# UNIT III SECURITY ANALYSIS

## Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk

## RISK MANAGEMENT

### Definition:

The formal process of identifying and controlling the risks facing an organization is called risk management. It is the probability of an undesired event causing damage to an asset. There are three steps

1. Risk Identification.
2. Risk Assessment
3. Risk Control

**Risk Identification**: It is the process of examining and documenting the security posture of an organization's information technology and the risk it faces.

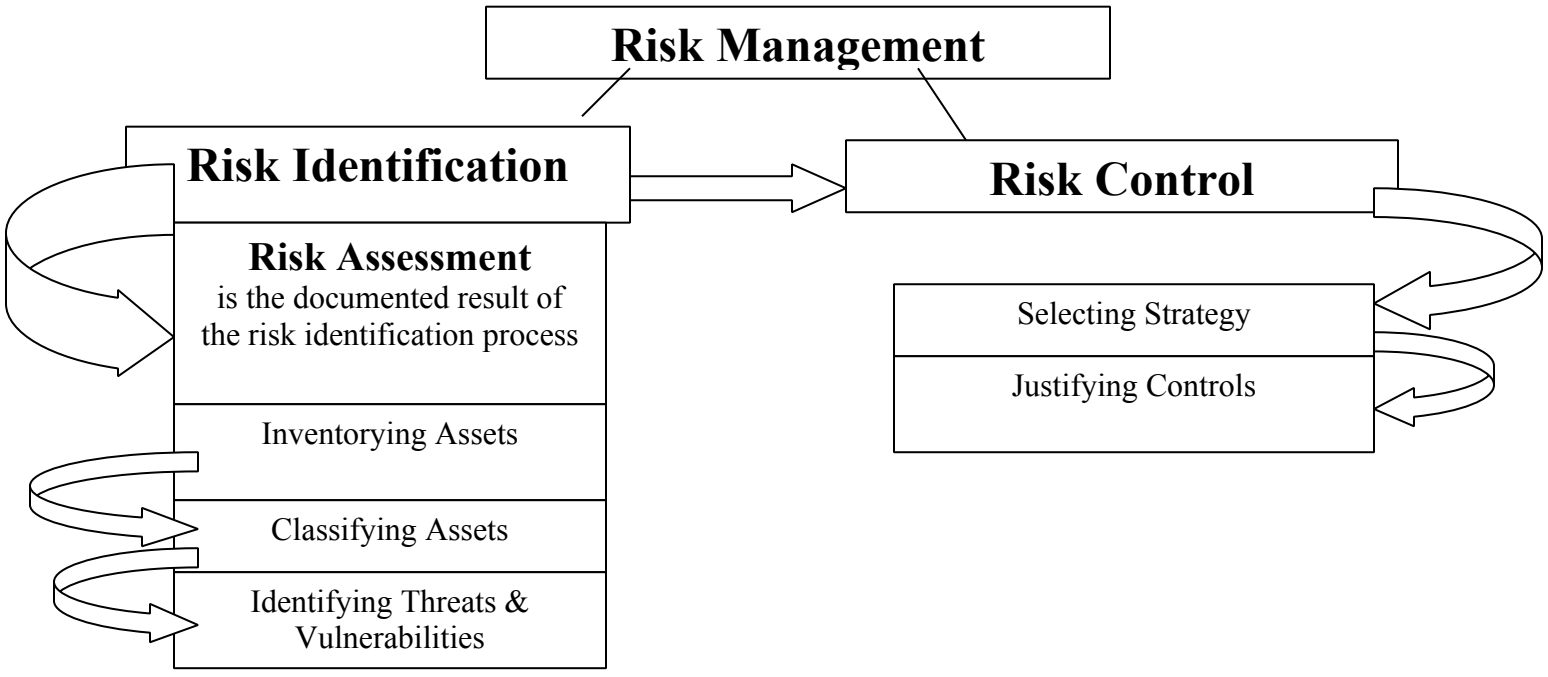
**Risk Assessment**: It is the documentation of the results of risk identification.

**Risk Control**: It is the process of applying controls to reduce the risks to an organization's data and information systems.

To keep up with the competition, organizations must design and create safe environments in which business process and procedures can function.

These environments must maintain Confidentiality & Privacy and assure the integrity of organizational data-objectives that are met through the application of the principles of risk management

### Components of Risk Management



# An Overview of Risk Management

Over 2,400 years ago by Chinese General Sun Tzu said

"1.If you know the enemy & know yourself, you need not fear the result of a hundred battles.

2. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

3. If you know neither the enemy nor yourself, you will succumb in every battle"

## Know Yourself

- Identify, Examine & Understand the information systems.
- To protect assets, you must understand what they are? How they add value to the organization, and to which vulnerabilities they are susceptible.
- The policies, Education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they are still effective.

## Know the Enemy

- Identifying, Examining & Understanding the threats facing the organization.

### The Roles of the Communities of Interest

- It is the responsibility of each community of interest to manage the risks that organization encounters.

### Information Security

- Understand the threats and attacks that introduce risk into the organization.
- Take a leadership role in addressing risk.

### Management & Users

- Management must ensure that sufficient resource are allocated to the information security & Information technology groups to meet the security needs of the organization.
- Users work with the systems and the data and are therefore well positioned to understand the value of the information assets.

## Information Technology

- Must build secure systems and operate them safely.

Three communities of interest are also responsible for the following

- Evaluating the risk controls.
- Determining which control options are cost effective.
- Acquiring or installing the needed controls.
- Overseeing that the controls remain effective.

**Important Risk Factors of information Security are**

i. Understand the threats and attacks that introduce risk into the organization.
ii. Taking asset inventory.

iii. Verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory, as well as the current controls and mitigation strategies.

iv. Review the cost effectiveness of various risk control measures.

**Risk Identification**

- IT professionals to know their organization's information assets through identifying, classifying and prioritizing them.
- Assets are the targets of various threats and threat agents, and the goal is to protect the assets from the threats.
- Once the organizational assets have been identified, a threat identification process is undertaken.
- The circumstances and settings of each information asset are examined to identify vulnerabilities.
- When vulnerabilities are found, controls are identified and assessed as to their capability to limit possible losses in the eventuality of attack.
- The process of Risk Identification begins with the identification of the organization's information assets and an assessment of their value.
- The Components of this process are shown in figure

## Asset Identification & Valuation

- Includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements.
- Then, you classify and categorize the assets, adding details.

