Information Security Management

Chapter 7
Risk Management:
Identifying and Assessing Risk

Webster University
Scott Granneman

“Once we know our weaknesses,
they cease to do us any harm.”

-- G. C. (Georg Christoph) Lichtenberg
(1742–1799),
German Physicist & Philosopher

Upon completion of this chapter,
you should be able to:

Define risk management
& its role in the organization

Begin using risk management techniques
to identify & prioritize
risk factors for information assets

Assess risk based on
the likelihood of adverse events
& the effects on information assets
when events occur

Begin to document
the results of risk identification

InfoSec 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,
2 formal processes are at work:

1. Risk identification & assessment
2. Risk control

Knowing ourselves means
identifying, examining & understanding
information & how it is
processed, stored, & transmitted

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

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

Knowing the enemy means
identifying, examining, & understanding
the threats facing
the organization's information assets

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

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

All communities of interest must work together on risk management:

✓ Evaluating risk controls

✓ Determining which control options are cost-effective

✓ Acquiring or installing appropriate controls

✓ Overseeing processes to ensure that controls remain effective

✓ Identifying risks

✓ Assessing risks

✓ Summarizing findings

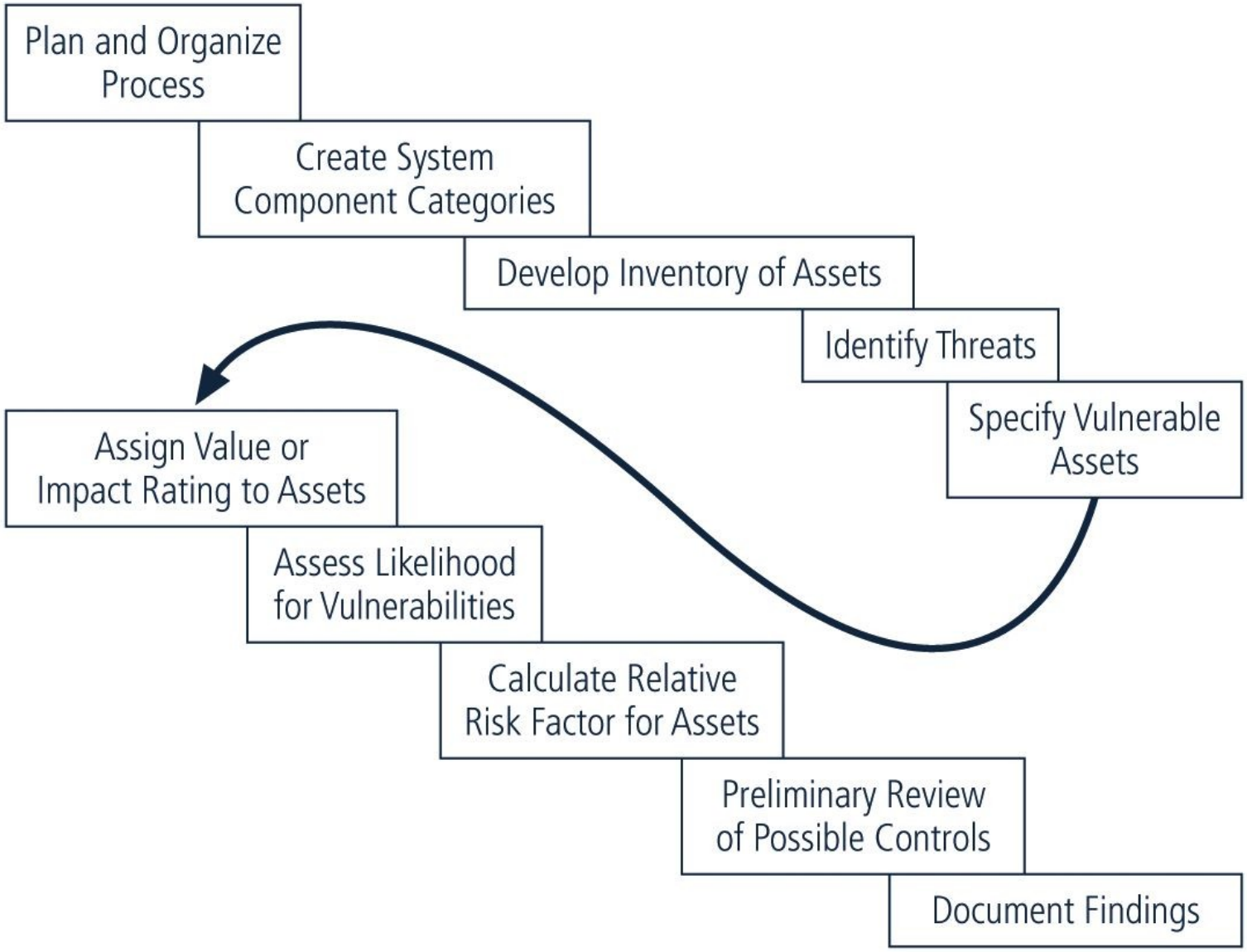

FIGURE 7-1 Risk Identification Process

Risk identification begins
with the process of self-examination

Managers identify
the organization's information assets,
classify them into useful groups,
& prioritize them
by their overall importance

