Chapter 7 Risk Management: Identifying and Assessing Risk

## Chapter Overview

Chapter 7 defines risk management and its role in the organization and allows the reader to begin using risk management techniques to identify and prioritize risk factors for information assets. The risk management model presented here allows the assessment of risk based on the likelihood of adverse events and the effects on information assets when events occur. The chapter concludes with a brief discussion on how to document the results of risk identification.

## Chapter Objectives

When you complete this chapter, you will be able to:

* Define risk management and its role in the organization
* Begin using risk management techniques to identify and prioritize risk factors for information assets
* Assess risk based on the likelihood of adverse events and the effects on information assets when events occur
* Begin to document the results of risk identification

## Set-up Notes

This chapter could be completed in a single class session, if there is sufficient time to cover the material. Unless the students have not had the opportunity to read the material in advance (in some settings, the textbooks are not made available until the first class meeting), it may be prudent to have a general discussion of the topic, with detailed lecture to follow at the next class meeting. The subject matter can be covered in 1.25 to 2.5 hours.

## Lecture Notes and Teaching Tips with Quick Quizzes

Introduction

Information security departments are created primarily to manage IT risk.

Managing risk is one of the key responsibilities of every manager within the organization.

In any well-developed risk management program, two formal processes are at work:

* risk identification and assessment
* risk control

Risk Management

 “If you know the enemy and know yourself, you need not fear the result of a hundred battles.

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

“If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu

Knowing Ourselves

This means identifying, examining and understanding the information and how it is processed, stored, and transmitted.

Armed with this knowledge, they can then initiate an in-depth risk management program.

Risk management is a process, which means the safeguards and controls that are devised and implemented are not install-and-forget devices.

Knowing the Enemy

This means identifying, examining, and understanding the threats facing the organization’s information assets.

Managers must be prepared to fully identify those threats that pose risks to the organization and the security of its information assets.

Risk management is the process of assessing the risks to an organization’s information and determining how those risks can be controlled or mitigated.

Accountability for Risk Management

All communities of interest must work together to:

* Evaluating the risk controls
* Determining which control options are cost-effective
* Acquiring or installing the appropriate controls
* Overseeing processes to ensure that the controls remain effective
* Identifying risks, which includes:
* Inventory information assets
* Classifying/organizing assets
* Assigning information asset value
* Identifying threats to the cataloged assets
* Pinpointing vulnerable assets by tying specific threats to specific assets
* Assessing risks, which includes:
* Determining likelihood of attacks on vulnerable systems by specific threats
* Assessing relative risk facing information assets, so risk management and control activities can prioritize
* Calculating the risks to which assets are exposed in their current setting
* Reviewing controls for identified vulnerabilities and says to control the risks that the assets face
* Documenting the findings of risk identification and assessment

Summarizing the findings, which involves stating the conclusions of the analysis stage of risk assessment in preparation for moving into the stage of controlling risk by exploring methods to mitigate risk

### Quick Quiz

1. What are the two formal processes within a risk management program? **ANSWER:** Risk identification and assessment and risk control.
2. What is risk management? **ANSWER:** Risk management is a process, which means the safeguards and controls that are devised and implemented are not install-and-forget devices.

Risk Identification

Risk identification begins with the process of self-examination.

At this stage, managers identify the organization’s information assets, classify them into useful groups, and prioritize them by their overall importance.

Creating an Inventory of Information Assets

The risk identification process begins with the identification of information assets, including people, procedures, data and information, software, hardware, and networking elements.

This step should be done without pre-judging the value of each asset; values will be assigned later in the process.





Identifying Hardware, Software, and Network Assets

Whether automated or manual, the inventory process requires a certain amount of planning.

Most importantly, you must determine which attributes of each of these information assets should be tracked.

That determination will depend on the needs of the organization and its risk management efforts, as well as the preferences and needs of the information security and information technology communities.

When deciding which attributes to track for each information asset, consider the following list of potential attributes:

* Name
* IP address
* MAC address
* Asset type
* Serial number
* Manufacturer name
* Manufacturer’s model or part number
* Software version, update revision, or FCO number
* Physical location
* Logical location
* Controlling entity

Identifying People, Procedures, and Data Assets

Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the necessary knowledge, experience, and judgment.