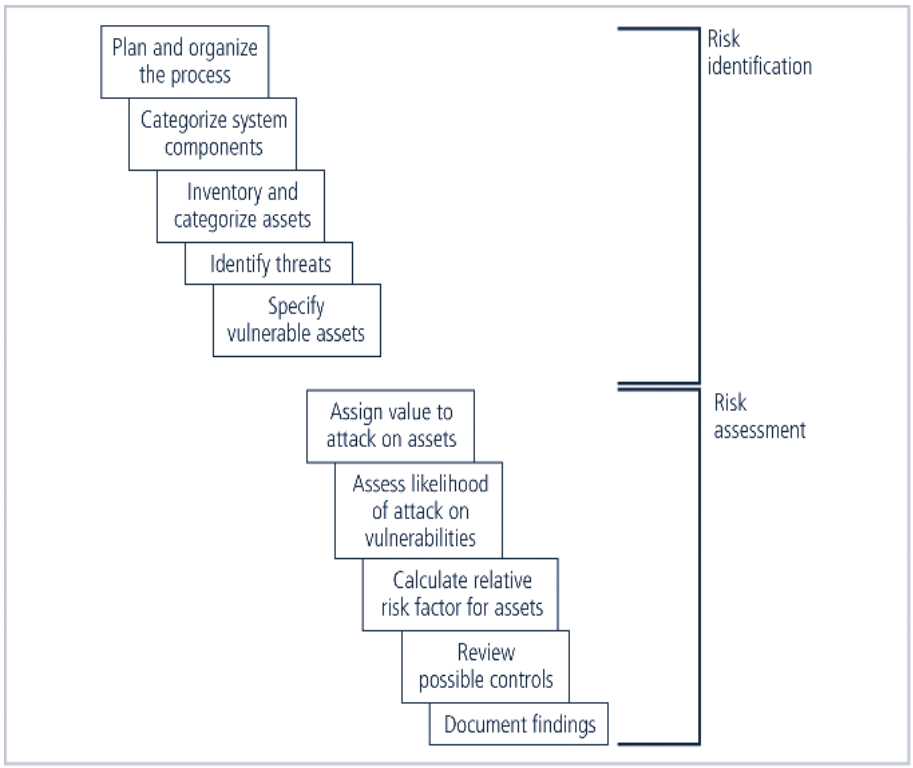



**FIGURE 4-2** Components of Risk Identification

# Components of Risk Identification

## Categorization of IT Components

**TABLE 4-1** Categorizing the Components of an Information System

| Traditional system components | SecSDLC and risk management system components | |
|---|---|---|
| People | Employees | Trusted employees<br>Other staff |
| | Nonemployees | People at trusted organizations<br>Strangers |
| Procedures | Procedures | IT and business standard procedures<br>IT and business sensitive procedures |
| Data | Information | Transmission<br>Processing<br>Storage |
| Software | Software | Applications<br>Operating systems<br>Security components |
| Hardware | System devices and peripherals | Systems and peripherals<br>Security devices |
| | Networking components | Intranet components<br>Internet or DMZ components |

- People include employees and nonemployees. There are two categories of employees: those who hold trusted roles and have correspondingly greater authority and accountability, and other staff who have assignments without special privileges. Nonemployees include contractors and consultants, members of other organizations with which the organization has a trust relationship, and strangers.
- Procedures fall into two categories: IT and business standard procedures, and IT and business sensitive procedures. The business sensitive procedures

are those that may assist a threat agent in crafting an attack against the organization or that have some other content or feature that may introduce risk to the organization.

- Data Components have been expanded to account for the management of information in all stages: Transmission, Processing, and Storage.
- Software Components can be assigned to one of three categories: Applications, Operating Systems, or security components. Software Components that provide security controls may span the range of operating systems and applications categories, but are differentiated by the fact that they are the part of the information security control environment and must be protected more thoroughly than other system components.
- **Hardware** is assigned to one of two categories: the usual systems devices and their peripherals, and the devices that are part of information security control systems. The latter must be protected more thoroughly than the former.

## People, Procedures,& Data Asset Identification

People : Position name/number/ID: Supervisor; Security clearance level; special skills.

Procedures : Description/intended purpose/relationship to software / hardware and networking elements; storage location for update; storage location for reference.

Data : Classification; owner; Creator; Manager; Size of data structure; data structure used; online/offline/location/backup procedures employed.

## Hardware, Software, and Network Asset Identification

Depends on the needs of the organization and its risk management efforts.

- **Name**: Should adopt naming standards that do not convey information to potential system attackers.
- **IP address**: Useful for network devices & Servers. Many organizations use the dynamic host control protocol (DHCP) within TCP/IP that reassigns IP numbers to devices as needed, making the use of IP numbers as part of the asset identification process problematic. IP address use in inventory is usually limited to those devices that use static IP addresses.
- **Media Access Control (MAC) address**: Electronic serial numbers or hardware addresses. All network interface hardware devices have a unique number. The MAC address number is used by the network operating system as a means to identify a specific network device. It is used by the client's network software to recognize traffic that it must process.

- **Element Type**: Document the function of each Element by listing its type. For hardware, a list of possible element types, such as servers, desktops, networking devices or test equipment.
    - One server might be listed as
        - Device class= S (Server)
        - Device OS= W2K ( Windows 2000)
        - Device Capacity = AS ( Advanced Server )

**Serial Number**: For hardware devices, the serial number can uniquely identify a specific device.

**Manufacturer Name**: Record the manufacturer of the device or software component. This can be useful when responding to incidents that involve these devices or when certain manufacturers announce specific vulnerabilities.

**Manufacturer's Model No or Part No:** Record the model or part number of the element. This record of exactly what the element is can be very useful in later analysis of vulnerabilities, because some vulnerability instances only apply to specific models of certain devices and software components.