Creating an inventory of information assets

Identify information assets, including:

- ✓ people
- ✓ procedures
- ✓ data & information
- ✓ software
- ✓ hardware
- ✓ networking elements

Should be done
without pre-judging value of each asset,
which will be assigned later in the process

TABLE 7-1 Organizational Assets Used in Systems

IT system components	Risk management components	
People	People inside an organization	Trusted employees Other staff
	People outside an organization	People at organizations we trust Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking components	Intranet components Internet or Extranet components

Identifying Hardware, Software,
& Network Assets

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

Determine which attributes
of each of these information assets
should be tracked

Will depend on the needs
of the organization
& its risk management efforts

When deciding which attributes
to track for each information asset,
consider the following 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,
& Data Assets

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

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

Suggested Attributes for People & Procedure Assets

People

- ✓ Position name &/or number &/or ID
- ✓ Supervisor name &/or number &/or ID
- ✓ Security clearance level
- ✓ Special skills

Procedures

- ✓ Description
- ✓ Intended purpose
- ✓ Software, hardware, & networking elements to which it is tied
- ✓ Storage location

Suggested Attributes for Data Assets

- ✓ Classification
- ✓ Owner/creator/manager
- ✓ Size of data structure
- ✓ Data structure used
- ✓ Online or offline
- ✓ Location
- ✓ Backup procedures

Classifying & Categorizing Assets

Once initial inventory is assembled, determine whether its asset categories are meaningful

Inventory should also reflect sensitivity & security priority assigned to each information asset

A classification scheme categorizes these information assets based on their sensitivity & security needs

more ... →

Each of these categories
designates 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 clearance needed to use the asset type

Classification categories
must be
comprehensive & mutually exclusive

As each information asset
is identified, categorized, & classified,
assign a relative value

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

Which information asset …

… is the most critical
to the organization’s success?

… generates the most revenue?

… generates the highest profitability?

… is the most expensive to replace?

… is the most expensive to protect?

… would be the most embarrassing
or cause the greatest liability
if it was lost or compromised?

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-maill (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 7-2 Sample Asset Classification Worksheet

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

Can be achieved by using
a weighted factor analysis worksheet

TABLE 7-2 Example Weighted Factor Analysis Worksheet

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading 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

EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Data owners
must classify information assets
for which they are responsible
& review the classifications periodically

Example:

✓ Public
✓ For official use only
✓ Sensitive
✓ Classified

U.S. military classification scheme
relies on
a more complex categorization system
than the schemes of most corporations

Uses a 5-level classification scheme
as defined in Executive Order 12958:

✓ Unclassified Data
✓ Sensitive But Unclassified (SBU) Data
✓ Confidential Data
✓ Secret Data
✓ Top Secret Data

Personnel Security Clearance Structure
is a complement
to data classification scheme

Each user of information asset
is assigned an authorization level
that indicates
level of information classification
he or she can access

Most organizations have developed
a set of roles
& corresponding security clearances

Individuals are assigned into groups
that correlate
with classifications of the information assets
they need for their work

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

Before he or she
is allowed access to a specific set of data,
that person must also
need-to-know the data as well

Managing an information asset
includes considering the

storage,
distribution,
portability,
& destruction

of that information asset

An information asset
that has a classification designation
other than unclassified or public:

✓ Must be clearly marked as such

✓ Must be available
only to authorized individuals

To maintain 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

FIGURE 7-3 Military Data Classification Cover Sheets

Threat Assessment

Any organization typically faces
a wide variety of threats

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

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

Each threat presents
a unique challenge to InfoSec

Must be handled with specific controls
that directly address particular threat
& threat agent's attack strategy

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

In general, referred to as
threat assessment

TABLE 7-3 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/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Source: ©2003 ACM, Inc., Included here by permission.

