MANAGEMENT of INFORMATION SECURITY
Third Edition

RISK MANAGEMENT: CONTROLLING RISK

Slides by: M. Whitman and H. Mattord

Objectives

- Upon completion of this chapter, you should be able to:
  - Recognize and select from the **risk mitigation strategy** options to **control risk**
  - **Evaluate** risk **controls** and formulate a **cost-benefit analysis**
  - Describe some recommended **Risk Control Practices**

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

Introduction

- This chapter builds on the concepts developed in the previous Chapter, which focused on the **identification** of **risk** and the **assessment** of its relative impact from all identified vulnerabilities.
  - This effort produces a list of documented **vulnerabilities**, ranked by **risk rating factor**.
- In this chapter, you will learn how to use such a list to **assess options**, **estimate costs**, **weigh** the **relative merits** of options, and gauge the benefits of various control approaches.

Risk Control Strategies

- An organization must choose one of four basic **strategies** to **control risks**
  - **1- Avoidance**
    - Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
  - **2- Transference**
    - Shifting the risk to other areas or to outside entities
  - **3- Mitigation**
    - Reducing the impact caused by the exploitation of vulnerability
  - **4- Acceptance**
    - Understanding the consequences and accepting the risk without control or mitigation

1- Avoidance

- The risk control strategy that attempts to **prevent** the exploitation of the vulnerability
- It is the preferred approach, as it seeks to avoid risk rather than deal with it after it has been realized
- **Avoidance is accomplished through:**
  - 1- Application of **policy**
  - 2- Application of **training** and **education**
  - 3- Implementation of technical **security controls** and safeguards

1- Avoidance (cont'd.)

- **Avoidance is accomplished through: (cont'd.)**
  - ***1- Application of policy***
    - The application of policy allows all levels of management to mandate that certain procedures always be followed.
  - ***2- Application of training and education***
    - It is essential to creating a safer and more controlled organizational environment and to achieving the necessary changes in end-user behavior.
  - ***3- Implementation of technical security controls and safeguards***
    - Risks can be avoided by countering the threats facing an asset and by eliminating its exposure to threats.
    - In the everyday world of information security, technical solutions are often required to reduce risk effectively
    - Example: secure FTP and Https, antivirus , Firewall, IDS

2- Transference

- The control approach that attempts to **shift** the risk to other assets, other processes, or other organizations
- **May be accomplished** by rethinking how services are offered
  - Outsourcing to other organizations
  - Purchasing insurance
  - Implementing service contracts with providers
- One of the eight characteristics of excellent organizations is that they "*stick to their knitting. They stay reasonably close to the business they know*." [1]

[1] Peters and Waterman, Search of Excellence

2- Transference (cont’ d.)

- If an organization does not have adequate security management and administration experience,
  - it should transfer it to individuals or firms with more experience in dealing with risks in those areas (outsourcing).
- A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery
  - And for guaranteeing server and Web site availability through service-level agreements.

3- Mitigation

- The control approach that attempts to **reduce** the damage caused by the exploitation of vulnerability
  - Using planning and preparation
- **Types of mitigation plans**
  1. Disaster recovery plan (DRP)
  2. Incident response plan (IRP)
  3. Business continuity plan (BCP)
- Mitigation **depends** on the **ability** to **detect** and respond to an attack as quickly as possible.

3- Mitigation (cont'd.)

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 DRP'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

Table 9-1 Summaries of mitigation plans

4- Acceptance

- The choice **to do nothing** to protect an information asset
  - To accept the loss when it occurs
- This control, or lack of control, assumes that it may be a sensible business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure
- It is different from Rejecting risk

4- Acceptance (cont’ d.)

- **Example**:
  - Suppose it would cost an organization $100,000 a year to protect a server. *(option1)*
  - The security assessment determines that the organization could replace the information contained in the server, replace the server itself, and cover associated recovery costs for $10,000 only *(option2)*
  - ***Which option is more sensible do you think?***

4- Acceptance (cont'd.)