**Software Version, Update revision, or FCO number**: Document the specific software or firmware revision number and, for hardware devices, the current field change order (FCO) number. An FCO is an authorization issued by an organization for the repair, modification, or update of a piece of equipment. Documenting the revision number and FCO is particularly important for networking devices that function mainly through the software running on them. For example, firewall devices often have three versions: an operating system (OS) version, a software version, and a basic input/output system (BIOS) firmware version.

**Physical location**: Note where this element is located physically (Hardware)

**Logical Location**: Note where this element can be found on the organization's network. The logical location is most useful for networking devices and indicates the logical network where the device is connected.

**Controlling Entity**: Identify which organizational unit controls the element.

## Automated Risk Management Tools

-Automated tools identify the system elements that make up the hardware, software, & network components.

-Many organizations use automated asset inventory systems.

-The inventory listing is usually available in a data base.

- Once stored, the inventory listing must be kept current, often by means of a tool that periodically refreshes the data.

**Information Asset Classification**- In addition to the categories, it is advisable to add another dimension to represent the sensitivity & Security priority of the data and the devices that store, transmit & process the data.

- Eg: Kinds of classifications are confidential data, internal data and public data.

## Information Asset Valuation

- As each asset is assigned to its category, posing a number of questions assists in developing the weighting criteria to be used for information asset valuation or impact evaluation. Before beginning the inventory process, the organization should determine which criteria can best be used to establish the value of the information assets. Among the criteria to be considered are:

- Which information Asset is the most critical to the success of the organization.
- Which information asset generates the most revenue?
- Which information asset generates the most probability?
- Which Information asset would be the expensive to replace?

**Sample Inventory Worksheet**

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

| Information assets | Data classification | Impact to profitability |
|---|---|---|
| **Information Transmitted:** | | |
| EDI Document Set 1 —Logistics BOL to outsourcer (outbound) | Confidential | High |
| EDI Document Set 2—Supplier orders (Outbound) | Confidential | High |
| EDI Document Set 2—Supplier fulfillment advice (inbound) | Confidential | Medium |
| Customer order via SSL (inbound) | Confidential | Critical |
| Customer service Request via e-mail (inbound) | Private | Medium |
| **DMZ Assets:** | | |
| Edge Router | Public | Critical |
| Web server #1—home page and core site | Public | Critical |
| Web server #2—Application server | Private | Critical |

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

**FIGURE 4-3** Example Worksheet for the Asset Identification of Information Systems

## Data Classification

1. Confidential

2. Internal
3. External

**Confidential**: Access to information with this classification is strictly on a need-to-know basis or as required by the terms of a contract.

**Internal**: Used for all internal information that does not meet the criteria for the confidential category and is to be viewed only by authorized contractors, and other third parties.

**External:** All information that has been approved by management for public release.

The military uses five level classifications

1. Unclassified data
2. Sensitive But Unclassified data (SBU)
3. Confidential data
4. Secret data
5. Top Secret data

**Unclassified data**: Information that can generally be distributed to the public without any threat to U.S. National interests.

**Sensitive But Unclassified data (SBU)** : Any information of which the loss, misuse, or unauthorized access to, or modification of might adversely affect U.S. national interests, the conduct of Department of Defense(DoD) programs, or the privacy of DoD personnel.

**Confidential data**: Any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

**Secret**: Any information or material the unauthorized disclosure of which reasonably could be cause serious damage to the national security.

**Top Secret Data:** Any information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

**Organization may have**

1. Research data
2. Personnel data
3. Customer data
4. General Internal Communications

**Some organization may use**

1. Public data
2. For office use only
3. Sensitive data
4. Classified data

- **Public**: Information for general public dissemination, such as an advertisement or public release.
- **For Official Use Only**: Information that is not particularly sensitive, but not for public release, such as internal communications.
- **Sensitive**: Information important to the business that could embarrass the company or cause loss of market share if revealed.
- **Classified**: Information of the utmost secrecy to the organization, disclosure of which could severely impact the well-being of the organization.

## Security Clearances

- The other side of the data classification scheme is the personnel security clearance structure.
- Each user of data must be assigned a single authorization level that indicates the level of classification he or she is authorized to view.
    - Eg: Data entry clerk, development Programmer, Information Security Analyst, or even CIO.
    - Most organizations have a set of roles and the accompanying security clearances associated with each role.
    - Overriding an employee's security clearance is the fundamental principle of "need-to-know".

## Management of classified data

- Includes its storage, distribution, portability, and destruction.
- Military uses color coordinated cover sheets to protect classified information from the casual observer.
- Each classified document should contain the appropriate designation at the top and bottom of each page.
- A clean desk policy requires that employees secure all information in appropriate storage containers at the end of each day.
- When Information are no longer valuable, proper care should be taken to destroy them by means of shredding, burning or transferring to a service offering authorized document destruction.
- **Dumpster diving→** to retrieve information that could embarrass a company or compromise information security.

## Threat Identification

After identifying the information assets, the analysis phase moves on to an examination of the threats facing the organization.

## Identify and Prioritize Threats and Threat Agents

### Threats to Information Security

**TABLE 4-3** Threats to Information Security

| Threat | Example |
|---|---|
| Act of human error or failure | Accidents, employee mistakes |
| Compromises to intellectual property | Piracy, copyright infringement |
| Deliberate acts of espionage or trespass | Unauthorized access and data collect |
| Deliberate acts of information extortion | Blackmail for information disclosure |
| Deliberate acts of sabotage or vandalism | Destruction of systems or informatic |
| Deliberate acts of theft | Illegal confiscation of equipment or i |
| Deliberate software attacks | Viruses, worms, macros, denial of ser |
| Forces of nature | Fire, flood, earthquake, lightning |
| Quality of service deviations from service providers | Power and WAN quality of service iss |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopl |
| Technological obsolescence | Antiquated or outdated technologies |



- This examination is known as a threat assessment. You can address each threat with a few basic questions, as follows:
- Which threats present a danger to an organization's assets in the given environment?
- Which threats represent the most danger to the organization's information?
- How much would it cost to recover from a successful attack?
- Which of the threats would require the greatest expenditure to prevent?

