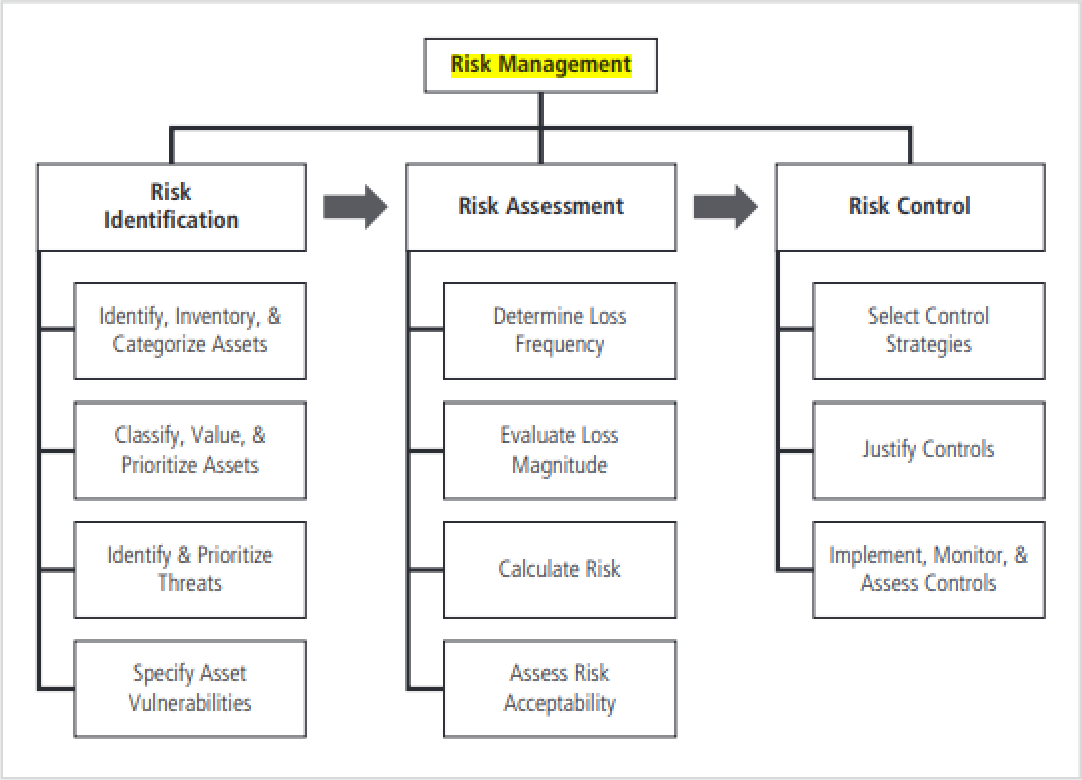
RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities in an organization’s information systems and taking carefully reasoned steps to assure

- Confidentiality
- Integrity
- Availability

Risk management involves three major undertakings:

- risk identification,
- risk assessment, and
- risk control


Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Determine Loss Frequency
Evaluate Loss Magnitude
Calculate Risk
Assess Risk Acceptability
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

© Cengage Learning 2015

Figure 5-1 Components of risk management

Residual risk

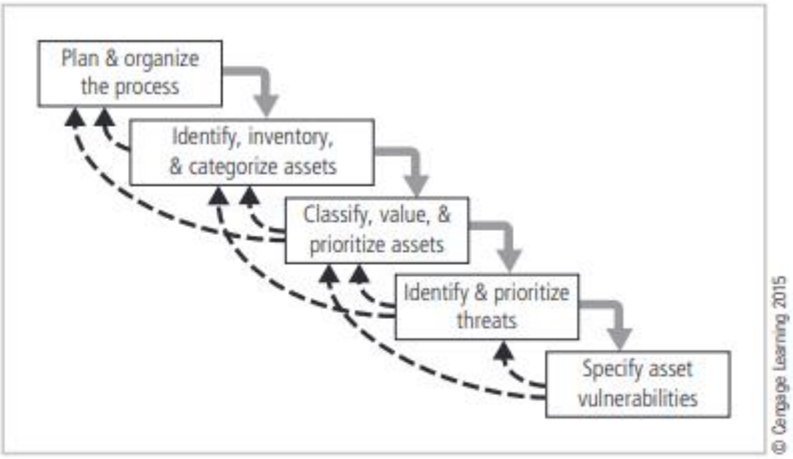
The amount of risk that remains to an information asset even after the organization has applied its desired level of controls.

Risk appetite

The amount of risk an organization is willing to accept.

Risk Identification

A risk management strategy requires that information security professionals know their organizations' information assets—that is, how to identify, classify, and prioritize them. Once the organizational assets have been identified, a threat assessment process is used to identify and quantify the risks facing each asset.


Plan & organize the process
Identify, inventory, & categorize assets
Classify, value, & prioritize assets
Identify & prioritize threats
Specify asset vulnerabilities

© Cengage Learning 2015

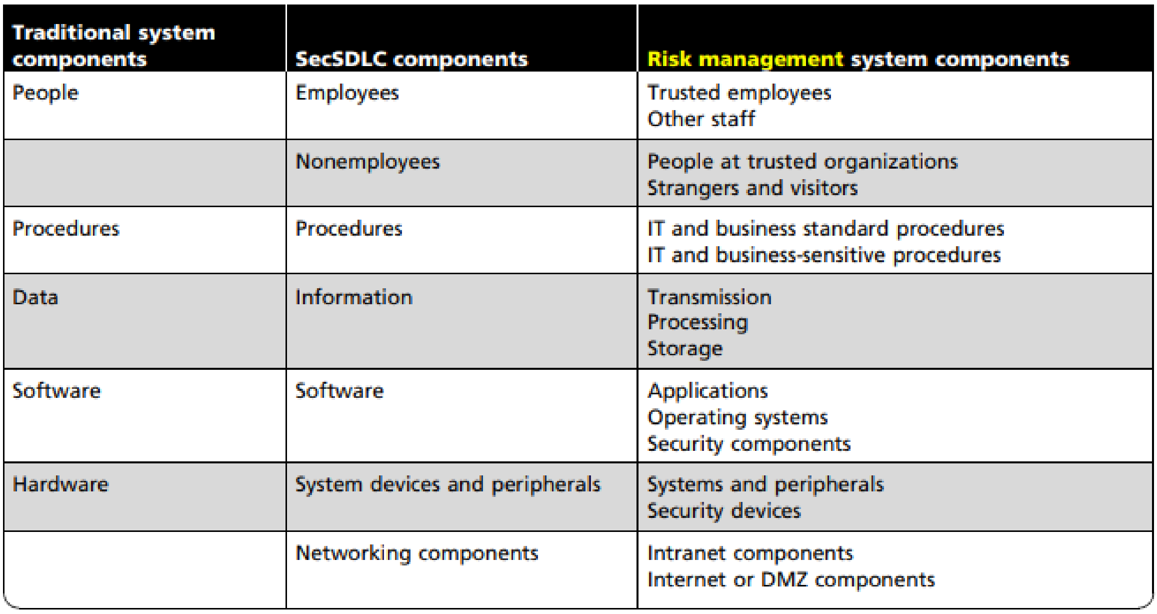
Figure 5-4 Components of risk identification

Planning and Organizing the Process:

The first step in risk identification is to follow your project management principles. You begin by organizing a team, which typically consists of representatives from all affected groups. Because risk can exist everywhere in the organization, representatives will come from every department and will include users, managers, IT groups, and information security groups. The process must then be planned, with periodic deliverables, reviews, and presentations to management. Once the project is ready to begin, the team can organize a meeting like the one Charlie is conducting in the opening case. Tasks are laid out, assignments are made, and timetables are discussed.

Identifying, Inventorying, and Categorizing Assets

This iterative process begins with the identification and inventory of assets, including all elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements. Then, you categorize the assets, adding details as you dig deeper into the analysis. The objective of this process is to establish the relative priority of assets to the success of the organization.



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

Table 5-1 **Categorizing the Components of an Information System**

People, Procedures, and Data Asset Identification

Identifying assets for human resources, documentation, and data is more difficult than identifying hardware and software assets. People with knowledge, experience, and judgment should be assigned the task. As assets for people, procedures, and data are identified, they should be recorded using a reliable data-handling process.

When deciding which information assets to track, consider the following asset attributes:

- **People:** Position name, number, or ID (avoid using people's names and stick to identifying positions, roles, or functions); supervisor; security clearance level; special skills

- **Procedures:** Description; intended purpose; relationship to software, hardware, and networking elements; storage location for reference; storage location for update

- **Data:** Classification; owner, creator, and manager; size of data structure; data structure used (sequential or relational); online or offline; location; backup procedures employed.

Hardware, Software, and Network Asset Identification

Consider the following asset attributes:

- **Name:** Use the most common device or program name. Organizations may have several names for the same product.
- **IP address:** This can be a useful identifier for network devices and servers, but it does not usually apply to software. You can, however, use a relational database to track software instances on specific servers or networking devices.
- **Media access control (MAC) address:** MAC addresses are sometimes called electronic serial numbers or hardware addresses. As part of the TCP/IP standard, all

network interface hardware devices have a unique number. The MAC address number is used by the network operating system to identify a specific network device. It is used by the client's network software to recognize traffic that it must process.

- **Element type:** For hardware, you can develop a list of element types, such as servers, desktops, networking devices, or test equipment. The list can have any degree of detail you require. For software elements, you may develop a list of types that includes operating systems, custom applications by type, packaged applications, and specialty applications, such as firewall programs.
- **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 the device or when certain manufacturers announce specific vulnerabilities.
- **Manufacturer's model number or part number**: Record the model or part number of the element. This exact record of the element can be very useful in later analysis of vulnerabilities, because some vulnerability instances apply only to specific models of certain devices and software components.
- **Software version, update revision, or FCO number**: An FCO is an authorization issued by an organization for the repair, modification, or update of a piece of equipment.
- **Physical location**: Note the element's physical location.
- **Logical location:** Note where the 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.

Asset Inventory

Creating an inventory of information assets is a critical function of understanding what the organization is protecting. The inventory process involves formalizing the identification process in some form of organizational tool. At this point in the process, simple spreadsheets and database tools can provide effective record keeping. The inventory information can be updated later with classification and valuation data. Automated tools can sometimes identify the system elements that make up hardware, software, and network components.

Asset Categorization

The SecSDLC and risk management categorizations introduce several new subdivisions:

- People comprise employees and nonemployees. There are two subcategories 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 trusted organizations, and strangers.
- Procedures essentially belong in one of two categories: procedures that do not expose knowledge a potential attacker might find useful, and sensitive procedures that could

allow an adversary to gain an advantage or craft an attack against the organization's assets.

- Data components account for the management of information in all its states: transmission, processing, and storage.
- Software components are assigned to one of three categories: applications, operating systems, or security components.
- Hardware is assigned to one of two categories: the usual system devices and their peripherals, and devices that are part of information security control systems.

Classifying, Valuing, and Prioritizing Information Assets

Most organizations further subdivide the categories. You should also include a dimension to represent the sensitivity and security priority of the data and the devices that store, transmit, and process the data—that is, a data classification scheme. Examples of data classification categories are confidential, internal, and public.

