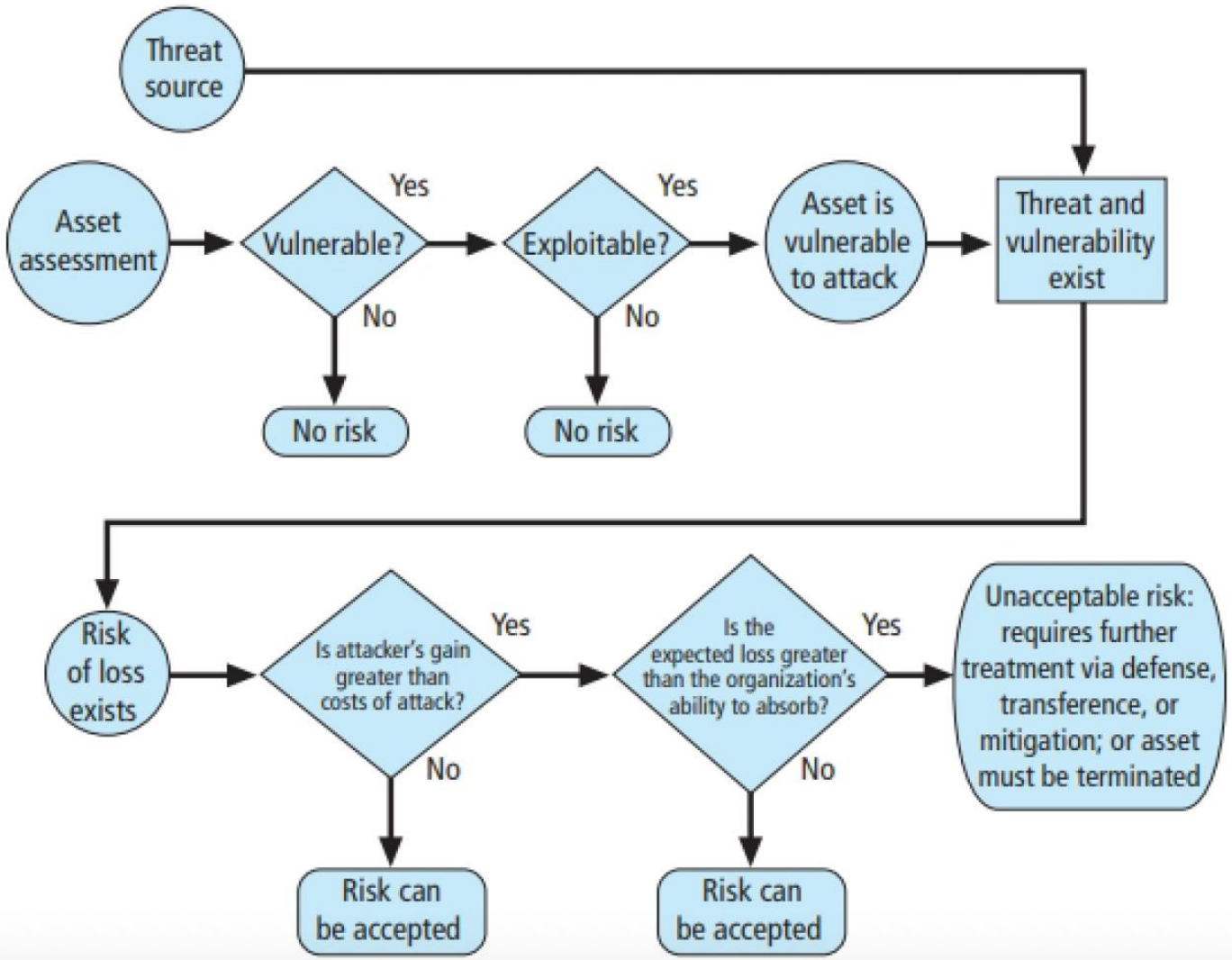
- Risk appetite (also known as risk tolerance)
  - ➢ The quantity and nature of risk that organizations are willing to accept
    - ✓As they evaluate the trade-offs between perfect security and unlimited accessibility
- The reasoned approach to risk is one that balances the expense (in terms of finance and the usability of information assets) against the possible losses if exploited

Residual Risk

- **Residual risk:** When vulnerabilities have been controlled as much as possible, there is often remaining risk that has not been completely removed, shifted, or planned for
- Residual risk is a combined function of: threats, vulnerabilities and assets, less the effects of the safeguards in place



Risk-Handling Action Points



- The goal of information security is not to bring residual risk to zero
  - ➢ Bring it in line with an organization's risk appetite