**Weighted Ranks of Threats to Information Security**

| Threat | Mean | Standard Deviation | Weight | Weighted Rank |
|---|---|---|---|---|
| Deliberate software attacks | 3.99 | 1.03 | 546 | 2178.3 |
| Forces of Nature | 2.80 | 1.09 | 218 | 610.9 |
| Acts of human error or failure | 3.15 | 1.11 | 350 | 1101.0 |
| Deliberate acts of theft | 3.07 | 1.30 | 226 | 694.5 |
| Technological obsolescence | 2.71 | 1.11 | 158 | 427.9 |
| Technical software failures or errors | 3.16 | 1.13 | 358 | 1129.9 |
| Compromises to intellectual | 2.72 | 1.21 | 181 | 494.8 |

| | | | | |
|---|---|---|---|---|
| property | | | | |

## Vulnerability Identification:

- Create a list of Vulnerabilities for each information asset.
- Groups of people work iteratively in a series of sessions give best result.
- At the end of Identification process, you have a list of assets and their vulnerabilities.

## Vulnerability Assessment of a Hypothetical DMZ Router

| Threat | Possible Vulnerabilities |
|---|---|
| Deliberate software attacks | Internet protocol is vulnerable to denial of service. |
| Acts of human error or failure | Employees may cause outage if configuration errors are made. |
| Technical software failures or errors | Vendor-supplied routing software could fail and cause an outage. |
| Technical hardware failures or errors | Hardware can fail and cause an outage. |
| Deviations in Quality of service | Power system failures are always possible. |
| Deliberate acts of sabotage or vandalism | Internet protocol is vulnerable to denial of service. |
| Deliberate acts of theft | This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised. |
| Technological obsolescence | If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service. |
| Forces of nature | All information assets in the organization are subject to forces of nature, unless suitable controls are provided. |
| Compromises to intellectual property | This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised. |

## Risk Assessment

- Assigns a risk rating or score to each Information asset.
- It is useful in gauging the relative risk to each Vulnerable asset.

## Valuation of Information assets

- Assign weighted scores for the value to the organization of each Information asset.
- National Institute of Standards & Technology (NIST) gives some standards.
- To be effective, the values must be assigned by asking he following questions.
- Which threats present a danger to an organization's assets in the given environment?
- Which threats represent the most danger to the organization's Information?
- How much would it cost to recover from a successful attack?
- Which of the threats would require the greatest expenditure to prevent?

## Likelihood

- It is the probability of specific vulnerability within an organization will be successfully attacked.
- NIST gives some standards.
- 0.1 = Low  1.0 = High
- Eg: Number of network attacks can be forecast based on how many network address the organization has assigned.

## Risk Determination

Risk = [ ( Likelihood of vulnerability occurrence ) X (Value of information Asset )] __ ( % of risk mitigated by current controls) + uncertainty of current knowledge of the Vulnerability

- For the purpose of relative risk assessment, risk equals:
  - Likelihood of vulnerability occurrence TIMES value (or impact)
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Eg: Information Asset A has a value score of 50 & has one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

**Solution:**

Risk = [(1.0) x 50] – 0% + 10%
= (50 x 1.0) – ((50 x 1.0)x 0.0) + ( (50 x 1.0) x 0.1)
= 50 – 0 + 5
= 55

## Identify Possible Controls ( For Residual Risk)

- Residual risk is the risk that remains to the information asset even after the existing control has been applied.
- Three general categories of controls

1. Policies
2. Programs
3. Technologies

1. Policies
   - General Security Policy
   - Program Security Policy
   - Issue Specific Policy
   - Systems Specific Policy
2. Programs
   - Education
   - Training
   - Awareness
3. Security Technologies
   - Technical Implementation Policies

**Access Controls**

- Specially addresses admission of a user into a trusted area of the organization.
- Eg: Computer rooms, Power Rooms.
- Combination of policies , Programs, & Technologies

## Types of Access controls

Mandatory Access Controls (MACs)

- Give users and data owners limited control over access to information resources.

Nondiscretionary Controls

- Managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Discretionary Access Controls ( DAC)

- Implemented at discretion or option of the data user

Lattice-based Access Control

- Variation of MAC - users are assigned matrix of authorizations for particular areas of access.

## Documenting the Results of Risk Assessment

By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them. The goal of this process is to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. You should also have collected some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown in the following table.

| Asset | Asset Impact or Relative value | Vulnerability | Vulnerability Likelihood | Risk Rating Factor |
|---|---|---|---|---|
| Customer Service Request via e-mail(inbound) | 55 | E-mail disruption due to hardware failure | 0.2 | 11 |
| Customer order via SSL - (inbound) | 100 | Lost orders due to Web server hardware failure | 0.1 | 10 |
| Customer order via SSL - (inbound) | 100 | Lost orders due to Web server or ISP service failure | 0.1 | 10 |
| Customer Service Request via e-mail(inbound) | 55 | E-mail disruption due to SMTP mail relay attack | 0.1 | 5.5 |
| Customer Service Request via e-mail(inbound) | 55 | E-mail disruption due to ISP service failure | 0.1 | 5.5 |
| Customer order via SSL - (inbound) | 100 | Lost orders due to Web server denial-of-service attack | 0.025 | 2.5 |
| Customer order via SSL - (inbound)SSL-Secure Sockets Layer | 100 | Lost orders due to Web server software failure | 0.01 | 1 |

# Risk Control Strategies

Four basic strategies to control each of the risks that result from these vulnerabilities.

1. Apply safeguards that eliminate the remaining uncontrolled risks for the vulnerability [Avoidance]
2. Transfer the risk to other areas (or) to outside entities[transference]
3. Reduce the impact should the vulnerability be exploited[Mitigation]
4. Understand the consequences and accept the risk without control or mitigation[Acceptance]

**Avoidance**

It is the risk control strategy that attempts to prevent the exploitation of the vulnerability, and is accomplished by means of

a) Countering threats
b) Removing Vulnerabilities in assets
c) Limiting access to assets
d) Adding protective safeguards.

Three common methods of risk avoidance are

1. Application of policy
2. Application of Training & Education
3. Application of Technology

## Transference

- Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.

- It may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing Insurance, Implementing Service contracts with providers.

Top 10 Information Security mistakes made by individuals.

