Information Security Management

Chapter 8
Risk Management:
Assessing and Controlling Risk

Webster University
Scott Granneman

“Weakness is a better teacher
than strength.
Weakness must learn
to understand the obstacles
that strength brushes aside.”

-- Mason Cooley
(1927-)

“Conan, what is good in life?”

“To crush your enemies,
to drive them before you,
& to hear the lamentations of their women!”

-- Conan the Barbarian,
25,675 BCE

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

Understand and select from the risk mitigation strategy options to control risk

Identify the risk control classification categories

Use existing conceptual frameworks to evaluate risk controls, & formulate a cost benefit analysis

Maintain and perpetuate risk controls

Understand the OCTAVE approach to managing risk, & locate more detailed information about it if & when necessary

To keep up with the competition,
organizations must design & create
a safe environment
in which business processes & procedures
can function

This environment must

- ✓ Maintain confidentiality & privacy
- ✓ Assure the integrity & availability of organizational data

These objectives are met
via the application of the principles
of risk management

An organization must choose one of 4 basic strategies to control risks:

Avoidance: applying safeguards
that eliminate or reduce
the remaining uncontrolled risks
for the vulnerability

Transference: shifting the risk
to other areas or to outside entities

Mitigation: reducing the impact
should the vulnerability be exploited

Acceptance: understanding the consequences
& accept the risk without control or mitigation

Avoidance: “Don’t go near the bear.”

Transference: “Get the bear to chase **you**.”

Mitigation: “Wear bear armor.”

Acceptance: “Here comes the bear. Oh well.”

Avoidance is the risk control strategy
that attempts to prevent
the exploitation of the vulnerability

Avoidance is accomplished through:

✓ Application of policy

✓ Application of training & education

✓ Countering threats

✓ Implementation of
technical security controls & safeguards

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

May be accomplished by:

✓ Rethinking how services are offered

✓ Revising deployment models

✓ Outsourcing to other organizations

✓ Purchasing insurance

✓ Implementing service contracts with providers

Mitigation is the control approach
that attempts to reduce,
by means of planning & preparation,
the damage caused
by the exploitation of vulnerability

This approach includes 3 types of plans:

- ✓ Disaster recovery plan (DRP)
- ✓ Incident response plan (IRP)
- ✓ Business continuity plan (BCP)

Mitigation depends upon the ability
to detect & respond to an attack
as quickly as possible