Data classification scheme A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.

The categories be comprehensive and mutually exclusive. Comprehensive means that all information assets must fit in the list somewhere, and mutually exclusive means that an information asset should fit in only one category.

Data Classification and Management

Corporate and government organizations use a variety of classification schemes. Many corporations use a data classification scheme to help secure the confidentiality and integrity of information. A simplified information classification scheme would have three categories: confidential, internal, and external.

The information classifications are as follows:

- **Confidential:** Used for the most sensitive corporate information that must be tightly controlled, even within the company. Information with this classification may also be referred to as "sensitive" or "proprietary."
- **Internal:** Used for all internal information that does not meet the criteria for the confidential category. Internal information is to be viewed only by corporate employees, authorized contractors, and other third parties.
- **External:** All information that has been approved by management for public release

For most NSI (National Security Information), which is vital to the security of the nation, the government uses a three-level classification scheme: Top Secret, Secret and Confidential.

- " 'Top Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

- ‘Secret’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- ‘Confidential’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

For non-NSI material, other classification schemes are employed. Each of these is defined below.

- Sensitive but Unclassified data (SBU): Information that if lost, misused, accessed without authorization, or modified might adversely affect U.S. interests, the conduct of DoD programs, or the privacy of DoD personnel. Common SBU categories include Restricted, For Official Use Only, Not for Public Release, and For Internal Use Only.
- Unclassified data: Information that can generally be distributed to the public without any threat to U.S. interests.

Security clearance

A component of a data classification scheme that assigns a status level to employees to designate the maximum level of classified data they may access.

Management of Classified Data

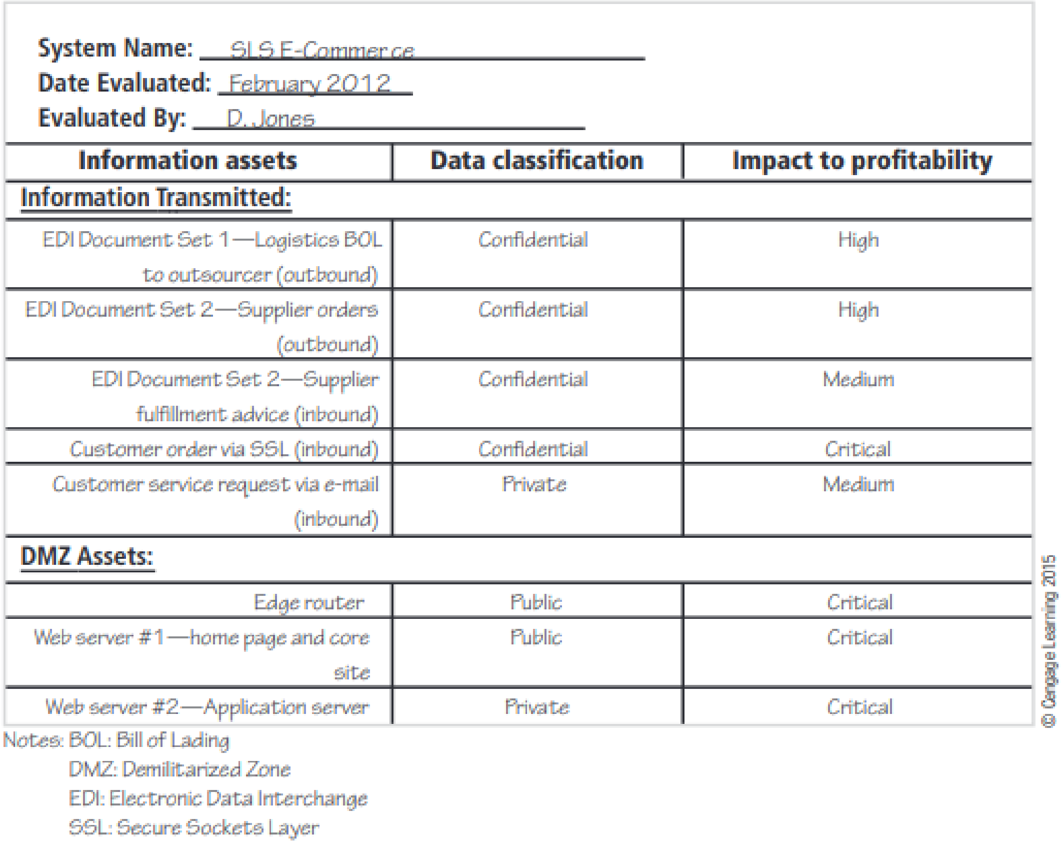
Management of classified data includes its storage, distribution, transportation, and destruction. All information that is not unclassified or public must be clearly marked.

- **clean desk policy** An organizational policy that specifies employees must inspect their work areas and ensure that all classified information, documents, and materials are secured at the end of every work day.
- **dumpster diving** An information attack that involves searching through a target organization’s trash and recycling bins for sensitive information

Information Asset Valuation

The process of assigning financial value or worth to each information asset.

To assist in the process of assigning values to information assets for risk assessment purposes, you can pose several questions and collect your answers on a worksheet for later analysis. Before beginning the inventory process, the organization should determine which criteria can best establish the value of the information assets.



System Name: SLS E-Commerce
Date Evaluated: February 2012
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

© Cengage Learning 2015

Figure 5-7 Sample inventory worksheet

Among the criteria to be considered are:

- Which information asset is most critical to the organization's success?
  When determining the relative importance of each asset, refer to the organization's mission statement or statement of objectives to determine which elements are essential, which are supportive, and which are merely adjuncts.
- Which information asset generates the most revenue?
  You can also determine which information assets are critical by evaluating how much of the organization's revenue depends on a particular asset.
- Which of these assets plays the biggest role in generating revenue or delivering services? Which information asset generates the most profitability? Organizations should evaluate how much of the organization's profitability depends on a particular asset.
- Which information asset would be the most expensive to replace? Sometimes an information asset acquires special value because it is unique.
- Which information asset would be the most expensive to protect? In this case, you are determining the cost of providing controls.
- Which information asset would most expose the company to liability or embarrassment if revealed? Almost every organization is aware of its local, national, and international image.

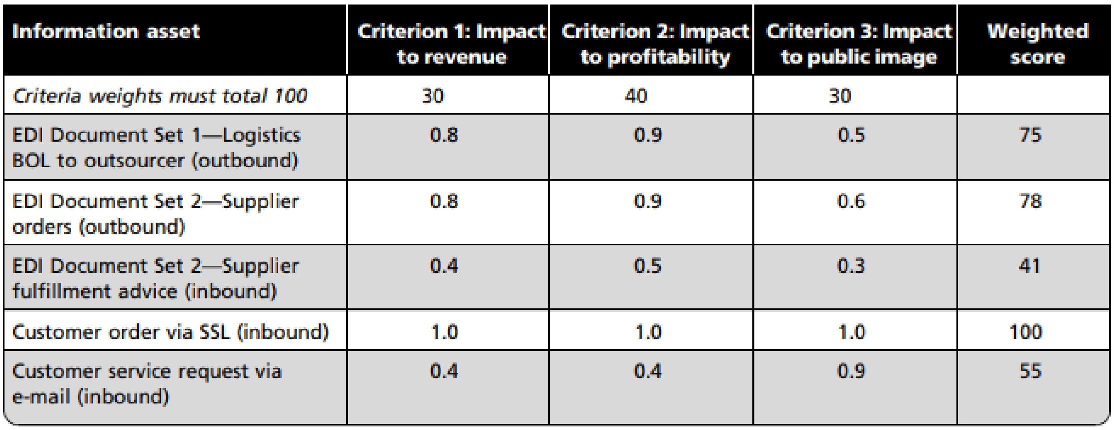
When it is necessary to calculate, estimate, or derive values for information assets, you might give consideration to the following:

- Value retained from the cost of creating the information asset: Information is created or acquired at some cost to the organization. This cost can be calculated or estimated. One category of this cost is software development, and another is data collection and processing.
- Value retained from past maintenance of the information asset: It is estimated that for every dollar spent developing an application or acquiring and processing data, many more dollars are spent on maintenance over the useful life of the data or software.
- Value implied by the cost of replacing the information: Another important cost associated with the loss or damage to information is the cost of replacing or restoring it.
- Value from providing the information: Separate from the cost of developing or maintaining information is the cost of providing it to the users who need it. This cost includes the value associated with delivery of information via databases, networks, and hardware and software systems. It also includes the cost of the infrastructure necessary to provide access and control of the information.
- Value incurred from the cost of protecting the information: This value is a recursive dilemma. In other words, the value of an asset is based in part on the cost of protecting it, while the amount of money spent to protect an asset is based in part on its value.
- Value to owners: How much is your Social Security number or telephone number worth to you? Placing a value on information can be a daunting task.
- Value of intellectual property: Related to the value of information is the specific consideration of the value of intellectual property.
- Value to adversaries: How much would it be worth to an organization to know what the competition is doing? Many organizations have departments that deal in competitive intelligence and that assess and estimate the activities of their competition.

To finalize this step of information asset identification, each organization should assign a weight to each asset based on the answers to the chosen questions.

Information Asset Prioritization

Once the inventory and value assessment are complete, you can prioritize each asset using a straightforward process known as weighted factor analysis.



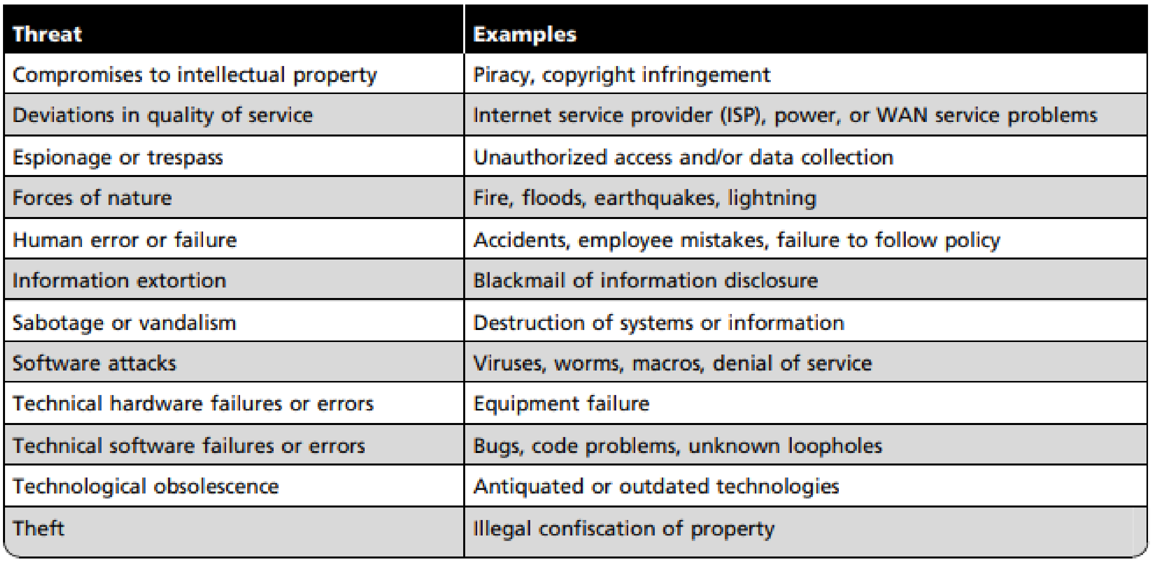
Information asset	Criterion 1: Impact to revenue	Criterion 2: Impact to profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 5-2 **Example of a Weighted Factor Analysis Worksheet**

In this process, each information asset is assigned scores for a set of assigned critical factors. a score is assessed for each asset according to three assigned critical factors. In the example, the scores range from 0.1 to 1.0, which is the range of values recommended in NIST SP 800-30, Risk Management for Information Technology Systems. The document is published by the National Institute of Standards and Technology. In addition, each critical factor is assigned a weight ranging from 1 to 100 to show the criterion's assigned importance for the organization.