1. Passwords on Post-it-Notes
2. Leaving unattended computers on.
3. Opening e-mail attachments from strangers.
4. Poor Password etiquette
5. Laptops on the loose (unsecured laptops that are easily stolen)
6. Blabber mouths ( People who talk about passwords)
7. Plug & Play[Technology that enables hardware devices to be installed and configured without the protection provided by people who perform installations]
8. Unreported Security Violations
9. Always behind the times.
10. Not watching for dangers inside the organization

## Mitigation

- It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning & preparation.
    - Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently and effectively.

- Includes 3 types of plans.

1. Incident response plan (IRP) -Actions to take while incident is in progress
2. Disaster recovery plan (DRP) - Most common mitigation procedure.
3. Business continuity plan (BCP) - Continuation of business activities if catastrophic event occurs.

### Incident Response Plan (IRP)

This IRP Plan provides answers to questions such as

1. What do I do now?
2. What should the administrator do first?
3. Whom should they contact?
4. What should they document?

**The IRP Supplies answers.**

For example, a system's administrator may notice that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee.

**The IRP** also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive.

### Disaster Recovery Plan (DRP)

- Can include strategies to limit losses before and during the disaster.
- Include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the floodwater recede.
- DRP focuses more on preparations completed before and actions taken after the incident, whereas the IRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

### Business Continuity Plan (BCP)

- BCP is the most strategic and long term of the three plans.
- It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building or operations center.
- The BCP includes planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.
- Many companies offer this service as a contingency against disastrous events such as fires. Floods, earthquakes, and most natural disasters.

## Acceptance

- It is the choice to do nothing to protect a vulnerability and do accept the outcome of its exploitation.
- This strategy occurs when the organization has:
  - Determined the level of risk.
  - Assessed the probability of attack.
  - Estimated the potential damage that could occur from attacks.
  - Performed a thorough cost benefit analysis.
  - Evaluated controls using each appropriate type of feasibility.
  - Decided that the particular function, service, information, or asset did not justify the cost of protection.

## Selecting a Risk Control Strategy

-Level of threat and value of asset play major role in selection of strategy
-Rules of thumb on strategy selection can be applied:

- When vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.
- When vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk.
- When the attacker's cost is less than his potential gain: Apply protections to increase the attacker's cost.
- When potential loss is substantial: Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss.

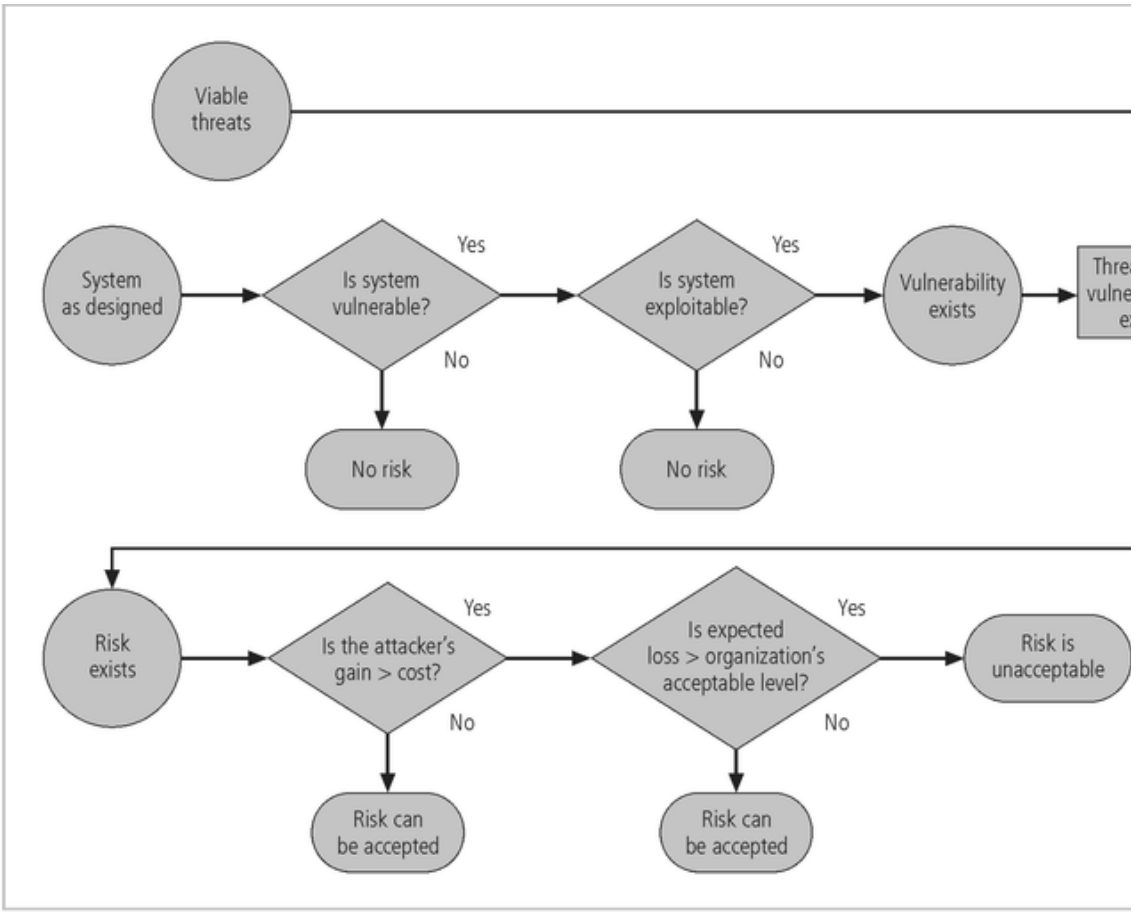



**FIGURE 5-2** Risk Handling Decision Points[7]

## Evaluation, Assessment & Maintenance of Risk Controls

- Once a control strategy has been implemented, it should be monitored, & measured on an ongoing basis to determine the effectiveness of the security controls and the accuracy of the estimate of the Residual risk
- There is no exit from this cycle; it is a process that continues for as long as the organization continues to function.