- **Before** using the acceptance strategy, 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 annual rate of occurrence (ARO) of such an attack
  - Estimate the potential loss from attacks
  - Perform a thorough cost benefit analysis
  - Evaluate controls using each appropriate type of feasibility analysis report
  - Decide that the particular asset did not justify the cost of protection

Managing Risk

- **Risk appetite** (also known as **risk tolerance**)
  - The **quantity** and **nature** of **risk** that organizations are willing to **accept**
- The most logical **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!
  - The key is for the organization to find balance in its decision-making processes and in its feasibility analyses,
  - thereby assuring that its risk appetite is based on *experience* and *facts*, and not on ignorance or wishful thinking.

Managing Risk (cont'd.)

- **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 after** the organization has implemented **policy**, education and **training**, and technical **controls** and **safeguards**
- Residual Risk is a combined function of:

(1)" a **threat** less the effect of threat-reducing safeguards;

(2) a **vulnerability** less the effect of vulnerability-reducing safeguards;

(3) an **asset** less the effect of asset value-reducing safeguards."

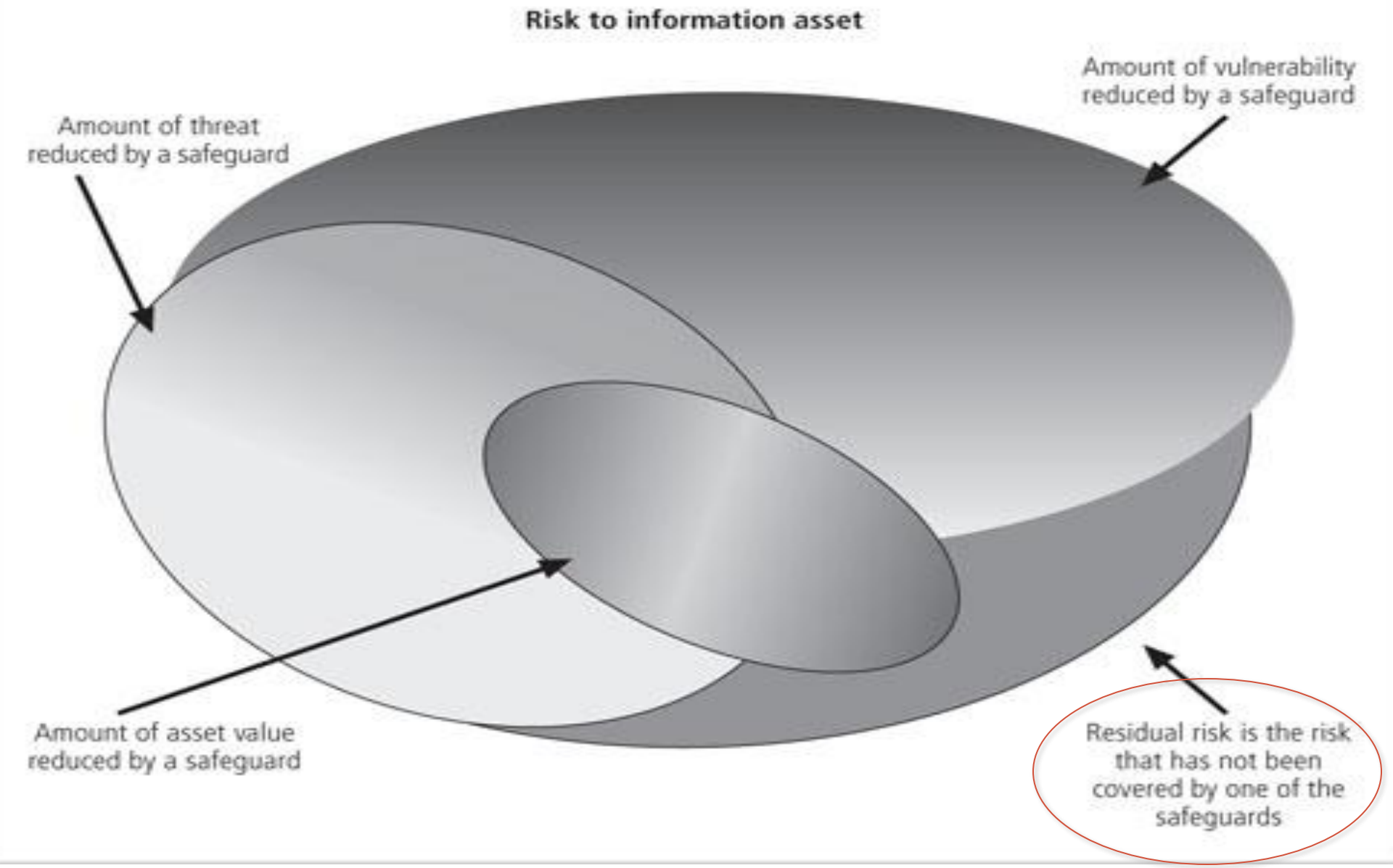


Figure 9-1 Residual risk

Managing Risk (cont'd.)