Weighted Ranks of Threats to Information Security					
	Threat	Mean	Standard Deviation	Weight	Weighted Rank
1.	Deliberate software attacks	3.99	1.03	546	**2178.3**
2.	Technical software failures or errors	3.16	1.13	358	**1129.9**
3.	Acts of human error or failure	3.15	1.11	350	**1101.0**
4.	Deliberate acts of espionage or trespass	3.22	1.37	324	**1043.6**
5.	Deliberate acts of sabotage or vandalism	3.15	1.37	306	**962.6**
6.	Technical hardware failures or errors	3.00	1.18	314	**942.0**
7.	Deliberate acts of theft	3.07	1.30	226	**694.5**
8.	Forces of nature	2.80	1.09	218	**610.9**
9.	Compromises to intellectual property	2.72	1.21	182	**494.8**
10.	Quality–of-service deviations from service providers	2.65	1.06	164	**433.9**
11.	Technological obsolescence	2.71	1.11	158	**427.9**
12.	Deliberate acts of information extortion	2.45	1.42	92	**225.2**

Weighted Ranking of Threat-Driven Expenditures

Top Threat-Driven Expenses	Rating
Deliberate software attacks	12.7
Acts of human error or failure	7.6
Technical software failures or errors	7.0
Technical hardware failures or errors	6.0
Quality-of-service deviations from service providers	4.9
Deliberate acts of espionage or trespass	4.7
Deliberate acts of theft	4.1
Deliberate acts of sabotage or vandalism	4.0
Technological obsolescence	3.3
Forces of nature	3.0
Compromises to intellectual property	2.2
Deliberate acts of information extortion	1.0

Vulnerability Assessment

Once you have identified
the information assets of the organization
& documented some threat assessment criteria,
you need to review
every information asset for each threat

Leads to creation of list of vulnerabilities
that remain potential risks to organization

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

more … →

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

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

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

Risk is

the likelihood of the occurrence of a vulnerability

Multiplied by

the value of the information asset

Minus

the % of risk mitigated by current controls

Plus

the uncertainty of current knowledge
of the vulnerability

Likelihood is the overall rating
– often a numerical value
on a defined scale (such as 0.1-1.0) –
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.

To be effective, the likelihood 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?

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

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

Uncertainty is an estimate
made by the manager
using judgment & experience

Risk Determination Example #1

Asset A has a value of 50
& has one vulnerability,
which has a likelihood of 1.0
with no current controls

Your assumptions & data are 90% accurate

Resulting risk rating for Asset A:
Vulnerability 1 rated as 55
= (50 × 1.0) – 0% + 10%

Risk Determination Example #2

Asset B has a value of 100
& has 2 vulnerabilities

Vulnerability #2 has a likelihood of 0.5
with a current control
that addresses 50% of its risk

Vulnerability # 3 has a likelihood of 0.1
with no current controls

Your assumptions & data are 80% accurate

Asset B: Vulnerability 2 rated as 35
= (100 × 0.5) – 50% + 20%
Asset B: Vulnerability 3 rated as 12
= (100 × 0.1) – 0 % + 20%

Resulting ranked list of risk ratings for the 3 vulnerabilities is as follows:

Asset A: Vulnerability 1 rated as 55
$= (50 \times 1.0) - 0\% + 10\%$

Asset B: Vulnerability 2 rated as 35
$= (100 \times 0.5) - 50\% + 20\%$

Asset B: Vulnerability 3 rated as 12
$= (100 \times 0.1) - 0\ \% + 20\%$

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

3 general categories of controls exist:

- ✓ Policies
- ✓ Programs
- ✓ Technical 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,
& even the organization in its entirety

Access controls usually consist
of a combination
of policies, programs, & technologies

Types of Access Controls

Mandatory Access Controls (MACs):

✓ Required

✓ Structured & coordinated
with a data classification scheme

✓ When implemented, users & data owners
have limited control over their access
to information resources

✓ Use data classification scheme
that rates each collection of information

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

Matrix contains subjects & objects,
with the boundaries
associated with each subject/object pair
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

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
& 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

The goal of the risk management process:

✓ Identify information assets
& their vulnerabilities
✓ Rank them
according to the need for protection

In preparing this list,
wealth of factual information
about the assets & 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**

TABLE 7-5 Ranked Vulnerability Risk Worksheet

Asset	Asset Impact	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 service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via Secure Sockets Layer (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 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 service request via e-mail (inbound)	55	E-mail disruption due to power 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
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.01	1

Documenting your results

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, & who reviews them

TABLE 7-6 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or 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 risk-rating ranked value to each uncontrolled asset–vulnerability pair

Summary

Introduction

Risk management

Risk identification

Risk assessment

Documenting the results of Risk Assessment

Thank you!

Scott Granneman