# Risk Control Cycle

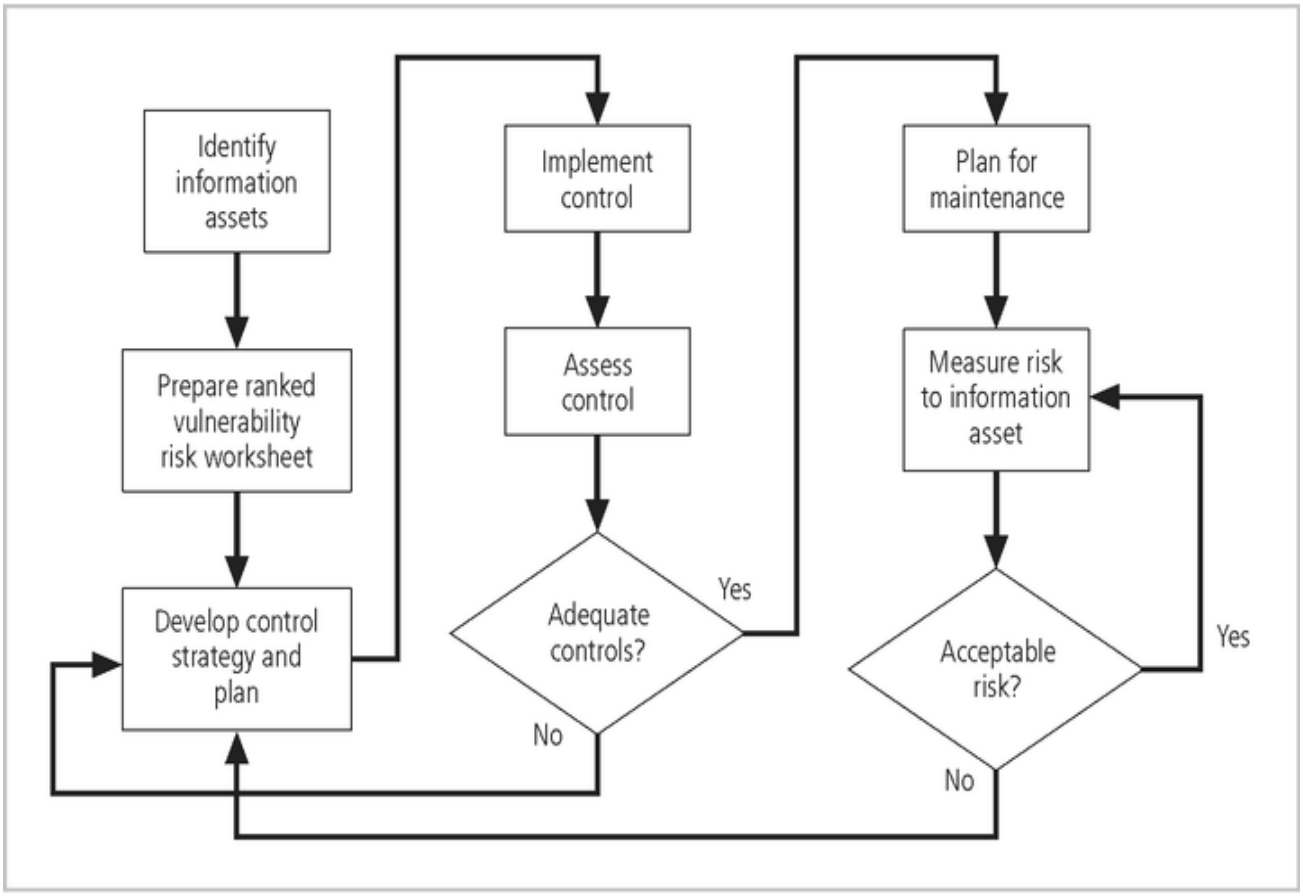



**FIGURE 5-3** Risk Control Cycle[8]

## Categories of Controls

- Controlling risk through avoidance, Mitigation or Transference may be accomplished by implementing controls or safeguards.
- Four ways to categorize controls have been identified.

  - **Control function**
    - Preventive or detective
  - **Architectural layer**
    - One or more layers of technical architecture
  - **Strategy layer**
    - Avoidance, mitigation …

- **Information security principle**

## Control Function

- Safeguards designed to defend systems are either preventive or detective.
- Preventive controls stop attempts to exploit a vulnerability by implementing a security principle, such as authentication, or Confidentiality.
- Preventive controls use a technical procedure, such as encryption, or some combination of technical means and enforcement methods.
- Detective controls – warn organizations of violations of security principles, organizational policies, or attempts to exploit vulnerabilities.
- Detective controls use techniques such as audit trails, intrusion detection and configuration monitoring.

## Architectural Layer

- Controls apply to one or more layers of an organization's technical architecture.
- The following entities are commonly regarded as distinct layers in an organization's Information architecture.

1. Organizational policy.
2. External Networks.
3. Extranets ( or demilitarized zones )
4. Intranets ( WANs and LANs )
5. Network devices that interface network zones.(Switches, Routers, firewalls and hubs)
6. Systems [ Mainframe, Server, desktop]
7. Applications.

## Strategy Layer

Controls are sometimes classified by the risk control strategy they operate within:

1. Avoidance
2. Mitigation
3. transference

## Characteristics of Secure Information

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Accountability

7. Privacy

**Confidentiality**: The control assures the confidentiality of data when it is stored, processed, or transmitted. An example of this type of control is the use of Secure Sockets Layer (SSL) encryption technology to secure Web content as it moves from Web server to browser.

**Integrity**: The control assures that the information asset properly, completely, and correctly receives, processes, stores, and retrieves data in a consistent and correct manner .Ex: Use of parity or cyclical redundancy checks in data transmission protocols.

**Availability**: The control assures ongoing access to critical information assets. Ex: Deployment of a network operations center using a sophisticated network monitoring toolset.

**Authentication**: The control assures that the entity (person or computer) accessing information assets is in fact the stated entity. Ex: The use of cryptographic certificates to establish SSL connections, or the use of cryptographic hardware tokens such as SecurID cards as a second authentication of identity.

**Authorization**: The control assures that a user has been specifically and explicitly authorized to access, update, or delete the contents of an information asset. Ex: Use of access control lists and authorization groups in the Windows networking environment. Another example is the use of a database authorization scheme to verify the designated users for each function.

**Accountability**: The control assures that every activity undertaken can be attributed to a specific named person or automated process. Ex: Use of audit logs to track when each user logged in and logged out of each computer.
Privacy: The control assures that the procedures to access, update, or remove personally identifiable information comply with the applicable laws and policies for that kind of information.