As these assets are identified, they should be recorded via a reliable data-handling process like the one used for hardware and software.

* People
* Position name/number/ID
* Supervisor name/number/ID
* Security clearance level
* Special skills
* Procedures
* Description
* Intended purpose
* Software/hardware/networking elements to which it is tied
* Location where it is stored for reference
* Location where it is stored for update purposes
* Data
* Classification
* Owner/creator/manager
* Size of data structure
* Data structure used
* Online or offline
* Location
* Backup procedures

Classifying and Categorizing Assets

Once the initial inventory is assembled, you must determine whether its asset categories are meaningful to the organization’s risk management program.

The inventory should also reflect the sensitivity and security priority assigned to each information asset.

A classification scheme should be developed that categorizes these information assets based on their sensitivity and security needs, i.e. confidential, internal, and public.

Each of these classification categories designates the level of protection needed for a particular information asset.

Some asset types, such as personnel, may require an alternative classification scheme that would identify the information security processes used by the asset type.

Classification categories must be comprehensive and mutually exclusive.

Assessing Values for Information Assets

As each information asset is identified, categorized, and classified, a relative value must also be assigned to it.

Relative values are comparative judgments made to ensure that the most valuable information assets are given the highest priority when managing risk.

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 highest profitability?

Which information asset is the most expensive to replace?

Which information asset is the most expensive to protect?

Which information asset’s loss or compromise would be the most embarrassing or cause the greatest liability?



Listing Assets in Order of Importance

The final step in the risk identification process is to list the assets in order of importance.

This goal can be achieved by using a weighted factor analysis worksheet.

Data Classification Model

Corporate and military organizations use a variety of classification schemes.

Data owners must classify the information assets for which they are responsible.

Data owners must review these classifications periodically to ensure that the data are still classified correctly and the access controls are in place.

For Example:

* Public
* For official use only
* Sensitive
* Classified

As you might expect, the U.S. military classification scheme relies on a more complex categorization system than the schemes of most corporations.

For most information, the U.S. military uses a five-level classification scheme as defined in Executive Order 12958:

* Unclassified Data:
* Sensitive But Unclassified (SBU) Data:
* Confidential Data:
* Secret Data:
* Top Secret Data:



Security Clearances

The other part of the data classification scheme is the personnel security clearance structure, in which each user of an information asset is assigned an authorization level that indicates the level of information classification he or she can access.

Most organizations have developed a set of roles and corresponding security clearances, so that individuals are assigned authorization levels that correlate with the classifications of the of information assets.

Beyond a simple reliance on the security clearance of the individual is the need-to-know principle.

Regardless of one’s security clearance, an individual is not allowed to view data simply because it falls within that individual’s level of clearance.

That is, after an individual is granted a security clearance but before he or she is allowed access to a specific set of data, that person must also meet the need-to-know requirement.

Management of the Classified Information Asset

Managing an information asset includes considering the storage, distribution, portability, and destruction of that information asset.

An information asset that has a classification designation other than unclassified or public must be clearly marked as such.

Classified documents must be available only to authorized individuals - locking cabinets, safes, etc.

To maintain the confidentiality of classified documents, managers can implement a clean desk policy.

When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving.

Military Data Classification Cover Sheets

Threat Identification

Any organization typically faces a wide variety of threats.

If you assume that every threat can and will attack every information asset, then the project scope becomes too complex.

To make the process less unwieldy, each step in the threat identification and vulnerability identification processes is managed separately and then coordinated at the end.

Identify and Prioritize Threats and Threat Agents

Each of these threats presents a unique challenge to information security and must be handled with specific controls that directly address the particular threat and the threat agent’s attack strategy.

Before threats can be assessed in the risk identification process, however, each threat must be further examined to determine its potential to affect the targeted information asset.

In general, this process is referred to as a threat assessment.



Vulnerability Assessment

Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat.

This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization.

Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset.

At the end of the risk identification process, a list of assets and their vulnerabilities has been developed.

This list serves as the starting point for the next step in the risk management process—risk assessment.

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

### Quick Quiz

1. What are the important elements of the risk identification process? **ANSWER:** The risk identification process begins with the identification of information assets, including people, procedures, data and information, software, hardware, and networking elements.