- The goal of information security program
  - ***Not to bring residual risk to zero***,
  - but to **bring** residual risk **in line with** an organization's **risk appetite.**
  - By **informing decision-makers** of uncontrolled risks
    - If they decide to **leave residual risk** in **place,**
    - then the information security program has accomplished its primary goal

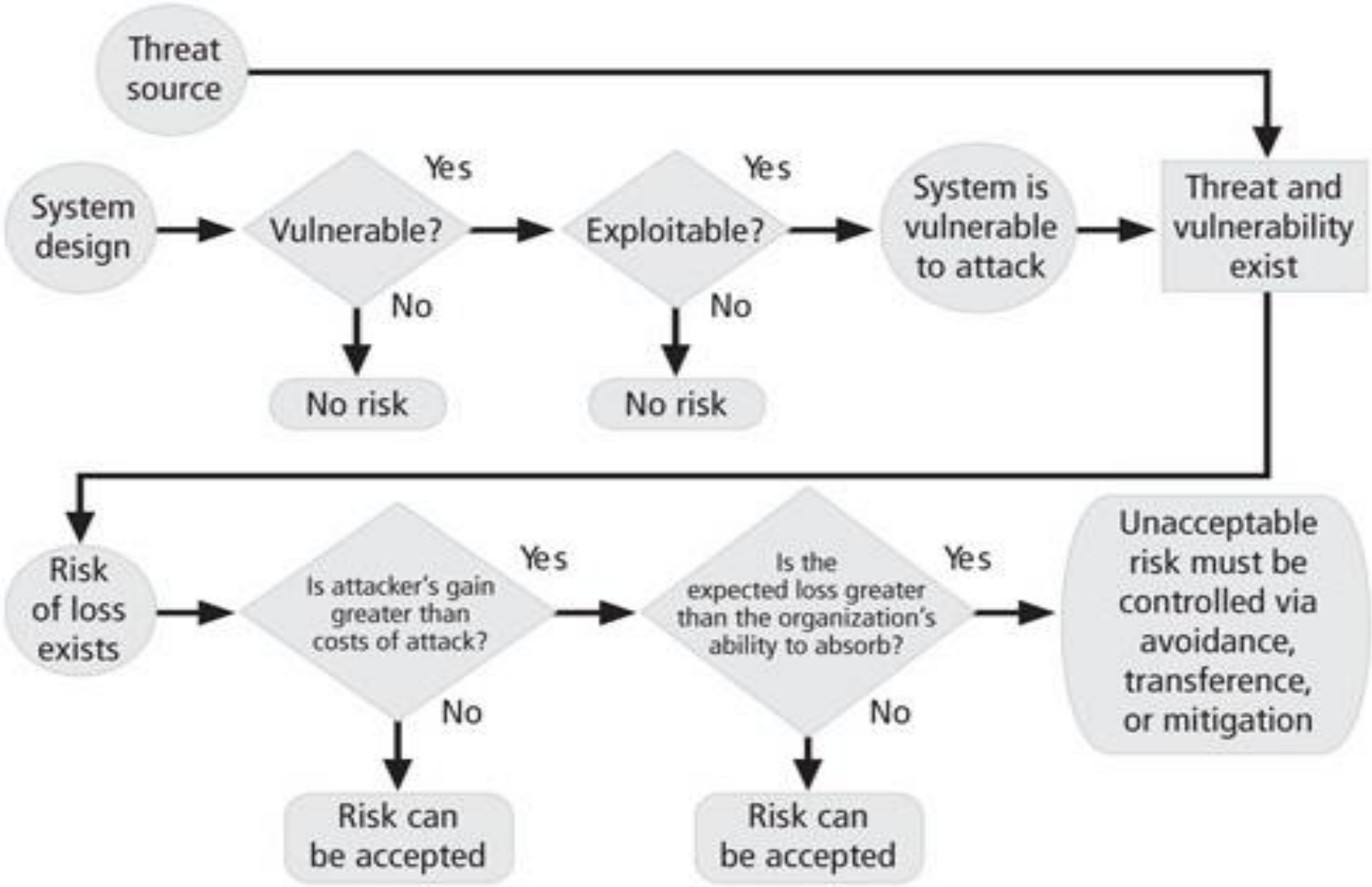


Figure 9-2 "**Risk-handling action points"** illustrates the process by which an organization chooses from among the four risk control strategies

Managing Risk (cont’ d.)