# Feasibility Studies

- Before deciding on the strategy (Avoidance, transference, mitigation, or acceptance), for a specific vulnerability, all the economic and non-economic consequences of the vulnerability facing the information asset must be explored.
- **Cost Avoidance**- It is the process of avoiding the financial impact of an incident by implementing a control.
- Includes
  1. Cost Benefit analysis

2. Organizational feasibility
3. Operational Feasibility
4. Technical Feasibility
5. Political feasibility.

# Cost Benefit Analysis (CBA)

- Organizations are urged to begin the cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets were compromised by the exploitation of a specific vulnerability.
- The formal process to document this decision making process is called a Cost Benefit analysis or an economic feasibility study.

## Cost Benefit Analysis or an Economic Feasibility study

- Some of the items that affect the cost of a control or safeguard include:
  1. Cost of development or acquisition [purchase cost] of hardware, software and services.
  2. Training Fees(cost to train personnel)
  3. Cost of Implementation[Cost to install, Configure, and test hardware, software and services]
  4. service Costs[Vendor fees for maintenance and upgrades]
  5. Cost of maintenance[Labor expense to verify and continually test, maintain and update]

Benefit is the value that an organization realizes by using controls to prevent losses associated with a specific vulnerability.

**Amount of benefit = Value of the Information asset and Value at risk.**

Asset Valuation is the process of assigning financial value or worth to each information asset.
Some of the components of asset valuation include:

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.
5. Value incurred from the cost of protecting the information.
6. Value to owners.
7. Value of intellectual property.
8. Value to adversaries.

9. Loss of Productivity while the information assets are unavoidable.
10. Loss of revenue while information assets are unavailable.

The organization must be able to place a dollar value on each collection of information and the information assets it owns. This value is based on the answers to these questions:

- How much did it cost to create or acquire this information?
- How much would it cost to recreate or recover this information?
- How much does it cost to maintain this information?
- How much is this information worth to the organization?
- How much is this information worth to the competition?

**A Single loss expectancy (SLE)** is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the **exposure factor (EF),** which is the expected percentage of loss that would occur from a particular attack, as follows:

**Single Loss Expectancy (SLE) = Asset value x Exposure factor [EF]**

EF → Expected percentage of loss that would occur from a particular attack.
The probability of threat occurring is usually a loosely derived table indicating the probability of an attack from each threat type within a given time frame (for example, once every 10 years). This value is commonly referred to as the **annualized rate of occurrence (ARO)**
The expected value of a loss can be stated in the following equation:
**Annualized loss Expectancy (ALE)** which is calculated from the ARO and SLE.

**ALE = SLE x ARO**

## Cost Benefit Analysis (CBA)Formula

CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability. The CBA is most easily calculated using the ALE from earlier assessments before the implementation of the proposed control, which is known as ALE (prior). Subtract the revised ALE, estimated based on control being in place, known as ALE (post). Complete the calculation by subtracting the annualized cost of the safeguard (ACS).

**CBA = ALE (Prior) - ALE (Post) - ACS**

Where:

-ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control.

-ALE post is the ALE examined after the control has been in place for a period of time.

-ACS is the Annual Cost of the Safeguard.

# Bench Marking

- An alternative approach to risk management
- Process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization.
- One of two measures typically used to compare practices:
  - **Metrics-based measures**
  - **Process-based measures**
- Good for potential legal protection.
- **Metrics-based measures** are comparisons based on numerical standards, such as:
  1. Numbers of successful attacks.
  2. Staff-hours spent on systems protection.
  3. Dollars spent on protection.
  4. Numbers of Security Personnel.
  5. Estimated value in dollars of the information lost in successful attacks.
  6. Loss in productivity hours associated with successful attacks.

The difference between an organization's measures and those of others is often referred to as a performance gap. The other measures commonly used in benchmarking are process-based measures. **Process-based measures** are generally less focused on numbers and more strategic than metrics-based-measures.

## Due Care/Due Diligence

- When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances - this is referred to as a standard of due care
- Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection
- Failure to support a standard of due care or due diligence can open an organization to legal liability

## Best Business Practices

- Security efforts that provide a superior level of protection of information are referred to as best business practices
- Best security practices (BSPs) are security efforts that are among the best in the industry
- When considering best practices for adoption in your organization, consider the following:
  - Does your organization resemble the identified target?
  - Are the resources you can expend similar?

- Are you in a similar threat environment?

## Microsoft's Ten Immutable Laws of Security

1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
2. If a bad guy can alter the operating system on your computer, it's not your computer anymore
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
4. If you allow a bad guy to upload programs to your web site, it's not your web site anymore
5. Weak passwords trump strong security
6. A machine is only as secure as the administrator is trustworthy
7. Encrypted data is only as secure as the decryption key
8. An out of date virus scanner is only marginally better than no virus scanner at all
9. Absolute anonymity isn't practical, in real life or on the web
10. Technology is not a panacea

## Problems

- The biggest problem with benchmarking in information security is that organizations don't talk to each other.
- Another problem with benchmarking is that no two organizations are identical
- A third problem is that best practices are a moving target.
- One last issue to consider is that simply knowing what was going on a few years ago, as in benchmarking, doesn't necessarily tell us what.

## Baselining

- Baselining is the analysis of measures against established standards,
- In information security, baselining is comparing security activities and events against the organization's future performance.
- When baselining it is useful to have a guide to the overall process

## Feasibility Studies and the Cost Benefit analysis

- Before deciding on the strategy for a specific vulnerability all information about the economic and non-economic consequences of the vulnerability facing the information asset must be explored.
- Fundamentally we are asking "What are the actual and perceived advantages of implementing a control contrasted with the actual and perceived disadvantages of implementing the control?"

## Cost Benefit Analysis (CBA)

- The most common approach for a project of information Security controls and safeguards is the economic feasibility of implementation.
- Begins by evaluating the worth of information assets are compromised.

- It is only common sense that an organization should not spend more to protect an asset than it is worth.
- The formal process to document this is called a cost benefit analysis or an economic feasibility study.