Identifying and Prioritizing Threats

After an organization identifies and performs the preliminary classification of its information assets, the analysis phase next examines threats to the organization.



Threat	Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Table 5-3 **Threats to Information Security**[8]

Each threat must be examined to assess its potential to endanger the organization. This examination is known as a threat assessment. You can begin a threat assessment by answering a few basic questions, as follows:

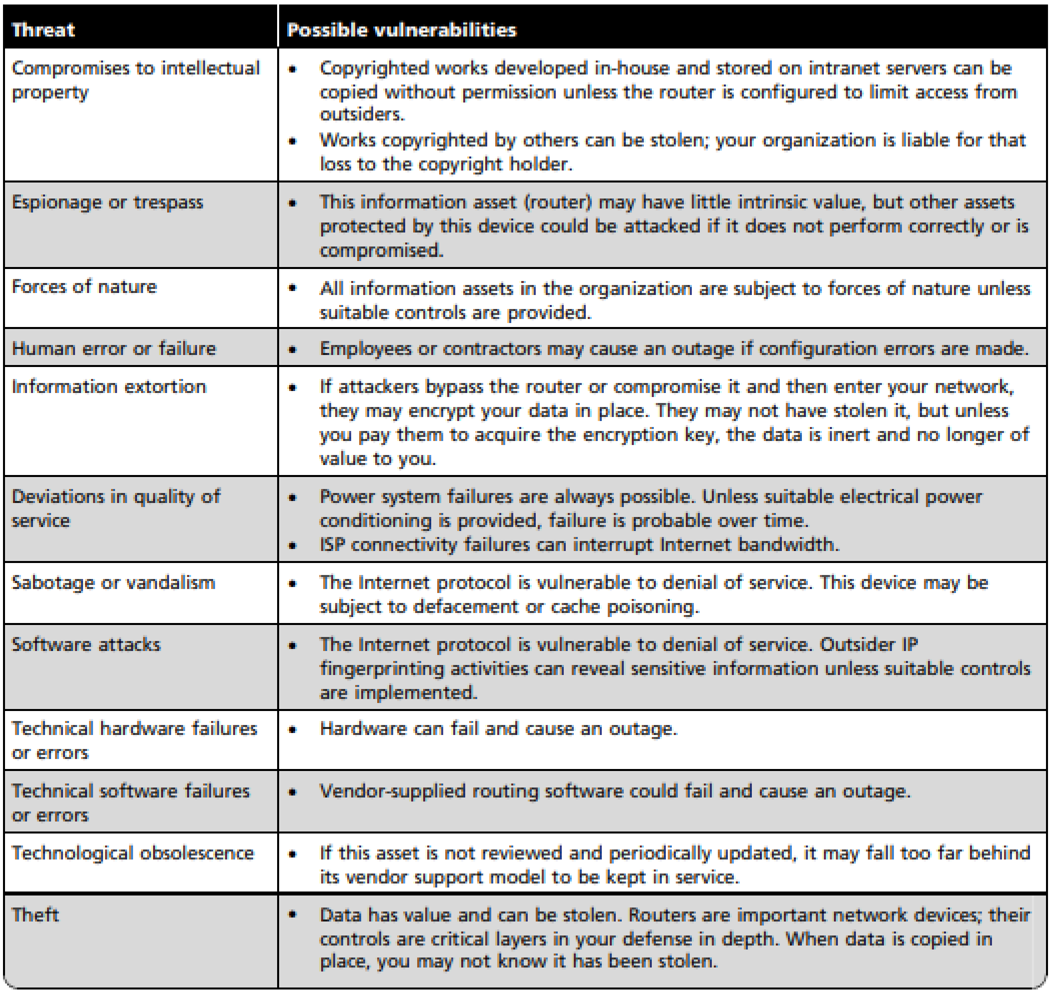
- Which threats present a danger to an organization's assets in the given environment?
- Which threats represent the most danger to the organization's information?

- How much would it cost to recover from a successful attack?
- Which of the threats would require the greatest expenditure to prevent?

Specifying Asset Vulnerabilities

Once you have identified the organization's information assets and documented some criteria for beginning to assess the threats it faces, you review each information asset for each relevant threat and create a list of vulnerabilities. Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset.

At this point in the risk identification phase, the focus is simply on identifying assets that have a vulnerability, not determining how vulnerable they are.

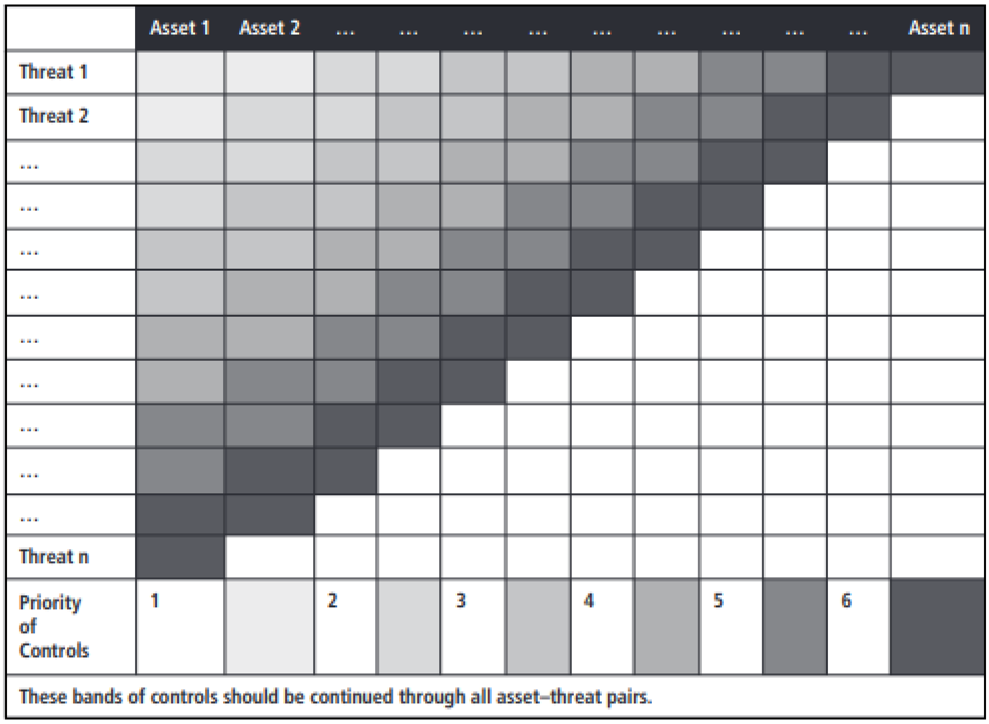


Threat	Possible vulnerabilities
Compromises to intellectual property	• Copyrighted works developed in-house and stored on intranet servers can be copied without permission unless the router is configured to limit access from outsiders. • Works copyrighted by others can be stolen; your organization is liable for that loss to the copyright holder.
Espionage or trespass	• This information asset (router) may have little intrinsic value, but other assets protected by this device could be attacked if it does not perform correctly or is compromised.
Forces of nature	• All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	• Employees or contractors may cause an outage if configuration errors are made.
Information extortion	• If attackers bypass the router or compromise it and then enter your network, they may encrypt your data in place. They may not have stolen it, but unless you pay them to acquire the encryption key, the data is inert and no longer of value to you.
Deviations in quality of service	• Power system failures are always possible. Unless suitable electrical power conditioning is provided, failure is probable over time. • ISP connectivity failures can interrupt Internet bandwidth.
Sabotage or vandalism	• The Internet protocol is vulnerable to denial of service. This device may be subject to defacement or cache poisoning.
Software attacks	• The Internet protocol is vulnerable to denial of service. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	• Hardware can fail and cause an outage.
Technical software failures or errors	• Vendor-supplied routing software could fail and cause an outage.
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.
Theft	• Data has value and can be stolen. Routers are important network devices; their controls are critical layers in your defense in depth. When data is copied in place, you may not know it has been stolen.

Table 5-7 Vulnerability Assessment of a Hypothetical DMZ Router

The TVA Worksheet

At the end of the risk identification process, you should have a prioritized list of assets and their vulnerabilities. You should also have a list that prioritizes the threats facing the organization based on the weighted table discussed earlier. These two lists can be combined into a threats-vulnerabilities-assets (TVA) worksheet in preparation for adding vulnerability and control information during risk assessment.



	Asset 1	Asset 2	…	…	…	…	…	…	…	…	…	Asset n
Threat 1	▁	▁	▂	▂	▃	▃	▄	▄	▅	▅	▆	▆
Threat 2	▁	▂	▂	▃	▃	▄	▄	▅	▅	▆	▆	
…	▂	▂	▃	▃	▄	▄	▅	▅	▆	▆		
…	▂	▃	▃	▄	▄	▅	▅	▆	▆			
…	▃	▃	▄	▄	▅	▅	▆	▆				
…	▃	▄	▄	▅	▅	▆	▆					
…	▄	▄	▅	▅	▆	▆						
…	▄	▅	▅	▆	▆							
…	▅	▅	▆	▆								
…	▅	▆	▆									
…	▆	▆										
Threat n	▆											
Priority of Controls	1	▁	2	▂	3	▃	4	▄	5	▅	6	▆
These bands of controls should be continued through all asset–threat pairs.												

Table 5-8 Sample TVA Spreadsheet

The prioritized list of threats is placed along the vertical axis, with the most important or most dangerous threat listed at the top. The resulting grid provides a convenient method of determining the exposure of assets, and allows a simplistic vulnerability assessment. As you begin the risk assessment process, create a list of threats-vulnerabilities-assets (TVA) triples to help identify the severity of vulnerabilities.

If the intersection of threat 1 and asset 1 has no vulnerability, then the risk assessment team simply crosses out that box. It is much more likely, however, that one or more vulnerabilities exist between the two. As these vulnerabilities are identified, they are categorized as follows:
T1V1A1—Vulnerability 1 that exists between Threat 1 and Asset 1

T1V2A1—Vulnerability 2 that exists between Threat 1 and Asset 1

T2V1A1—Vulnerability 1 that exists between Threat 2 and Asset 1 … and so on.

In the risk assessment phase, the assessment team examines not only vulnerabilities but any existing controls that protect the asset or mitigate possible losses. Cataloging and categorizing these controls is the next step in the TVA spreadsheet.

Risk Assessment

The process of evaluating the relative risk for each vulnerability is known as risk assessment.