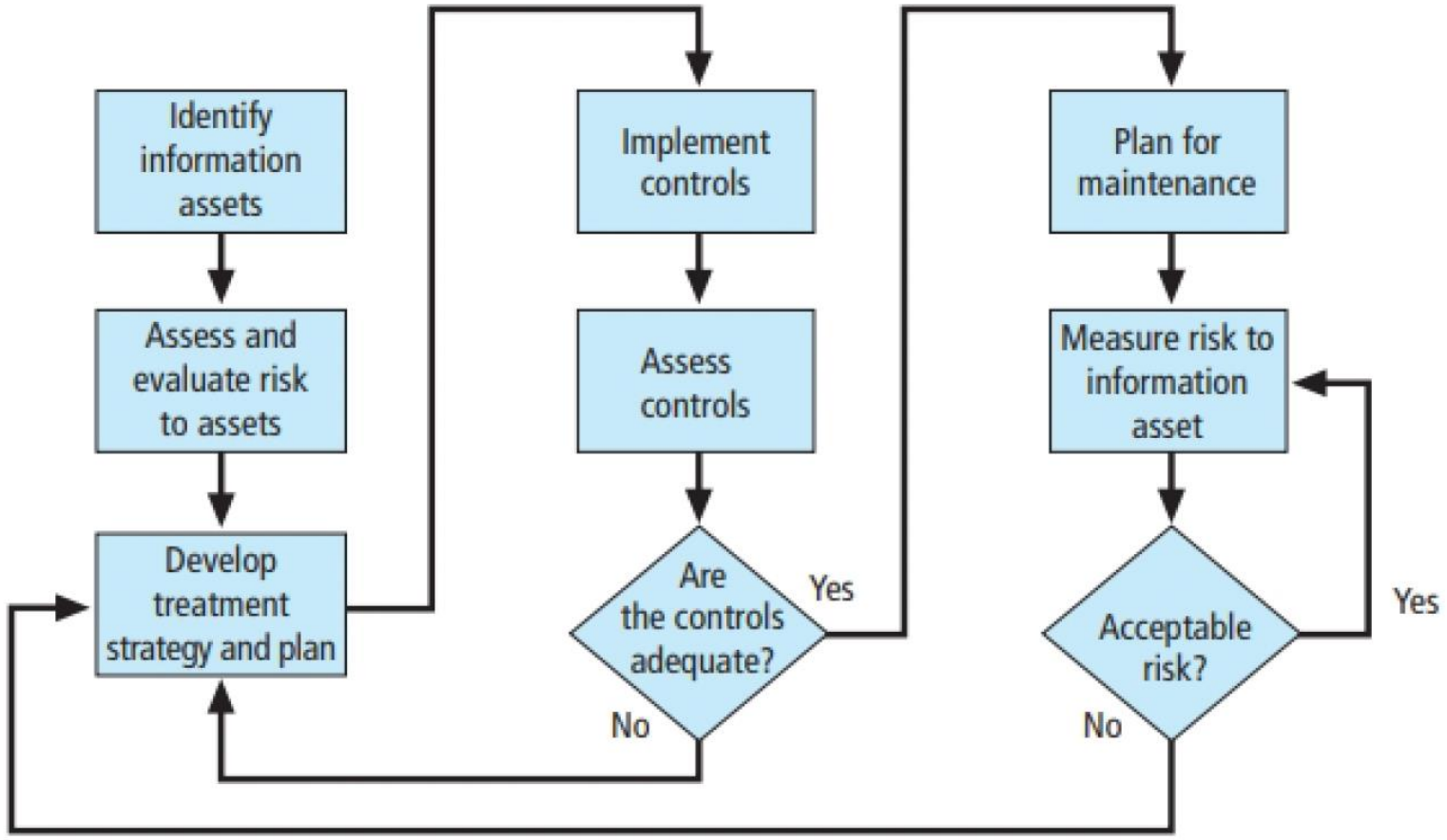
If decision makers have been informed of uncontrolled risks and the proper authority groups within the communities of interest decide to leave residual risk in place, then the information security program has accomplished its primary goal

Strategy Selection for Risk Control

- Guidelines for risk control strategy selection
  - **When a vulnerability exists:** Implement security controls to reduce the likelihood of a vulnerability being exercised
  - **When a vulnerability can be exploited:** Apply layered controls to minimize the risk or prevent occurrence
  - **When the attacker's potential gain is greater than the costs of attack:** Apply technical or managerial controls to increase the attacker's cost, or reduce his gain
  - **When potential loss is substantial:** Apply design controls to limit the extent of the attack, thereby reducing the potential for loss