## CBA: Cost Factors

- Some of the items that the cost of a control or safeguard include:
- Cost of Development or Acquisition
- Training Fees
- Cost of implementation.
- Service Costs
- Cost of Maintenance

## CBA: Benefits

- Benefit is the value that the organization recognizes by using controls to prevent losses associated with a specific vulnerability.
- This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk.

## CBA: Asset Valuation

- Asset Valuation is the process of assigning financial value or worth to each information asset.
- The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss and litigation.
- These estimates are calculated for each set of information bearing systems or information assets.
- There are many components to asset valuation.

## CBA: Loss Estimates

- Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence.
- This process results in the estimate of potential loss per risk.
- The questions that must be asked here include:
    - What damage could occur, and what financial impact would it have?
    - What would it cost to recover from the attack, in addition to the costs above?
    - What is the single loss expectancy for each risk?

## Organizational Feasibility

- Organizational Feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization.
- Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

## Operational feasibility

- Addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stake holders.
- Sometimes known as behavioral feasibility, because it measures the behavior of users.
- One of the fundamental principles of systems development is obtaining user buy in on a project and one of the most common methods for obtaining user acceptance and support is through user involvement obtained through three simple steps:

- Communicate
- Educate
- Involve

## Technical Feasibility

- The project team must also consider the technical feasibilities associated with the design, implementation, and management of controls.
- Examines whether or not the organization has or can acquire the technology necessary to implement and support the control alternatives.

## Political feasibility

- For some organizations, the most significant feasibility evaluated may be political
- Within Organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest.
- The limits placed on an organization's actions or a behavior by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

## Risk Management Discussion Points

Not every organization has the collective will to manage each vulnerability through the application of controls

- Depending on the willingness to assume risk, each organization must define its risk appetite
- Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility

## Residual Risk

- When we have controlled any given vulnerability as much as we can, there is often risk that has not been completely removed or has not been completely shifted or planned for this remainder is called residual risk.
- To express it another way, "Residual risk is a combined function of
    1. A threat less the effect of some threat –reducing safeguards.
    2. Vulnerability less the effect of some vulnerability- reducing safeguards.
    3. an asset less the effect of some asset value-reducing safeguards "

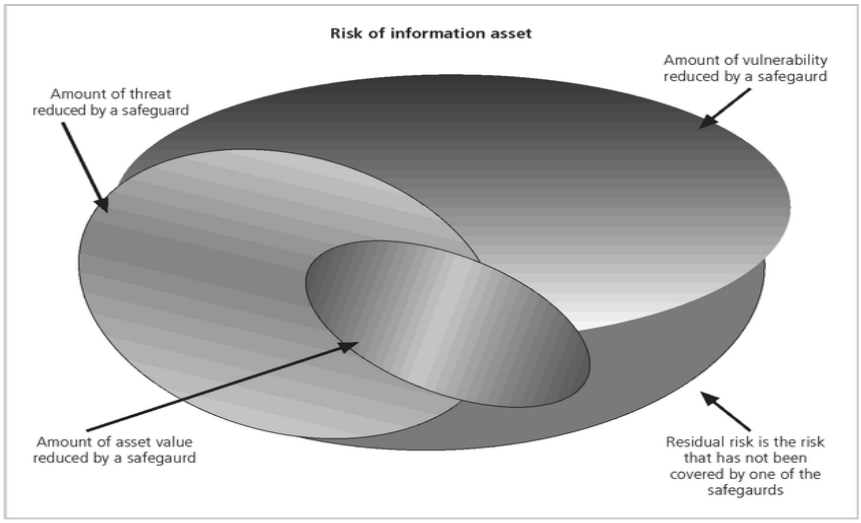



**FIGURE 5-4** Risk Residual

## Documenting Results

- At minimum, each information asset-vulnerability pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed.
- Some organizations document the outcome of the control strategy for each information asset-vulnerability pair as an action plan
- This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual

## Recommended Practices in Controlling Risk

- We must convince budget authorities to spend up to the value of the asset to protect a particular asset from an identified threat
- Each and every control or safeguard implemented will impact more than one threat-asset pair

## Qualitative Measures

- The spectrum of steps described above was performed with real numbers or best guess estimates of real numbers-this is known as a quantitative assessment.
- However, an organization could determine that it couldn't put specific numbers on these values.
- Fortunately, it is possible to repeat these steps using estimates based on a qualitative assessment.
- Instead of using specific numbers, ranges or levels of values can be developed simplifying the process

## Delphi Technique

- One technique for accurately estimating scales and values is the Delphi Technique.

- The Delphi Technique, named for the Oracle at Delphi, is a process whereby a group of individuals rate or rank a set of information
- The individual responses are compiled and then returned to the individuals for another iteration
- This process continues until the group is satisfied with the result.

## Review Questions

1. What is Risk Management? Why is the identification of risks, by listing assets and their vulnerabilities, so important to the risk management process?
2. According to Sun Tzu, what two key understandings must you achieve to be successful in battle?
3. Mention the benefits of Risk Management.
4. State the roles involved in Risk Management.
5. What is Risk Management? State the methods of identifying and assessing risk management?
6. What do you mean by Risk identification?
7. Discuss in detail the process of assessing and controlling risk management issues.
8. Who is responsible for risk management in an organization? Which community of interest usually takes the lead in information security risk management?
9. In risk management strategies, why must periodic review be a part of the process?
10. What are vulnerabilities? How do you identify them?
11. What are the four strategies for controlling risk?
12. Write the important risk factors of information security.
13. Describe risk avoidance. Name three common methods of risk avoidance.
14. Describe risk transference. Describe how outsourcing can be used for risk transference.
15. Describe risk mitigation. What three planning approaches are discussed in the text as opportunities, to mitigate risk?
16. List any four Information Security Policies.
17. How do you categories the components of an information system? Explain.
18. What do you mean by access control? Describe the different types of access control and risk control strategies.
19. How is an incident response plan different from a disaster recovery plan?
20. What is risk appetite? Explain why risk appetite varies from organization to organization.
21. What is cost benefit analysis?
22. What is the definition of single loss expectancy? What is annual loss expectancy?
23. What is residual risk?
24. Which is more important to the system components classification scheme: that the asset identification list be comprehensive or mutually exclusive?