Risk Assessment

Risk is the likelihood of the occurrence of a vulnerability

Multiplied by

The value of the information asset

Minus

The percentage of risk mitigated by current controls

Plus

The uncertainty of current knowledge of the vulnerability



Likelihood

Likelihood is the overall rating—a numerical value on a defined scale (.1 – 1.0)—of the probability that a specific vulnerability will be exploited.

Using the information documented during the risk identification process, you can assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc.

Assessing Potential Loss

To be effective, the values must be assigned by asking:

* Which threats present a danger to this 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 threats would require the greatest expenditure to prevent?
* Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

Percentage of Risk Mitigated by Current Controls

If a vulnerability is fully managed by an existing control, it can be set aside.

If it is partially controlled, estimate what percentage of the vulnerability has been controlled.

Uncertainty

It is not possible to know everything about every vulnerability.

The degree to which a current control can reduce risk is also subject to estimation error. A factor that accounts for uncertainty must always be added to the equations; it consists of an estimate made by the manager using good judgment and experience.

Risk Determination

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.

Asset A has a value of 50 and has one vulnerability, which has a likelihood of 1.0 with no current controls. Your assumptions/data are 90% accurate.

Asset B has a value of 100 and has two vulnerabilities: Vul #2 has a likelihood of 0.5 with a current control that addresses 50% of its risk; vul # 3 has a likelihood of 0.1 with no current controls. Your assumptions and data are 80% accurate.

The resulting ranked list of risk ratings for the three vulnerabilities is as follows:

* Asset A: Vulnerability 1 rated as 55 = (50 × 1.0) – 0% + 10%.
* Asset B: Vulnerability 2 rated as 35 = (100 × 0.5) – 50% + 20%.
* Asset B: Vulnerability 3 rated as 12 = (100 × 0.1) – 0 % + 20%.

Identify Possible Controls

For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas.

Three general categories of controls exist: policies, programs, and technical controls.

Access Controls

Access controls specifically address admission of a user into a trusted area of the organization.

These areas can include information systems, physically restricted areas such as computer rooms, and even the organization in its entirety.

Access controls usually consist of a combination of policies, programs, and technologies.

Types of Access Controls

Mandatory Access Controls (MACs) are required and are structured and coordinated with a data classification scheme.

When MACs are implemented, users and data owners have limited control over their access to information resources.

MACs use a data classification scheme that rates each collection of information.

Types of Access Controls

In lattice-based access controls, users are assigned a matrix of authorizations for particular areas of access.

The matrix contains subjects and objects, and the boundaries associated with each subject/object pair are clearly demarcated.

With this type of control, the column of attributes associated with a particular object is called an access control list (ACL).

The row of attributes associated with a particular subject is a capabilities table.

Nondiscretionary controls are determined by a central authority in the organization and can be based on roles—called role-based controls—or on a specified set of tasks—called task-based controls.

Task-based controls can, in turn, be based on lists maintained on subjects or objects.

Role-based controls are tied to the role that a particular user performs in an organization, whereas task-based controls are tied to a particular assignment or responsibility.

Discretionary Access Controls (DACs) are implemented at the discretion or option of the data user.

The ability to share resources in a peer-to-peer configuration allows users to control and possibly provide access to information or resources at their disposal.

The users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources.



### Quick Quiz

1. What do access controls specifically address? **ANSWER:** Access controls specifically address admission of a user into a trusted area of the organization.

Documenting the Results of Risk Assessment

The goal of the risk management process so far has been to identify information assets and their vulnerabilities and to rank them according to the need for protection.

In preparing this list, a wealth of factual information about the assets and the threats they face is collected.

Also, information about the controls that are already in place is collected.

The final summarized document is the ranked vulnerability risk worksheet.



Ranked Vulnerability Risk Worksheet

Documenting the Results of Risk Assessment

* What should the documentation package look like?
* What are the deliverables from this stage of the risk management project?

The risk identification process should designate what function the reports serve, who is responsible for preparing them, and who reviews them.

### Quick Quiz

1. What is the goal of the risk management process? **ANSWER:** The goal of the risk management process so far has been to identify information assets and their vulnerabilities and to rank them according to the need for protection.

## Key Terms

access control list (ACL)

capabilities table

dumpster diving

lattice-based access control

need-to-know

Programs

Risk management

role-based controls

task-based controls

threat identification

U.S. military classification scheme