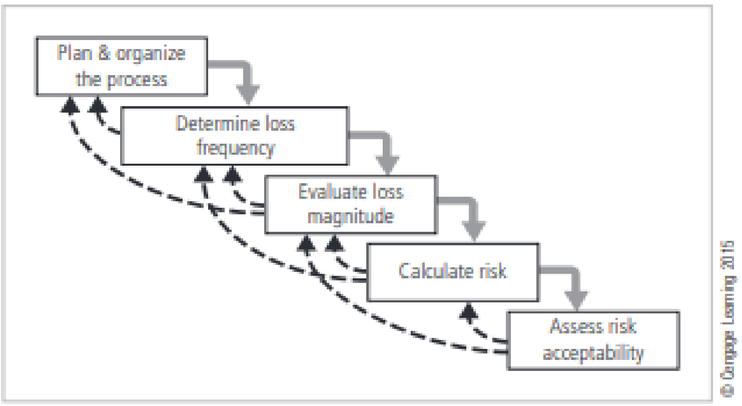
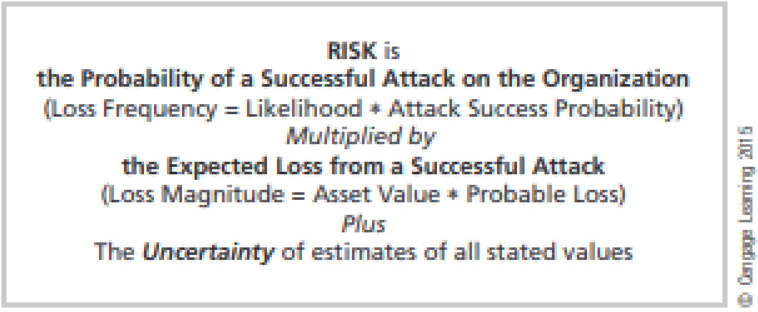


Figure 5-8 Major stages of risk assessment

1) Planning and Organizing Risk Assessment

The goal at this point is to create a method for evaluating the relative risk of each listed vulnerability.



RISK is
the Probability of a Successful Attack on the Organization
(Loss Frequency = Likelihood * Attack Success Probability)
Multiplied by
the Expected Loss from a Successful Attack
(Loss Magnitude = Asset Value * Probable Loss)
Plus
The *Uncertainty* of estimates of all stated values

© Cengage Learning 2015

Figure 5-9 Factors of risk

2) Determining the Loss Frequency

Loss frequency describes an assessment of the likelihood of an attack combined with its expected probability of success if it targets your organization (attack success probability). The resulting information will be coupled with an expected level of loss in evaluating risk. This calculation is also known as the annualized rate of occurrence.

Likelihood In risk assessment, you assign a numeric value to the likelihood of an attack on your organization. For each threat, the organization must determine the expected likelihood of attack, which is typically converted to an annual value. For example, if an organization within a particular industry is targeted by hackers once every five years, the annualized likelihood of attack is 1/5, or 20 percent. This likelihood is often relayed as a 20 percent probability of an attack, given the current control structure.

An event with a likelihood of more than once a year obviously has a higher probability of attack.

Attack Success Probability The second half of the loss frequency calculation is determining the probability of an attack's success if the organization becomes a target. The key component of this assessment is that the attack successfully compromises vulnerabilities in the organization's information asset. Another important part of the assessment is determining the organization's current level of protection.

Loss Event Frequency Combining the likelihood and attack success probability results in an assessment of the loss frequency, also known as loss event frequency. Loss frequency is the probability that an organization will be the target of an attack, multiplied by the probability that the organization's information assets will be successfully compromised if attacked.

3) Evaluating Loss Magnitude

The next important step of risk assessment is to determine how much of an information asset could be lost in a successful attack. This quantity is known as the loss magnitude or asset exposure; its evaluation can be quantitative or qualitative.

The event loss magnitude combines the value of an information asset with the percentage of that asset that would be lost in the event of a successful attack.

The difficulty of making these calculations is twofold:

- Valuating an information asset is extremely difficult, but if the organization can assess an asset to provide a working value, it is the first component of the loss magnitude.
- The second difficulty is estimating what percentage of an information asset might be lost during each of the best-case, worst-case, and most likely scenarios, given that the organization may have little or no experience in assessing such losses. Again, information from industry surveys, insurance organizations, and other sources may assist.

4) Calculating Risk

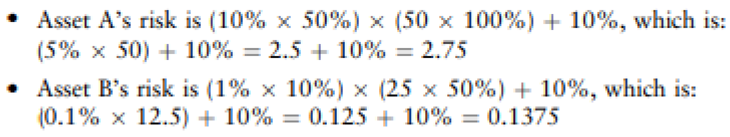
If an organization can determine loss frequency and loss magnitude for an asset, it can then calculate the risk to the asset. For the purpose of relative and simplistic risk determination, risk equals loss frequency times loss magnitude plus an element of uncertainty.

Example:

- Information asset A is an online e-commerce database. Industry reports indicate a 10 percent chance of an attack this year, based on an estimate of one attack every 10 years. The information security and IT departments report that if the organization is attacked, the attack has a 50 percent chance of success based on current asset vulnerabilities and protection mechanisms. The asset is valued at a score of 50 on a scale of 0 to 100, and information security and IT staff expect that 100 percent of the asset would be lost or compromised by a successful attack. You estimate that the assumptions and data are 90 percent accurate.
- Information asset B is an internal personnel database behind a firewall. Industry reports indicate a 1 percent chance of an attack. The information security and IT departments report that if the organization is attacked, the attack has a 10 percent chance of success based on current asset vulnerabilities and protection mechanisms. The asset is valued

at a score of 25 on a scale of 0 to 100, and information security and IT staff expect that 50 percent of the asset would be lost or compromised by a successful attack, because not all of the asset is stored in a single location. You estimate that the assumptions and data are 90 percent accurate.

Here are the risk ratings for the two vulnerabilities:



- Asset A's risk is (10% × 50%) × (50 × 100%) + 10%, which is:
  (5% × 50) + 10% = 2.5 + 10% = 2.75
- Asset B's risk is (1% × 10%) × (25 × 50%) + 10%, which is:
  (0.1% × 12.5) + 10% = 0.125 + 10% = 0.1375

Based on these calculations, the organization's asset A has a much higher level of risk than asset B.

5) **Assessing Risk Acceptability**

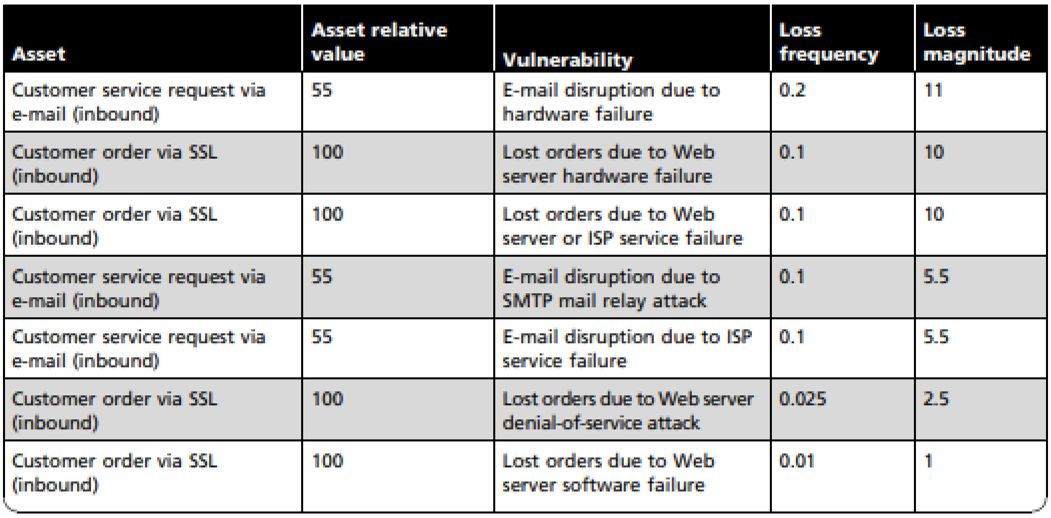
For each threat and its associated vulnerabilities that have residual risk, you must create a ranking of their relative risk level. Next, the organization must compare the residual risk to its risk appetite—the amount of risk the organization is willing to tolerate.

- When the organization's risk appetite is less than an asset's residual risk, it must move to the next stage of risk control and look for additional strategies to further reduce the risk. Failure to do so indicates negligence on the part of the organization's security and management teams.
- When the organization's risk appetite is greater than the asset's residual risk, the organization should move to the latter stages of risk control and continue to monitor and assess its controls and assets.

Documenting the Results of Risk Assessment

By the end of the risk assessment process, you will probably have long lists of information assets and data about each of them. The goal so far has been to identify the information assets that have specific vulnerabilities, list them, and then rank them according to which need protection most.

The final summarized document is the ranked vulnerability risk worksheet.



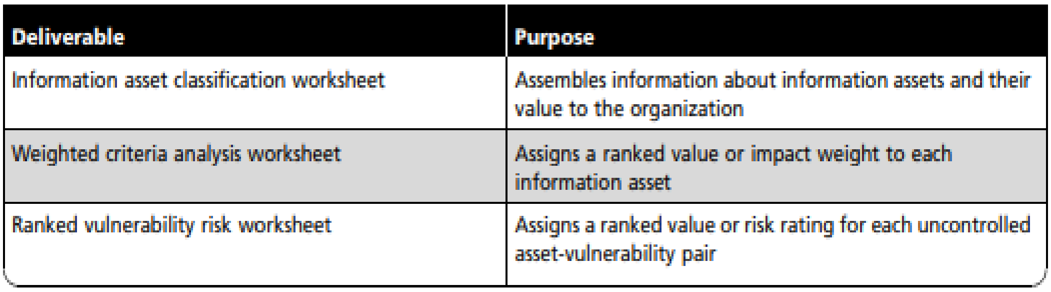
Asset	Asset relative value	Vulnerability	Loss frequency	Loss magnitude
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost 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)	100	Lost orders due to Web server software failure	0.01	1

Table 5-9 **Ranked Vulnerability Risk Worksheet**

The worksheet is organized as follows:

- Asset: List each vulnerable asset.
- Asset relative value: Show the results for the asset from the weighted factor analysis worksheet. This is a number from 1 to 100.
- Vulnerability: List each uncontrolled vulnerability. Some assets might be listed more than once.
- Loss frequency: Estimate the cumulative likelihood that the vulnerability will be successfully exploited by threat agents, as noted in the previous examples. In the table, the number ranges from 0 to 1.0 and corresponds to values of 0 percent to 100 percent.
- Loss magnitude: Calculate the estimated loss magnitude by multiplying the asset's relative value by the loss frequency. In this example, the calculation will yield a number from 0 to 100

The ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk. The following table shows a sample list of worksheets that might be prepared by the information security project team.



Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns a ranked value or risk rating for each uncontrolled asset-vulnerability pair

Table 5-10 **Risk Identification and Assessment Deliverables**

The FAIR Approach to Risk Assessment

The FAIR methodology, which was developed by risk management consultant Jack Jones and promoted through his consulting agency Risk Management Insight and its new parent company

CXO Media, provides a qualitative approach to risk assessment. The major stages in the FAIR analysis consist of 10 steps in four stages:

“Stage 1—Identify scenario components

1. Identify the asset at risk

2. Identify the threat community under consideration

Stage 2—Evaluate loss event frequency (LEF)

3. Estimate the probable threat event frequency (TEF)

4. Estimate the threat capability (TCap)

5. Estimate control strength (CS)

6. Derive vulnerability (Vuln)

7. Derive loss event frequency (LEF) Stage 3—Evaluate probable loss magnitude (PLM)

8. Estimate worst-case loss

9. Estimate probable loss Stage 4—Derive and articulate risk

10. Derive and articulate risk”

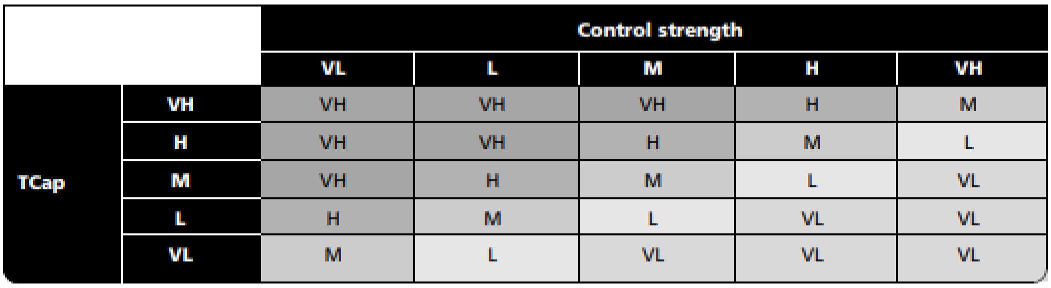
Stage 1 includes the tasks associated with risk identification, and Stages 2–4 include phases recommended under risk assessment. The FAIR approach includes specific range-based calculations to determine vulnerability and loss frequency for a single asset/threat pair as noted in Stage 2 above, as follows:

3. Estimate the probable threat event frequency (TEF) by ranking it on a scale of very low (such as less than 10 percent or once every 10 years) to very high (over 100 times a year).

4. Estimate the threat capability (TCap) by ranking it on a scale of very low (the bottom 2 percent of the overall threat population) to very high (the top 2 percent).

5. Estimate control strength (CS), which is an assessment of current protection capabilities of the organization’s protection system. The CS can be a ranking from very low, which protects only against the bottom 2 percent of the average threat population, to very high, which protects against all but the top 2 percent of the average threat population.

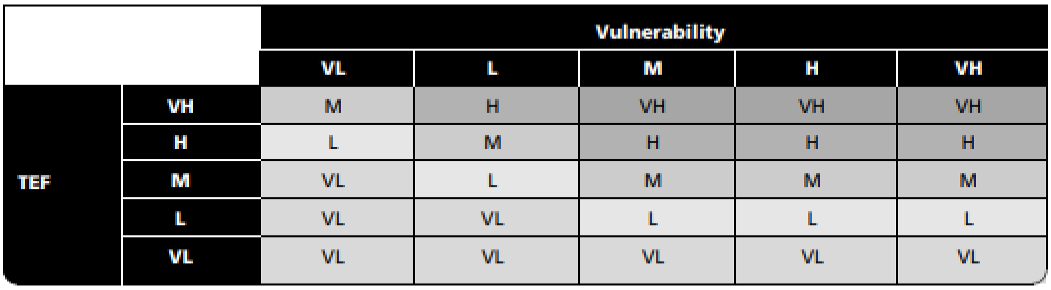
6. Derive vulnerability (Vuln), which is the probability that an asset will be unable to resist the actions of a threat agency. The Vuln value is taken from a table that compares the TCap to the control strength. Rankings are VL (very low), L (low), M (medium), H (high), and VH (very high).



		Control strength				
		VL	L	M	H	VH
TCap	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL

Table 5-11 Vulnerability Assessment Definitions[13]

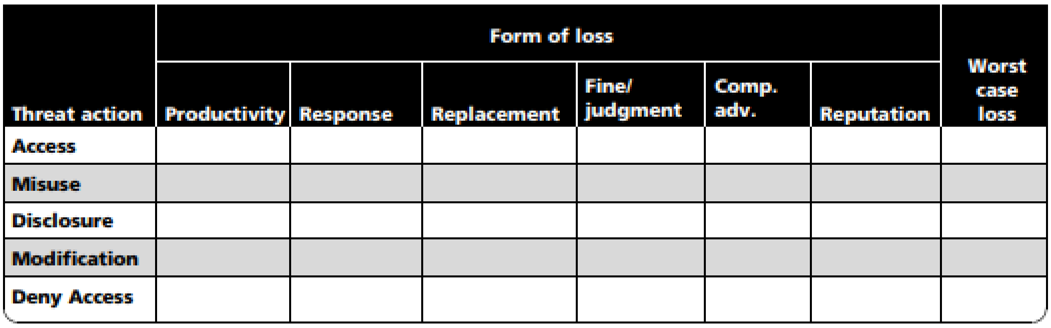
7. Derive loss event frequency (LEF). The following table compares the Vuln values derived from Table 5-11 with the TEF specified during FAIR Step 3. The result is the loss event frequency, which is rated on a scale of very low to very high. This value is used later to determine the overall risk present between the asset and its paired threat. FAIR Stage 3 involves calculating the worst-case loss and most likely (probable) loss of an asset to its paired threat.



		Vulnerability				
		VL	L	M	H	VH
TEF	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL

Table 5-12 Loss Event Frequency Descriptions[14]

8. Estimating the worst-case loss involves determining the magnitude of loss to an asset if a threat becomes a successful attack. Assign values to each cell to represent the comparison between threat actions (rows) and forms of loss (columns). Each column identifies the estimated impact of a form of loss. Some losses represent a direct impact on productivity; others include expenses from managing loss during the incident response process, costs for replacement of equipment or data, and payments to settle legal fines or regulatory judgments.



	Form of loss						
Threat action	Productivity	Response	Replacement	Fine/ judgment	Comp. adv.	Reputation	Worst case loss
Access							
Misuse							
Disclosure							
Modification							
Deny Access							

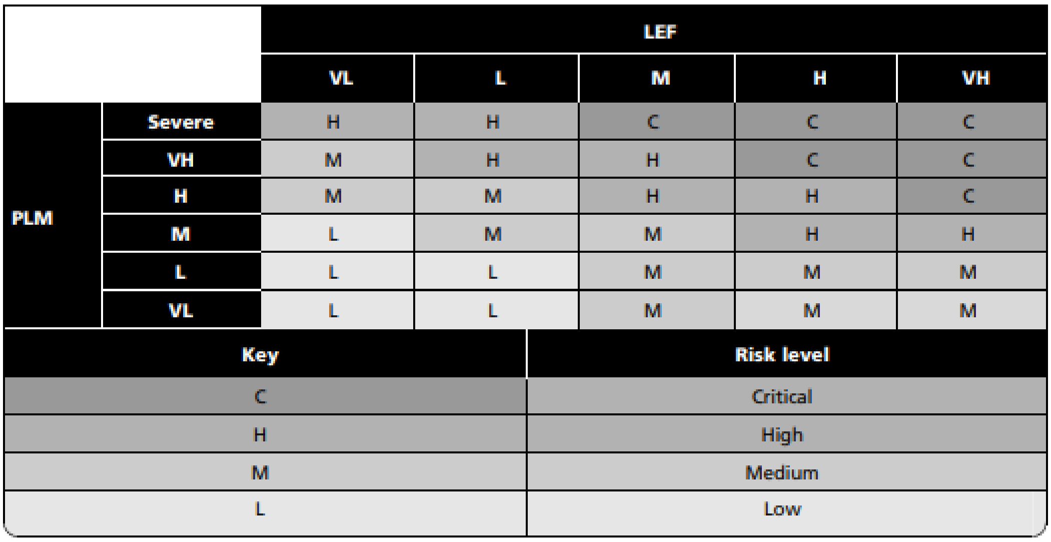
Table 5-13 Worst-Case Loss Table for Information Assets and Threats[15]

Source: FAIR Basic Risk Assessment Guide.

9. Estimate probable loss. Use the same process described in FAIR Step 8, but this time use the most likely outcome instead of the worst-case scenario.

Probable loss magnitude (PLM) is calculated by entering the correct Mid Range magnitude value

The final stage of the FAIR method is to assess the level of risk within an asset/threat pair by comparing the PLM in Stage 3 to the loss frequency from Stage 2. Risk assessments are presented as Low, Medium, High, and Critical. The values are used to create an "outcome assessment of risk.".



		LEF				
		VL	L	M	H	VH
PLM	Severe	H	H	C	C	C
	VH	M	H	H	C	C
	H	M	M	H	H	C
	M	L	M	M	H	H
	L	L	L	M	M	M
	VL	L	L	M	M	M

Key	Risk level
C	Critical
H	High
M	Medium
L	Low

Table 5-16 Risk Assessment Evaluation[19]

Risk Control

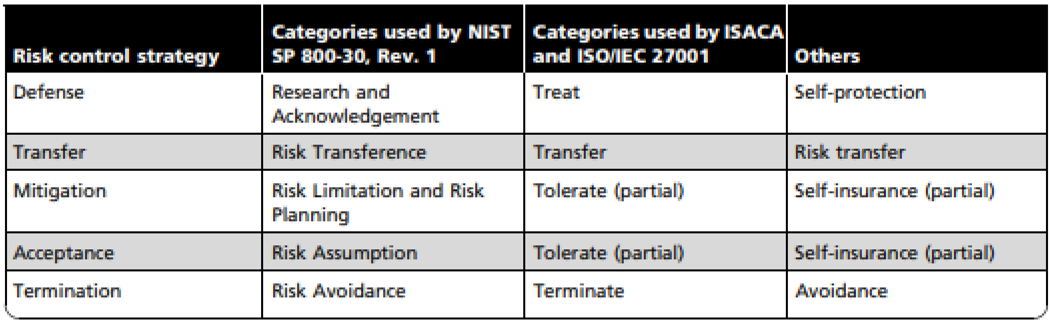
Risk control involves three basic steps:

1. selection of control strategies,
2. justification of these strategies to upper management, and
3. the implementation, monitoring, and ongoing assessment of the adopted controls.

1) Selecting Control Strategies

Once the project team for information security development has created the ranked vulnerability risk worksheet, the team must choose a strategy for controlling each risk that results from these vulnerabilities. The five strategies are

- defense,
- transfer,
- mitigation,
- acceptance, and
- termination



Risk control strategy	Categories used by NIST SP 800-30, Rev. 1	Categories used by ISACA and ISO/IEC 27001	Others
Defense	Research and Acknowledgement	Treat	Self-protection
Transfer	Risk Transference	Transfer	Risk transfer
Mitigation	Risk Limitation and Risk Planning	Tolerate (partial)	Self-insurance (partial)
Acceptance	Risk Assumption	Tolerate (partial)	Self-insurance (partial)
Termination	Risk Avoidance	Terminate	Avoidance

Table 5-17 Summary of Risk Control Strategies

Defense

The defense control strategy attempts to prevent the exploitation of vulnerabilities. This strategy is the preferred approach to controlling risk. It is accomplished by

- ➔ countering threats,
- ➔ removing vulnerabilities from assets,
- ➔ limiting access to assets, and
- ➔ adding protective safeguards.

