Risk Control

Part 6

Risk Control

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas
- Three general categories of controls exist:
  - **Policies**
  - **Programs**
  - **Technical controls**

Introduction

- 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 via the application of the principles of risk management

Risk Control Strategies

- **Four basic strategies to control risks**
  - **Avoidance**
    - **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

Avoidance

- The risk control strategy that **attempts to prevent the exploitation of the vulnerability**
- Avoidance is accomplished through:
  - Application of policy
  - Application of training and education
  - Countering threats
  - Implementation of technical security controls and safeguards

Transference

- The control approach **that attempts to shift the risk to other assets, other processes, or other organi**zations
- May be accomplished by rethinking how services are offered
  - Revising deployment models
  - Outsourcing to other organizations
  - Purchasing insurance
  - Implementing service contracts with providers

Mitigation

- The control approach that **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)

Mitigation (cont'd.)

Plan	Description	Example	When deployed	Timeframe
Incident Response (IR) Plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As 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 disaster • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost 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 DRP's ability to quickly restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organization

Summaries of mitigation plans

Acceptance

- **do nothing to protect an information asset**
  - **To accept the loss when it occurs**
- 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

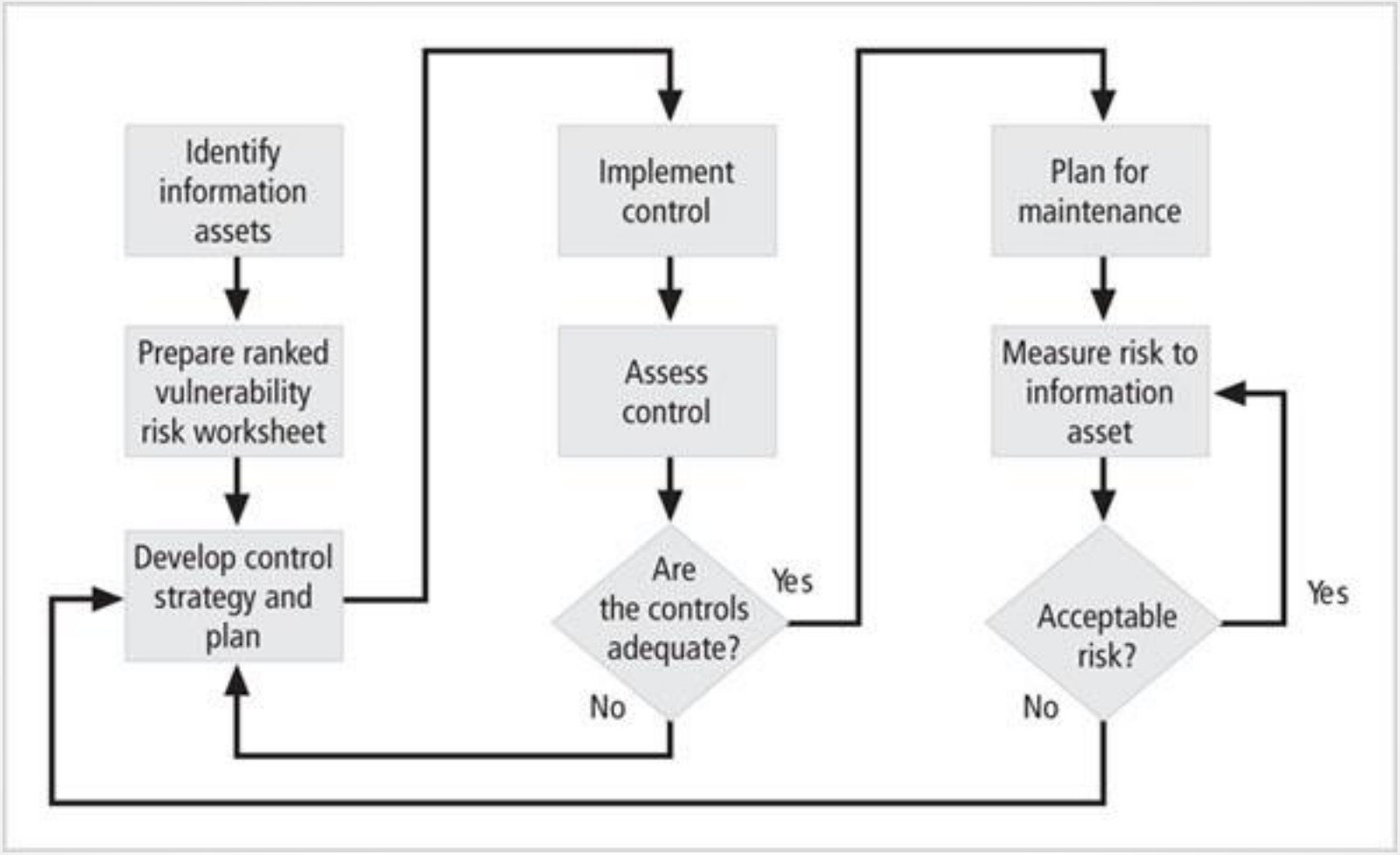
Acceptance (contd.)

- the organization must:
  - Determine the level of risk to the information asset
  - Assess the probability of attack and the likelihood of a successful exploitation of a vulnerability
  - Approximate the ARO of the exploit
  - 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

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



Risk control cycle

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-Benefit Analysis

- Economic feasibility
  - The criterion most commonly used when evaluating a project that implements information security controls and safeguards
- It is difficult to determine the value of information
  - It is also difficult to determine the cost of safeguarding it

Cost-Benefit Analysis (cont'd.)

- Factors that affect the cost of a safeguard
  - Cost of development or acquisition of hardware, software, and services
  - Training fees
  - Cost of implementation
  - Service and maintenance costs

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
  - 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

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