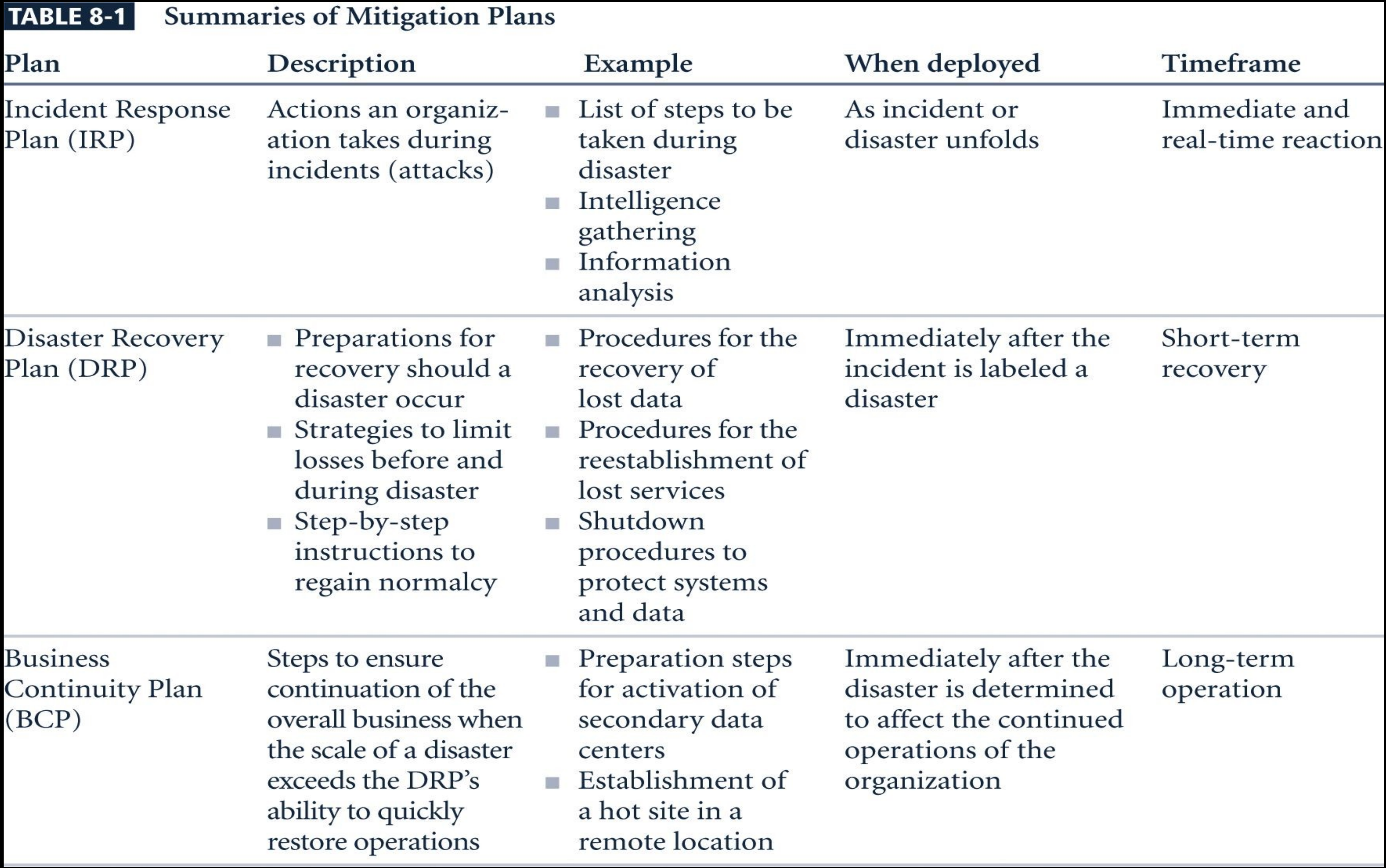

TABLE 8-1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Timeframe
Incident Response Plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan (DRP)	■ Preparations for recovery should a disaster occur ■ Strategies to limit losses before and during disaster ■ Step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

Acceptance is the choice
to do nothing
to protect an information asset
& to accept the loss when it occurs

This control, or lack of control,
assumes that
it may be a prudent business decision to

✓ Examine alternatives
✓ Conclude the cost
of protecting an asset
does not justify the security expenditure

Only valid use of acceptance strategy occurs when organization has:

✓ Determined level of risk to information asset

✓ Assessed probability of attack
& likelihood of a successful exploitation of vulnerability

✓ Approximated ARO of the exploit

✓ Estimated potential loss from attacks

✓ Performed a thorough cost benefit analysis

✓ Evaluated controls
using each appropriate type of feasibility

✓ Decided that the particular asset
did not justify the cost of protection

Risk control involves
selecting 1 of the 4 risk control strategies
for the vulnerabilities
present within the organization

If the loss is within the range of losses
the organization can absorb,
or if the attacker’s gain
is less than expected costs of the attack,
the organization may choose
to accept the risk