The defense strategy includes three common methods:

- ➢ Application of policy
- ➢ Education and training
- ➢ Application of technology

Transfer

The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. These controls can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

Mitigation

The mitigation control strategy attempts to reduce the impact of an attack rather than reduce the success of the attack itself. This approach requires the creation of three types of contingency plans: the incident response plan, the disaster recovery plan, and the business continuity plan. Each of these plans relies on the quality of the other plans and depends on the organization's ability to detect an attack and respond to it as quickly as possible. Mitigation begins with the early detection of an attack in progress and a quick, efficient, and effective response.

The most common mitigation plans are contingency plans:

- ➢ Incident response (IR) plan: The actions an organization can and should take while an incident is in progress. The IR plan also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive.

- Disaster recovery (DR) plan: The most common of the mitigation procedures, the DR plan includes all preparations for the recovery process, strategies to limit losses during a disaster, and detailed steps to follow in the aftermath.
- Business continuity (BC) plan: The most strategic and long-term plan of the three. The BC plan includes the steps necessary to ensure the continuation of the organization when the disaster's scope or scale exceeds the ability of the DR plan to restore operations, usually through relocation of critical business functions to an alternate location

Acceptance

The acceptance control strategy is the choice to do nothing more to protect a vulnerability based on the current residual risk and the organization's risk appetite. This strategy may or may not be a conscious business decision. The only recognized valid use of this strategy occurs when the organization has done the following:

- 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

This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure.

Termination

The termination control strategy directs the organization to avoid business activities that introduce uncontrollable risks. For example, if an organization studies the risks of implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs—perhaps developing new channels for product distribution or new partnership opportunities. By terminating the questionable activity, the organization reduces risk exposure.

Selecting a Risk Control Strategy

Risk control involves selecting one of the five risk control strategies for each vulnerability.

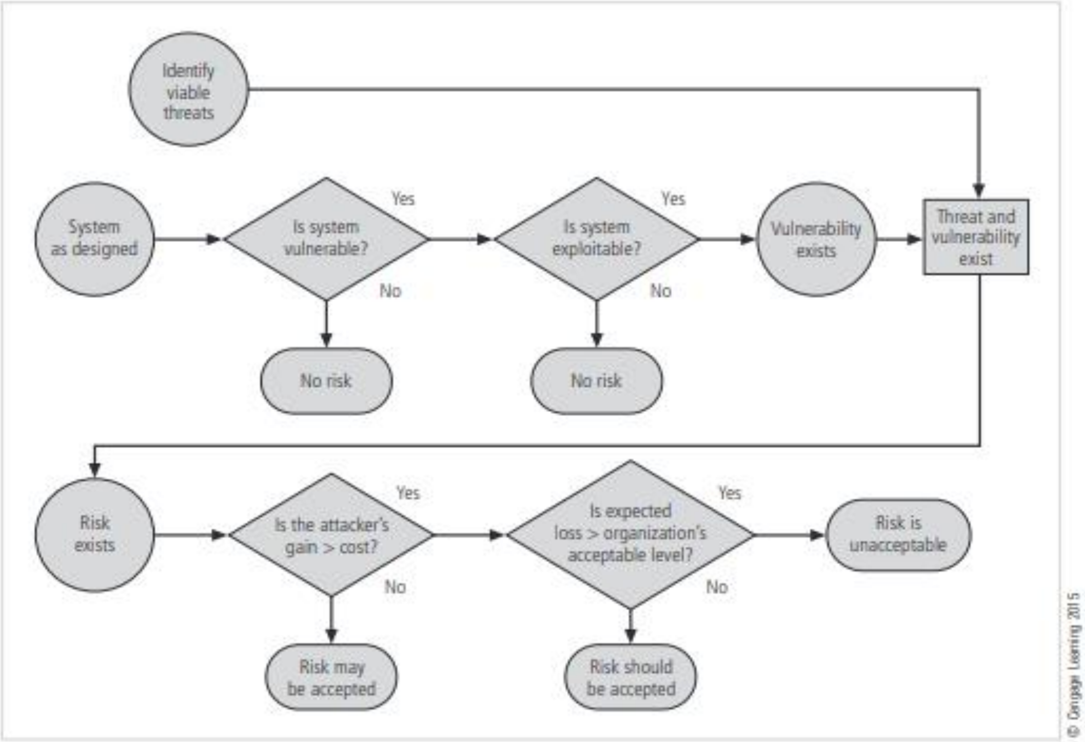


Figure 5-10 Risk handling decision points

After the information system is designed, you query whether the protected system has vulnerabilities that can be exploited. If the answer is yes and a viable threat exists, you begin to examine what the attacker would gain from a successful attack. To determine whether the risk is acceptable, you estimate the expected loss the organization might incur if the risk is exploited.

Rules of thumb for selecting a risk control strategy

- When a vulnerability exists, implement security controls to reduce the likelihood of the vulnerability being exploited.
- When a vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize risk or prevent occurrence.
- When the attacker's cost is less than his or her potential gain, apply protections to increase the attacker's cost. For example, use system controls to limit what a system user can access and do, which significantly reduces an attacker's gain.
- When potential loss is substantial, apply design principles, architectural designs, and other protections to limit the extent of the attack. These protections reduce the potential for loss

By adopting all reasonable and prudent measures given its risk appetite, an organization can implement an effective security strategy.

2) Justifying Controls
Before implementing one of the five control strategies described in the previous section for a specific vulnerability, the organization must explore all consequences of the vulnerability

to the information asset. To justify use of a control, the organization must determine the actual and perceived advantages of the control as opposed to its actual and perceived disadvantages.

Information security staff must prepare effective business justifications for information security expenditures, illustrating the costs, benefits, and other reasons that upper management should make the additional investments. Some investments involve time and effort, but virtually all boil down to some form of economic feasibility, which organizations must consider when implementing information security controls and safeguards.

Organizations must gauge the cost of protecting an asset against the value of that asset. This formal decision making process is called a cost-benefit analysis (CBA) or an economic feasibility study.

The following list contains some of the items that affect the cost of a control or safeguard:

- Cost of development or acquisition of hardware, software, and services
- Training fees for personnel
- Cost of implementation, which includes the costs to install, configure, and test hardware, software, and services
- Service costs, which include vendor fees for maintenance and upgrades
- Cost of maintenance, which includes labor expenses to verify and continually test, maintain, and update

The amount of the benefit is usually determined by valuing the information asset(s) exposed by the vulnerability, determining how much of that value is at risk, and determining how much risk exists for the asset.

The valuation of assets involves estimating real and perceived costs associated with design, development, installation, maintenance, protection, recovery, and defense against loss and litigation. These estimates are calculated for every set of information-bearing systems or information assets.

- **annualized cost of a safeguard (ACS)**

In a cost-benefit analysis, the total cost of a control or safeguard, including all purchase, maintenance, subscription, personnel, and support fees, divided by the total number of expected years of use.

- **annualized loss expectancy (ALE)**

In a cost-benefit analysis, the product of the annualized rate of occurrence and single loss expectancy.

ALE = SLE x ARO

- **annualized rate of occurrence (ARO)**

In a cost-benefit analysis, the expected frequency of an attack, expressed on a per-year basis. cost avoidance The process of preventing the financial impact of an incident by implementing a control.

- **cost-benefit analysis (CBA)**

Also known as an economic feasibility study, the formal assessment and presentation of the economic expenditures needed for a particular security control, contrasted with its projected value to the organization.

- **exposure factor (EF)**

In a cost-benefit analysis, the expected percentage of loss that would occur from a particular attack.

- **single loss expectancy (SLE)**

In a cost-benefit analysis, the calculated value associated with the most likely loss from an attack. The SLE is the product of the asset's value and the exposure factor.

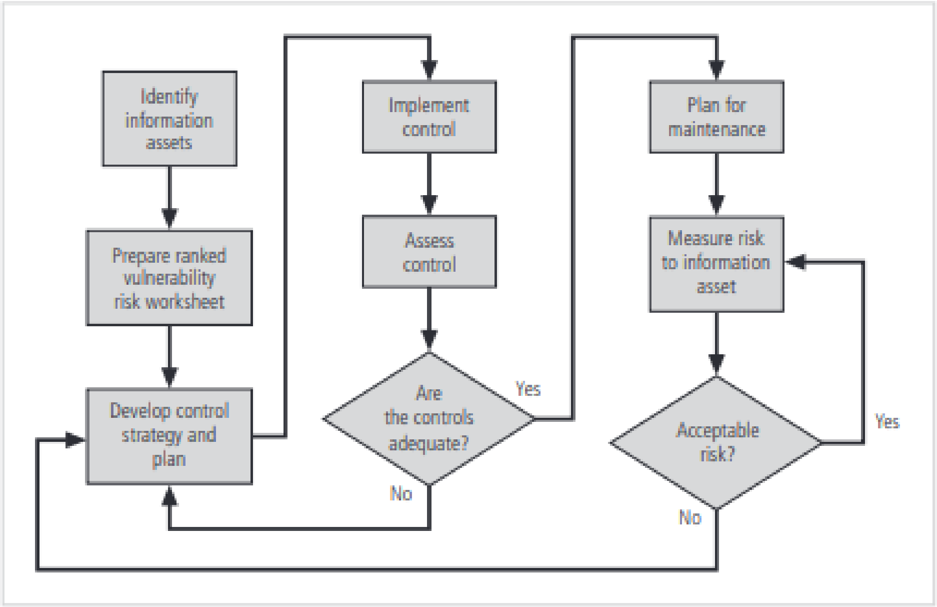
SLE = exposure factor (EF) x asset value (AV)

The Cost-Benefit Analysis (CBA) Formula

In its simplest definition, CBA (or economic feasibility) determines whether a particular control is worth its cost. CBAs may be calculated before a control or safeguard is implemented to determine if the control is worth implementing. CBAs can also be calculated after controls have been functioning for a while. Observation over time adds precision to evaluating the benefits of the safeguard and determining whether it is functioning as intended.

CBA = ALE(prior) - ALE(post) - ACS

3) **Implementation, Monitoring, and Assessment of Risk Controls**
   The selection of a control strategy is not the end of a process. The strategy and its accompanying controls must be implemented and then monitored on an ongoing basis to determine their effectiveness and to accurately calculate the estimated residual risk.


Identify information assets
Prepare ranked vulnerability risk worksheet
Develop control strategy and plan
Implement control
Assess control
Are the controls adequate?
Yes
No
Plan for maintenance
Measure risk to information asset
Acceptable risk?
Yes
No

© Cengage Learning 2015

Figure 5-11 Risk control cycle

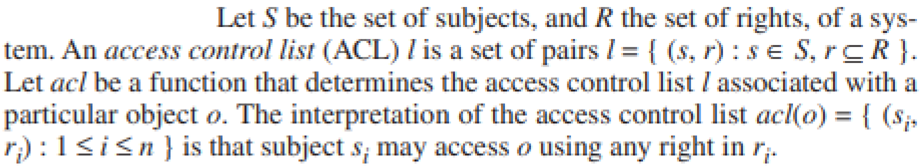
Once controls are implemented, it is crucial to continually examine their benefits to determine when they must be upgraded, supplemented, or replaced.