- A **control strategy** should be selected for each asset-threat-vulnerability combination that identifies any residual risk
- After the control strategy is **selected** and **implemented**, the **effectiveness** of controls should be **monitored** and measured regularly
  - To **determine** its effectiveness and the accuracy of the estimate of the residual risk
- Some organizations **document** the **outcome** of the **control strategy** for each information asset-threat pair in **an action plan**

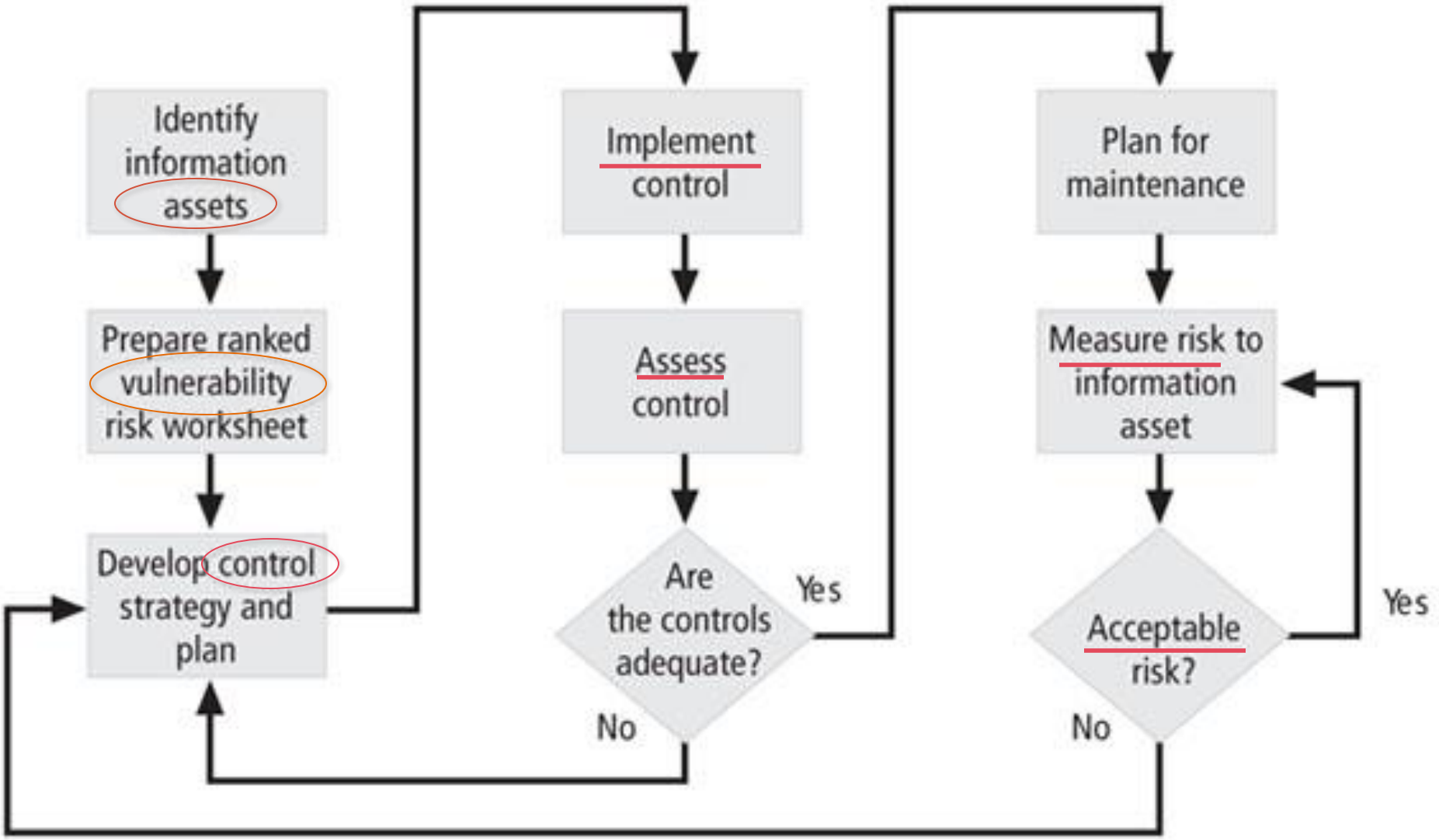


Figure 9-3 **Risk control cycle**

Feasibility and Cost-Benefit Analysis

- **Before deciding** on the **strategy** for a specific vulnerability

1. An **organization** must **explore** all readily accessible information about the **economic** and **non-economic consequences** of the **vulnerability**.
2. Attempt to answer *"what are the **advantages** of implementing a control as opposed to the **disadvantages** of implementing the control?"*

Feasibility and Cost-Benefit Analysis (cont'd.)

- There are economic and noneconomic **ways** to **determine** the **advantage** or **disadvantage** of a specific control.
- Primary means are **based** on the **value** of the information **assets** that it is designed to protect, and the **savings** from economic cost **avoidance**
- **Cost avoidance** is the **money saved** by using the defense strategy (control implementation) thus eliminating the financial cost as a consequence of an incident.
- This decision-making process is called
  - **Cost-benefit analysis (CBA)** OR **economic feasibility study**

Cost-Benefit Analysis

- **Economic feasibility**
  - The criterion most commonly used when evaluating a project that implements information security controls and safeguards
- Economic feasibility **analysis** begins with
  - **Valuing** the **information** asset to be protected and the **loss** in **value** if those information assets are **compromised** by the exploitation of a specific vulnerability.
  - An organization must not spend more to protect an asset than its worth.

Cost-Benefit Analysis (cont'd.)

- **Cost**
  - It is difficult to determine the **value** of **information,** and **cost** of **safeguarding** it
- **Factors that affect the cost of a safeguard**
  - Cost of **development** or acquisition of (**hardware**, software, and services)
  - **training** fees