Risk Control Cycle

- Once a control strategy has been selected and implemented:
  - Controls should be monitored and measured on an ongoing basis to determine its effectiveness and the accuracy of the estimate of the residual risk

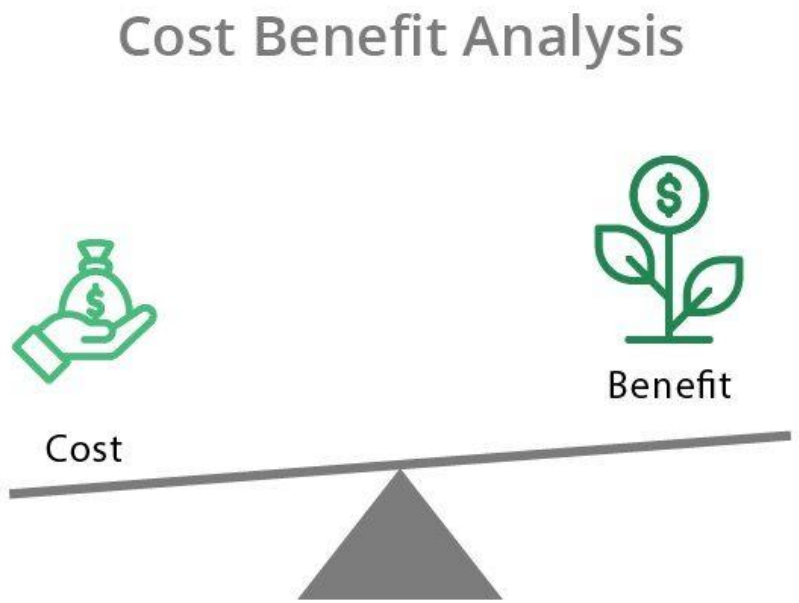


Feasibility and Cost-Benefit Analysis

- Before deciding on the strategy for a specific vulnerability
  - ➢ All readily accessible information about the consequences of the vulnerability must be explored
    - ✓Ask “what are the advantages of implementing a control as opposed to the disadvantages of implementing the control?”
- There are a number of ways to determine the advantage or disadvantage of a specific control
- The primary means are based on the value of the information assets that it is designed to protect
- Cost avoidance is the money saved by using the defense strategy via the implementation of a control, thus eliminating the financial ramifications of an incident.

Cost-Benefit Analysis (CBA)

- **Economic feasibility:** The criterion most commonly used when evaluating a project that implements information security controls and safeguards
- Begin a cost-benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised
- This decision-making process is called **cost-benefit analysis** or economic feasibility study



Cost-Benefit Analysis (cont'd.)

- **Cost:** It is difficult to determine the value of information
  - ➢ It is also difficult to determine the cost of safeguarding it
- Factors that affect the cost of a safeguard
  - ➢ Cost of development or acquisition of hardware, software, and services
  - ➢ Training fees
  - ➢ Cost of implementation
  - ➢ Service costs
  - ➢ Cost of maintenance

Cost-Benefit Analysis (cont'd.)

- **Benefit**
  - The value to the organization of using controls to prevent losses associated with a specific vulnerability
  - Usually determined by valuing the information assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset
  - This is expressed as the annualized loss expectancy (ALE)

Cost-Benefit Analysis (cont'd.)

- **Asset valuation**
  - ➢ The process of assigning financial value or worth to each information asset
  - ➢ The value of information differs within and between organizations
    - ✓ Based on the characteristics of information and the perceived value of that information
  - ➢ Involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against loss and litigation

Cost-Benefit Analysis (cont'd.)

- **Asset valuation components**
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information

Cost-Benefit Analysis (cont'd.)

- **Asset valuation components (cont'd.)**
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Cost-Benefit Analysis (cont'd.)

- Potential loss is that which could occur from the exploitation of vulnerability or a threat occurrence

- Ask these questions:
  - What loss could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the financial impact of damage?
  - What is the single loss expectancy for each risk?

Cost-Benefit Analysis (cont'd.)

- A **single loss expectancy (SLE)**: The calculation of the value associated with the most likely loss from an attack. SLE is based on the value of the asset and the expected percentage of loss that would occur from a particular attack
- **SLE = asset value (AV) x exposure factor (EF)**
  - Where EF is the percentage loss that would occur from a given vulnerability being exploited
  - A Web site had an estimated value of $1,000,000 and a sabotage or vandalism scenario indicated that 10 percent of the Web site would be damaged or destroyed in such an attack (the EF). In this case, the SLE for the Web site would be $1,000,000 x 0.10 = $100,000.
  - This information is usually estimated

Cost-Benefit Analysis (cont'd.)