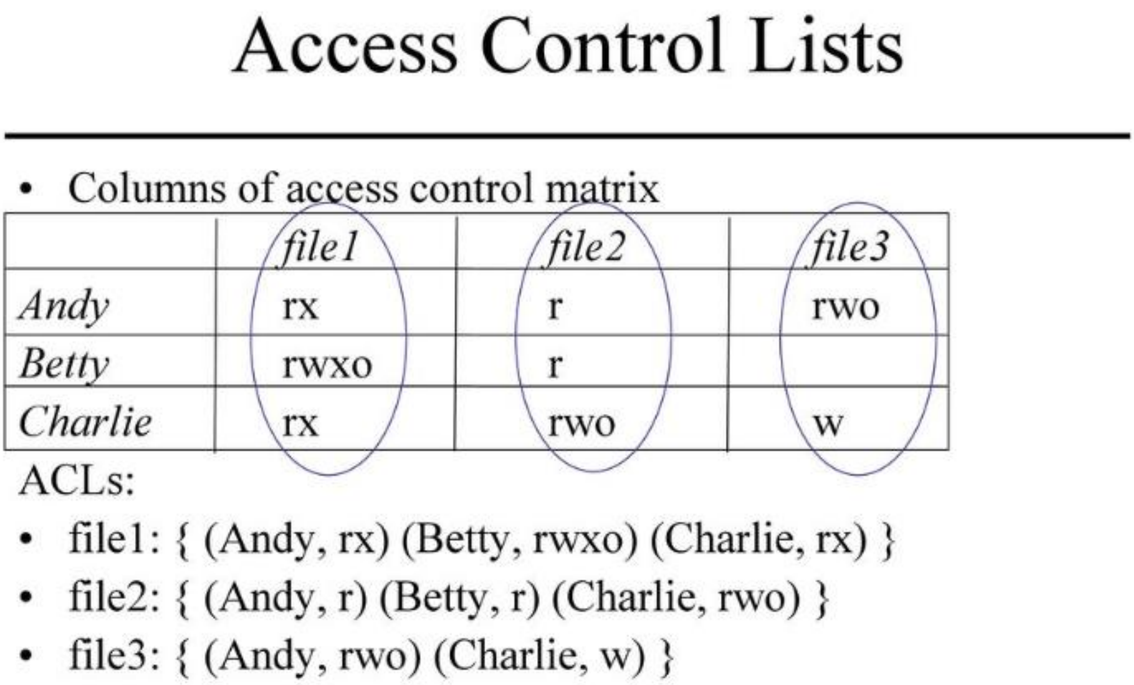
Access Control Mechanisms

- Access Control Lists
- Capability Lists
- Locks and Keys
- Rings-based Access Control
- Propagated Access Control Lists

➢ Access Control Lists

An obvious variant of the access control matrix is to store each column with the object it represents. Thus, each object has associated with it a set of pairs, with each pair containing a subject and a set of rights. The named subject can access the associated object using any of those rights.


Let S be the set of subjects, and R the set of rights, of a system. An *access control list* (ACL) l is a set of pairs $l = \{ (s, r) : s \in S, r \subseteq R \}$. Let *acl* be a function that determines the access control list l associated with a particular object o. The interpretation of the access control list $acl(o) = \{ (s_i, r_i) : 1 \leq i \leq n \}$ is that subject s_i may access o using any right in r_i.



Access Control Lists

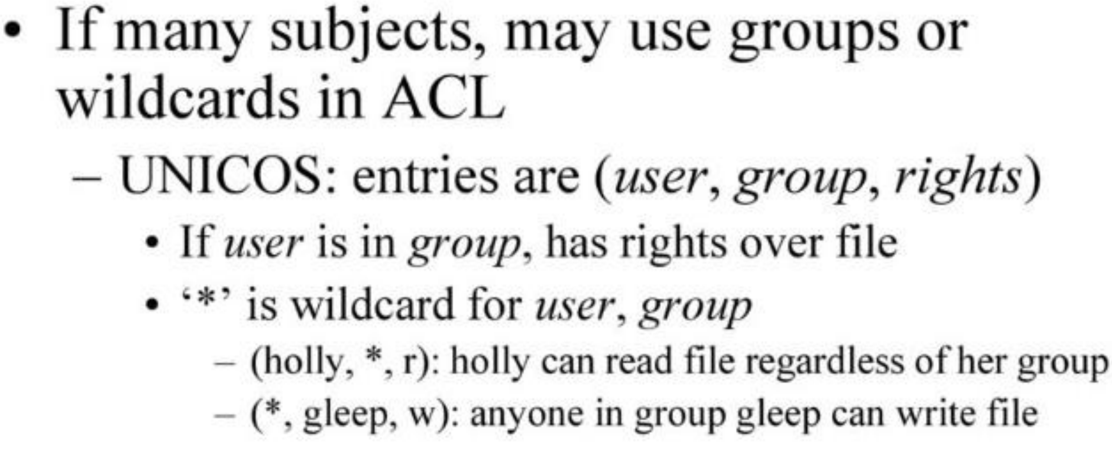
- Columns of access control matrix

	file1	*file2*	*file3*
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rwo	w

ACLs:

- file1: { (Andy, rx) (Betty, rwxo) (Charlie, rx) }
- file2: { (Andy, r) (Betty, r) (Charlie, rwo) }
- file3: { (Andy, rwo) (Charlie, w) }

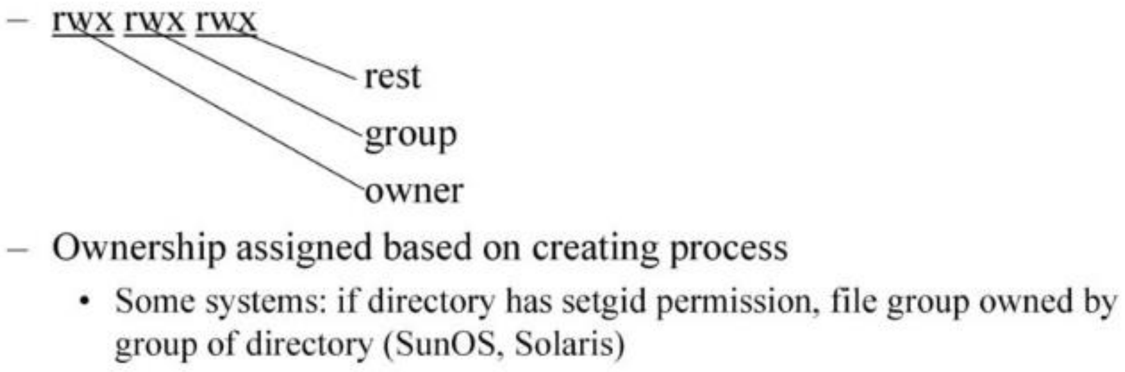
One issue is the matter of default permission. If a subject is not named in the ACL, it has no rights over the associated object. On a system with many subjects, the ACL may be very large. If many subjects have the same right over the file, one could define a "wildcard" to match any unnamed subjects, and give them default rights.



- If many subjects, may use groups or wildcards in ACL
  - UNICOS: entries are (*user*, *group*, *rights*)
    - If *user* is in *group*, has rights over file
    - '*' is wildcard for *user*, *group*
      - (holly, *, r): holly can read file regardless of her group
      - (*, gleep, w): anyone in group gleep can write file

Abbreviations of Access Control Lists

Some systems abbreviate access control lists. The basis for file access control in the UNIX operating system is of this variety. UNIX systems divide the set of users into three classes: the owner of the file, the group owner of the file, and all other users. Each class has a separate set of rights.



- rwx rwx rwx

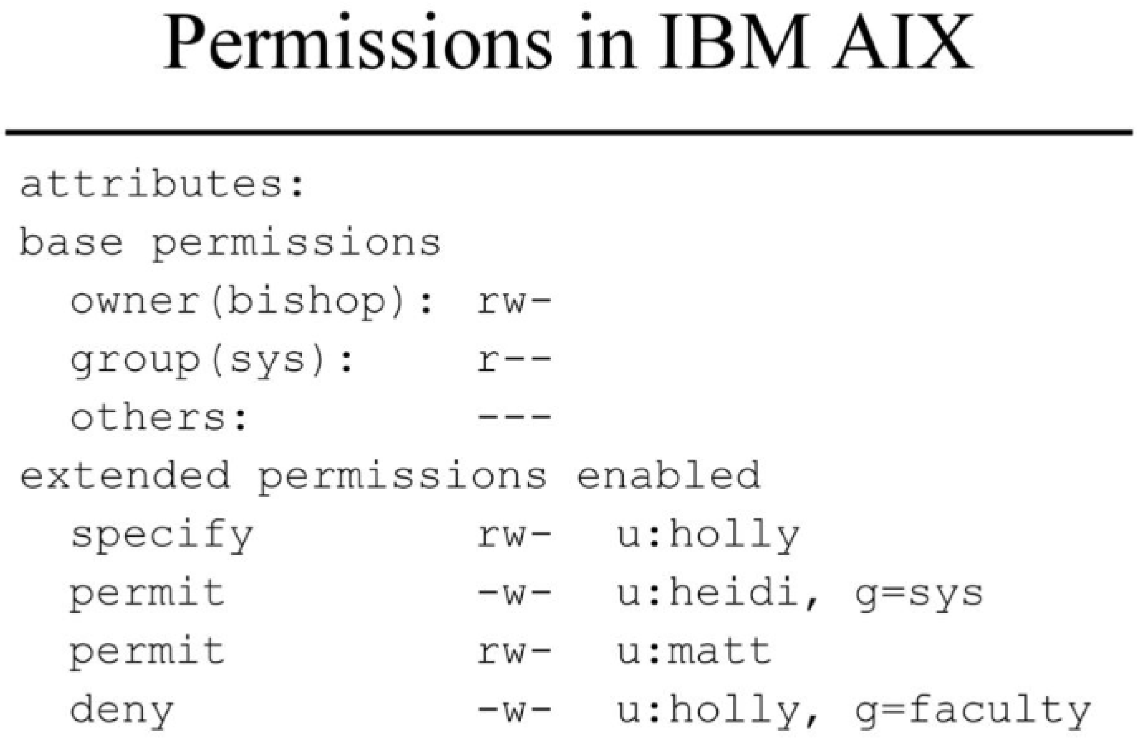
- Ownership assigned based on creating process
  - Some systems: if directory has setgid permission, file group owned by group of directory (SunOS, Solaris)

Abbreviations of access control lists, such as those supported by the UNIX operating system, suffer from a loss of granularity.

Many systems augment abbreviations of ACLs with full-blown ACLs. This scheme uses the abbreviations of ACLs as the default permission controls; the explicit ACL overrides the defaults as needed. The exact method varies.