  - **implementation** cost (installing, configuring, and testing hardware, software, and services)
  - **Service** costs (vendor fees for maintenance and upgrades)
  - and **maintenance** costs (labor expense to verify and continually test, maintain, train, and update)

Cost-Benefit Analysis (cont'd.)

- **Benefit**
  - The **value** to the organization **of using controls** to prevent losses associated with a specific vulnerability
  - 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 cost of design, development, installation, maintenance, protection, recovery, and defense against loss and litigation

Cost-Benefit Analysis (cont’ d.)

- **Asset valuation (cont’d.)**
  - A further complication is that some information assets gain value over time that is beyond their **intrinsic value**—the essential worth—of the asset under consideration.
  - This higher **acquired value** is the most appropriate value in most cases.

Cost-Benefit Analysis (cont’ d.)

- **Asset valuation must consider the following:**

1. Value retained from **the cost of creating** the information asset
2. Value retained from **past maintenance** of the information asset
3. Value implied by the **cost of replacing** the information
4. Value from **providing the information** (delivery, network, H/W, S/W)
5. Value acquired from the **cost of protecting the information**
6. Value to **owners**
7. Value of **intellectual property**
8. Value to **adversaries** (worth to know what the competition is doing?)
9. **Loss of productivity** while the information assets are unavailable
10. **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:**
  1. What **loss** could occur, and what **financial impact** would it have?
  2. What would it cost to **recover** from the attack, in addition to the financial impact of damage?
  3. What is the **Single Loss Expectancy (SLE)** 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**

SLE Example

AV

- **A Web site**
  - Has an estimated value of $1,000,000 (as determined by asset valuation)
  - Sabotage or vandalism (hacker defacement) scenario indicates that 10 percent of the Web site would be damaged or destroyed in such an attack (the exposure factor)

EF

- The SLE for this Web site would be

  $1,000,000 X 0.10 = $100,000.

- This estimate is then used to calculate another value

  Annual Loss Expectancy (ALE).

Cost-Benefit Analysis (cont'd.)