- In most cases, the probability of a threat occurring is the probability of loss from an attack within a given time frame
- This value is commonly referred to as the annualized rate of occurrence (ARO)

ALE = SLE * ARO

- If SLE = $100,000 and ARO = 0.5, then ALE = $50,000.

Cost-Benefit Analysis (cont'd.)

- CBA determines whether or not a control alternative is worth its associated cost

- CBAs may be calculated before a control or safeguard is implemented
  - To determine if the control is worth implementing

- Or calculated after controls have been implemented and have been functioning for a time

Cost-Benefit Analysis (cont'd.)

- Cost-benefit analysis formula

CBA = ALE (prior) – ALE (post) – ACS

  - ALE (prior to control) is the annualized loss expectancy of the risk before the implementation of the control
  - ALE (post-control) is the ALE examined after the control has been in place for a period of time
  - ACS is the annual cost of the safeguard

- Once the controls are implemented, it is crucial to examine their benefits continuously to determine when they must be upgraded, supplemented, or replaced.

Cost-Benefit Analysis (cont'd.)

- Asset: data worth $50K. Threat: viruses, estimated damage: 30%.
- Frequency of occurrence: 1 per 6 months.
- Control: Antiviruses. Cost: $10K. Frequency of occurrence after implementing antiviruses: 1 per year.
- Is the control worth the cost? How much does it save?

SLE = AV * EF = $50K * 30% = $15K

ALE(prior) = SLE * ARO = $15K * 2 = $30K

ALE(post) = $15K * 1 = $15K

CBA = ALE(prior) – ALE(post) – ACS = $30K - $15K - $10K = $5K

Other Methods of Establishing Feasibility

- **Organizational feasibility analysis**
  - Examines how well the proposed information security alternatives will contribute to the operation of an organization

- **Operational feasibility**
  - Addresses user and management acceptance and support
  - Addresses the overall requirements of the organization's stakeholders

Other Methods of Establishing Feasibility (cont'd.)

- **Technical feasibility**
  - Examines whether or not the organization has or can acquire the technology to implement and support the alternatives

- **Political feasibility**
  - Defines what can and cannot occur based on the consensus and relationships between the communities of interest

Alternatives to Feasibility Analysis

- Benchmarking
- Due care and due diligence
- Best business practices
- Gold standard
- Government recommendations
- Baselining

Alternative Risk Management Methodologies

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method:** an InfoSec risk evaluation methodology promoted by the Computer Emergency Response Team (CERT) Coordination Center *(www.cert.org).*
  - ➢ Allows organizations to balance the protection of critical information assets against the costs of providing protective and detection controls.
  - ➢ Can enable an organization to measure itself against known or accepted good security practices and then establish an organization-wide protection strategy and InfoSec risk mitigation plan.
- **Microsoft Risk Management approach:** Microsoft asserts that risk management is not a stand-alone subject and should be part of a general governance program to allow the organizational general-management community of interest to evaluate the organization's operations and make better, more informed decisions. The purpose of the risk management process is to prioritize and manage security risks.

Alternative Risk Management Methodologies (cont'd)

- **ISO Standards for InfoSec Risk Management:**

  - ISO 27005:2022 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks): Provides guidance to fulfil the requirements of ISO 27001 concerning actions to address InfoSec risks, and to perform InfoSec risk management activities

  - ISO 31000 (Risk Management): developed using AS/NZS 4360:2004 as a foundation, it provides principles, a framework and a process for managing risk. It addresses any type of risk management (enterprise, financial, environmental)

Alternative Risk Management Methodologies (cont'd)

- **NIST Risk Management Framework (RMF):** NIST has modified its fundamental approach to systems management and certification/accreditation to one that follows the industry standard of effective risk management.
  - NIST SP 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View"
    - ✓ intends to offer a complete and organization-wide approach that integrates risk management into all operations and decisions
  - NIST SP 800-37, Rev. 1: "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
    - ✓ uses the framework level described in SP 800-39 and proposes processes for implementation called the Risk Management Framework (RMF).
    - ✓ emphasizes the building of InfoSec capabilities into information systems using managerial, operational, and technical security controls.

Alternative Risk Management Methodologies (cont'd)

- FAIR (Factor Analysis of Information Risk): a risk management framework developed by Jack A. Jones, can help organizations understand, analyze and measure information risk

- Mitre: a risk management plan presented by Mitre – a non-profit organization

- ENISA (European Network and Information Security Agency): an agency of the EU, provides a utility that enables users to compare risk management methods and tools

- New Zealand's IsecT Ltd.: an independent governance, risk management, and compliance consultancy