EXAMPLE:

IBM’s version of the UNIX operating system, called AIX, uses an ACL (called “extended permissions”) to augment the traditional UNIX abbreviations of ACL (called “base permissions”)



Permissions in IBM AIX

```
attributes:
base permissions
  owner(bishop):  rw-
  group(sys):     r--
  others:         ---
extended permissions enabled
  specify         rw-   u:holly
  permit          -w-   u:heidi, g=sys
  permit          rw-   u:matt
  deny            -w-   u:holly, g=faculty
```

Creation and Maintenance of Access Control Lists

Specific implementations of ACLs differ in details. Some of the issues are as follows.

1. Which subjects can modify an object’s ACL?
2. If there is a privileged user (such as root in the UNIX system or administrator in Windows NT), do the ACLs apply to that user?
3. Does the ACL support groups or wildcards (that is, can users be grouped into sets based on a system notion of “group” or on pattern matching)?
4. How are contradictory access control permissions handled? If one entry grants read privileges only and another grants write privileges only, which right does the subject have over the object?
5. If a default setting is allowed, do the ACL permissions modify it, or is the default used only when the subject is not explicitly mentioned in the ACL?

❖ **Which Subjects Can Modify an Object’s ACL?**

When an ACL is created, rights are instantiated. Chief among these rights is the one we will call own. Possessors of the own right can modify the ACL. Creating an object also creates its ACL, with some initial value.

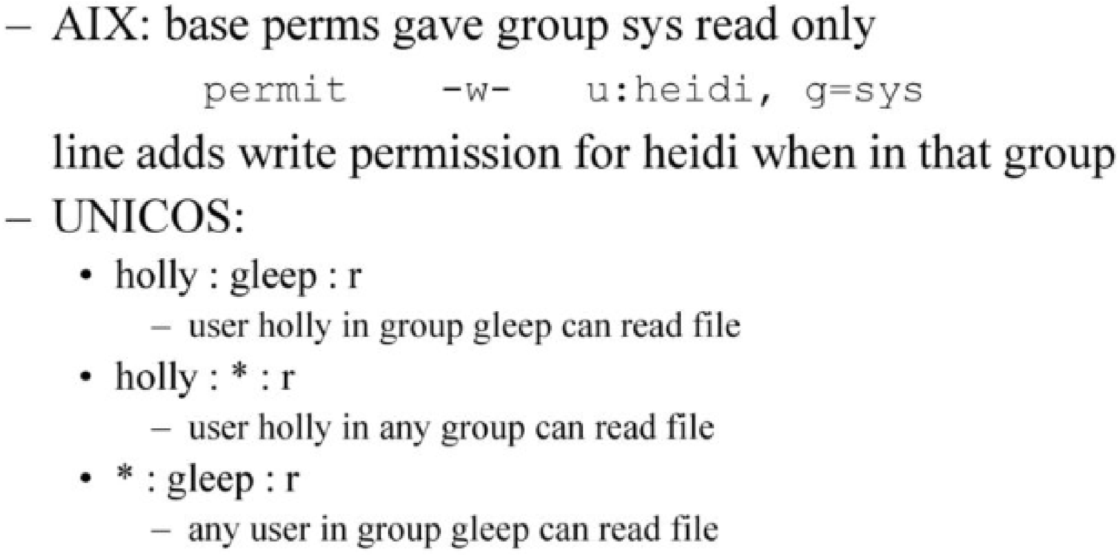
By convention, the subject with own rights is allowed to modify the ACL. However, some systems allow anyone with access to manipulate the rights.

❖ **Do the ACLs Apply to a Privileged User?**

Many systems have users with extra privileges. The two best known are the root superuser on UNIX systems and the administrator user on Windows NT and 2000 systems. Typically, ACLs (or their degenerate forms) are applied in a limited fashion to such users.

❖ **Does the ACL Support Groups and Wildcards?**

In its classic form, ACLs do not support groups or wildcards. In practice, systems support one or the other (or both) to limit the size of the ACL and to make manipulation of the lists easier. A group can either refine the characteristics of the processes to be allowed access or be a synonym for a set of users (the members of the group).



– AIX: base perms gave group sys read only

```
permit    -w-   u:heidi, g=sys
```

line adds write permission for heidi when in that group

– UNICOS:
  - holly : gleep : r
    – user holly in group gleep can read file
  - holly : * : r
    – user holly in any group can read file
  - * : gleep : r
    – any user in group gleep can read file

- **Conflicts**

  A conflict arises when two access control list entries in the same ACL give different permissions to the subject. The system can allow access if any entry would give access, deny access if any entry would deny access, or apply the first entry that matches the subject.

- **ACLs and Default Permissions**

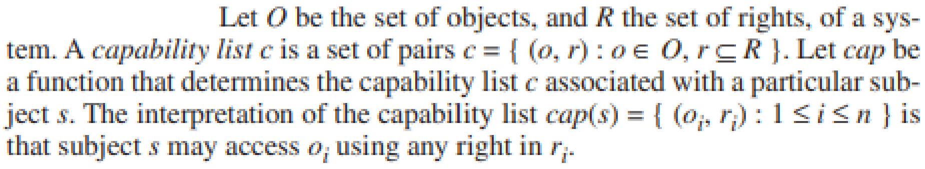
  When ACLs and abbreviations of access control lists or default access rights coexist (as on many UNIX systems), there are two ways to determine access rights. The first is to apply the appropriate ACL entry, if one exists, and to apply the default permissions or abbreviations of access control lists otherwise. The second way is to augment the default permissions or abbreviations of access control lists with those in the appropriate ACL entry.

Revocation of Rights

Revocation, or the prevention of a subject's accessing an object, requires that the subject's rights be deleted from the object's ACL. Preventing a subject from accessing an object is simple. The entry for the subject is deleted from the object's ACL. If only specific rights are to be deleted, they are removed from the relevant subject's entry in the ACL. If ownership does not control the giving of rights, revocation is more complex.

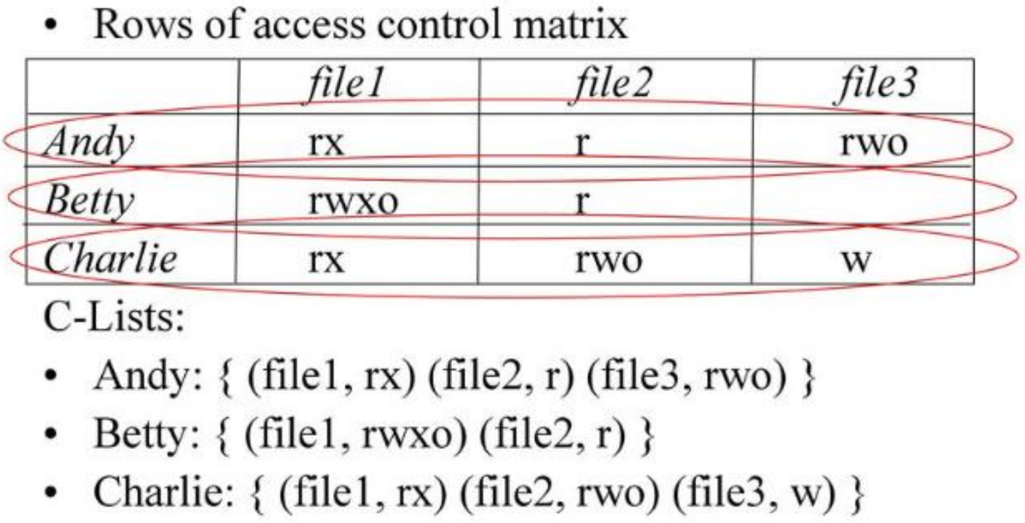
Capabilities

Conceptually, a capability is like the row of an access control matrix. Each subject has associated with it a set of pairs, with each pair containing an object and a set of rights. The subject associated with this list can access the named object in any of the ways indicated by the named rights.



Let O be the set of objects, and R the set of rights, of a system. A *capability list* c is a set of pairs $c = \{ (o, r) : o \in O, r \subseteq R \}$. Let *cap* be a function that determines the capability list c associated with a particular subject s. The interpretation of the capability list $cap(s) = \{ (o_i, r_i) : 1 \leq i \leq n \}$ is that subject s may access o_i using any right in r_i.

"Capability list" is abbreviated as C-List.



- Rows of access control matrix

	file1	*file2*	*file3*
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rwo	w

C-Lists:

- Andy: { (file1, rx) (file2, r) (file3, rwo) }
- Betty: { (file1, rwxo) (file2, r) }
- Charlie: { (file1, rx) (file2, rwo) (file3, w) }

Implementation of Capabilities

Three mechanisms are used to protect capabilities: tags, protected memory, and cryptography. A tagged architecture has a set of bits associated with each hardware word. The tag has two states: set and unset. If the tag is set, an ordinary process can read but not modify the word. If the tag is unset, an ordinary process can read and modify the word. Further, an ordinary process cannot change the state of the tag; the processor must be in a privileged mode to do so.

More common is to use the protection bits associated with paging or segmentation. All capabilities are stored in a page (segment) that the process can read but not alter. A third alternative is to use cryptography. The goal of tags and memory protection is to prevent the capabilities from being altered. This is akin to integrity checking.

Cryptographic checksums are another mechanism for checking the integrity of information. Each capability has a cryptographic checksum associated with it, and the checksum is digitally enciphered using a cryptosystem whose key is known to the operating system.

Copying and Amplifying Capabilities

The ability to copy capabilities implies the ability to give rights. To prevent processes from indiscriminately giving away rights, a copy flag is associated with capabilities. A process cannot copy a capability to another process unless the copy flag is set. If the process does copy the capability, the copy flag may be turned off.

Amplification is the increasing of privileges. The idea of modular programming, and especially of abstract data types, requires that the rights a process has over an object be amplified.

Revocation of Rights

In a capability system, revoking access to an object requires that all the capabilities granting access to that object be revoked. Conceptually, each process could be checked, and the capabilities deleted.

The simplest mechanism is indirection. Define one or more global object tables. In this scheme, each object has a corresponding entry in a table. Capabilities do not name the object directly; they name the entry in the table corresponding to the object.

This scheme has several advantages.

- First, to revoke capabilities, the entry in the global object table is invalidated. Then any references will obtain an invalid table entry and will be rejected.
- Second, if only some of the capabilities are to be revoked, the object can have multiple entries, each corresponding to a different set of rights or a different group of users.

An alternative revocation mechanism uses abstract data type managers. Included with each abstract data type is a revocation procedure. When access is to be revoked, the type manager simply disallows further accesses by the subject whose rights are being revoked.

Locks and Keys

The locks and keys technique combines features of access control lists and capabilities. A piece of information (the lock) is associated with the object and a second piece of information (the key) is associated with those subjects authorized to access the object and the manner in which they are allowed to access the object. When a subject tries to access an object, the subject's set of keys is checked. If the subject has a key corresponding to any of the object's locks, access of the appropriate type is granted.

The difference between locks and keys and the other access control mechanisms is the dynamic nature of the former. An access control list is static in the sense that all changes to it are manual; a user or process must interact with the list to make the change. Locks and keys, on the other hand, may change in response to system constraints, general instructions about how entries are to be added, and any factors other than a manual change.

Type Checking

Type checking restricts access on the basis of the types of the subject and object. It is a form of locks and keys access control, the pieces of information being the type. Systems use type checking in areas other than security.