- Usually, the probability of a threat occurring is depicted as a table that indicates **how *frequently* an attack** from each threat type is likely to occur within a given time frame
  - This value is commonly referred to as the **annualized rate of occurrence (ARO)**
  - It simply indicates **how often you expect** a specific type of attack to occur.
  - This information is usually **estimated**

Cost-Benefit Analysis (cont'

???------ 1 year
1--------2 years

???------ 12 moths
1----------1 month

???------ 12 moths
1---------3 month

- **Examples:**

1. If a successful act of sabotage or vandalism occurs about once every two years
   - ARO would be 50 percent (0.5).
2. A network attack that can occur multiple times per second might be successful once each month
   - ARO Would be 12.

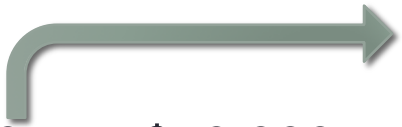
Cost-Benefit Analysis (cont' d.)

- Once you determine the **loss** from a **single attack** and the likely **frequency** of **successful attacks**

- To calculate the overall loss potential per risk expressed as an **annualized loss expectancy (ALE)** using the values for the *ARO* and *SLE*

ALE = SLE * ARO

- To use previous example, if SLE= $100,000 and ARO= 0.5, then



ALE = $100,00 X 0.5 = $50,000

Cost-Benefit Analysis (cont'd.)

- How much can the organization expects to lose per year?
- How much can the organization expect to lose per year if a successful act of sabotage or vandalism occurs about once every year?

Cost-Benefit Analysis *Formula*

- CBA (**or economic feasibility**) determines whether or not a control alternative is worth its associated cost
- CBAs may be **calculated before** a control or safeguard is implemented (if the control is worth implementing)
- Or **calculated after** controls have been implemented and have been functioning for a time (whether the safeguard is functioning as intended)

Cost-Benefit Analysis *Formula* (cont'd.)

- **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**

CBA > ALE (Prior) = not worth
CBA < ALE (Prior) = worth
CBA (minus)= not worth

Cost-Benefit Analysis *Formula* (cont'd.)

- Once the controls are implemented, **examine** their **benefits** continuously to determine when they must be upgraded, supplemented, or replaced.
- **Security** is an **investment, not an expense** as risks make it possible to satisfy changing business requirements without hurting the business's viability (survival).

Recommended Risk Control Practices

- Organizations typically look for a more **straightforward** method of implementing controls
- The following sections cover some of these alternatives.
  1. **Qualitative and Hybrid Measures**
  2. **Delphi Technique**
  3. **ISO 27005 *Standard for Information Security Risk Management***

Qualitative and Hybrid Measures

- **Quantitative assessment**
  - Perform asset valuation with actual values or estimates
  - May be difficult to assign specific values
- **Qualitative assessment**
  - Use overall quality instead of specific estimates
- **Hybrid (mixture) assessment**
  - Try to improve upon the ambiguity of qualitative measures without using an estimating process (using scales)

Delphi Technique

- Example of Qualitative risk analysis [1]

1. It is a process whereby a group **rates or ranks (1-10 or low-mid and high) a set of information and then post it *anonymously*** [1]
2. The **individual responses are compiled** and
3. Then **responses are returned** to the group for another ***iteration***.

Delphi Technique (cont'd.)

- This process continues until the entire group is satisfied with the result.
- This technique can be applied to the development of scales, asset valuation, asset or threat ranking, or any scenario that can benefit from the input of more than one decision maker.

ISO 27005 *Standard for Information Security Risk Management*

- The ISO 27000 series includes a standard for the performance of Risk Management
  - ISO 27005
- The 27005 document includes a **five-stage** risk management methodology
  - Information security risk assessment (ISRA)
  - Information security risk treatment
  - Information security risk acceptance
  - Information security risk communication
  - Information security risk monitoring and review

Summary

- Introduction
- Risk control strategies
- Risk control strategy selection
- Risk management discussion points
- Feasibility studies and cost-benefit analysis
- Recommended risk control practices
  - Delphi Technique
  - Qualitative and Hybrid Measures
  - ISO 27005

Reference

- [1] CISSP Exam guide, 5th edition, Shon Harris, Mcgraw Hill
- ***Internet Security Threat Report:***

http://www.symantec.com/threatreport/

- ***Data breach investigation report 2012:***

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

- ***McAfee Threats Report***:

http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2012.pdf