Otherwise, 1 of the other control strategies
will have to be selected

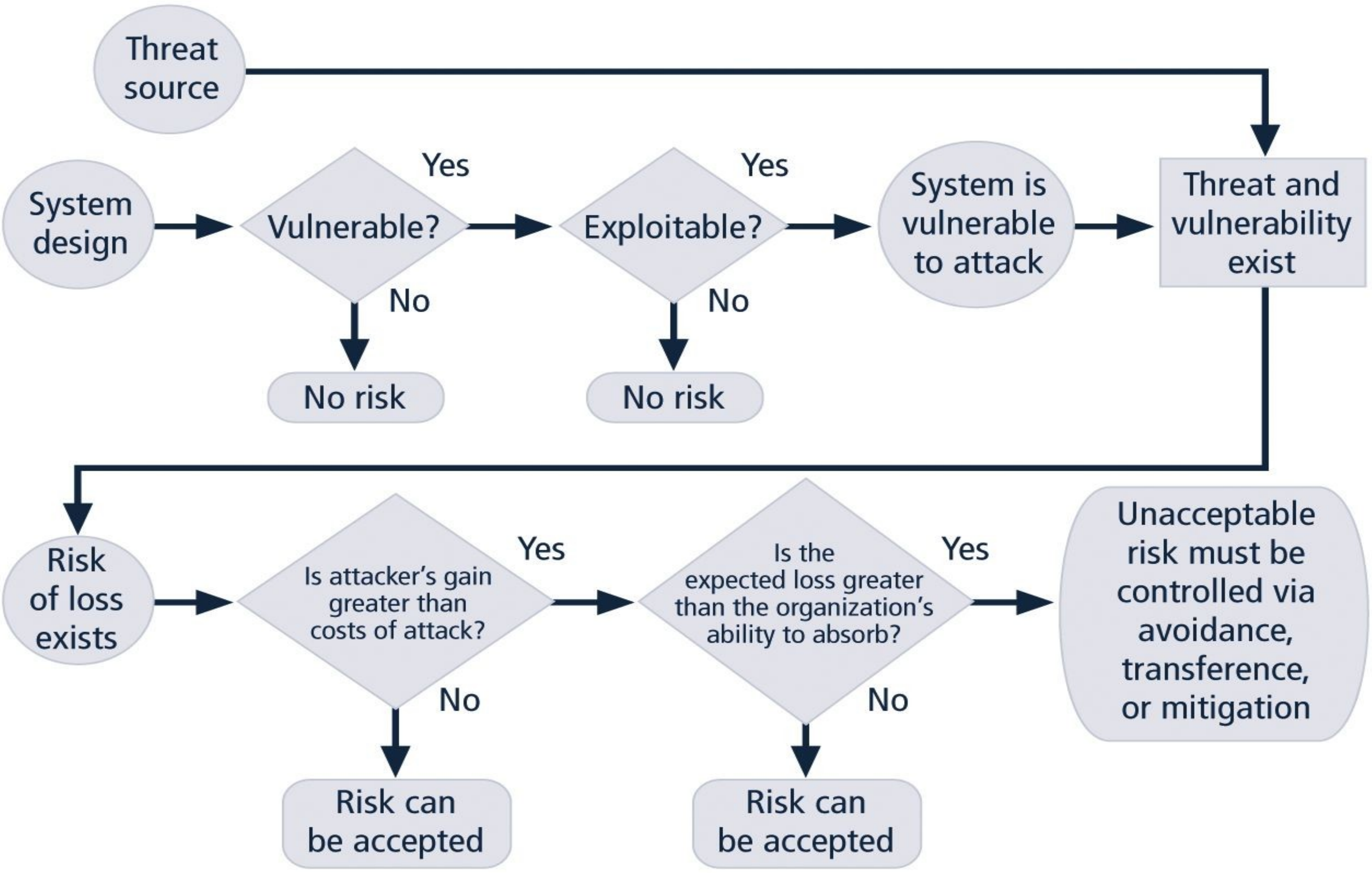
Threat source
System design
Vulnerable?
Yes
No
No risk
Exploitable?
Yes
No
No risk
System is vulnerable to attack
Threat and vulnerability exist
Risk of loss exists
Is attacker's gain greater than costs of attack?
Yes
No
Risk can be accepted
Is the expected loss greater than the organization's ability to absorb?
Yes
No
Risk can be accepted
Unacceptable risk must be controlled via avoidance, transference, or mitigation

FIGURE 8-2 Risk-Handling Action Points

Some rules

When a vulnerability exists:
Implement security controls
to reduce the likelihood
of a vulnerability being exercised

When a vulnerability can be exploited:
Apply layered controls
to minimize the risk or prevent occurrence

**When the attacker’s potential gain
is greater than the costs of attack**:
Apply protections to increase the attacker’s cost,
or reduce the attacker’s gain,
using technical or managerial controls

When potential loss is substantial:
Apply design controls
to limit the extent of the attack,
thereby reducing the potential for loss

Once a control strategy
has been selected & implemented,
the effectiveness of controls
should be monitored & measured
on an ongoing basis
to determine its effectiveness

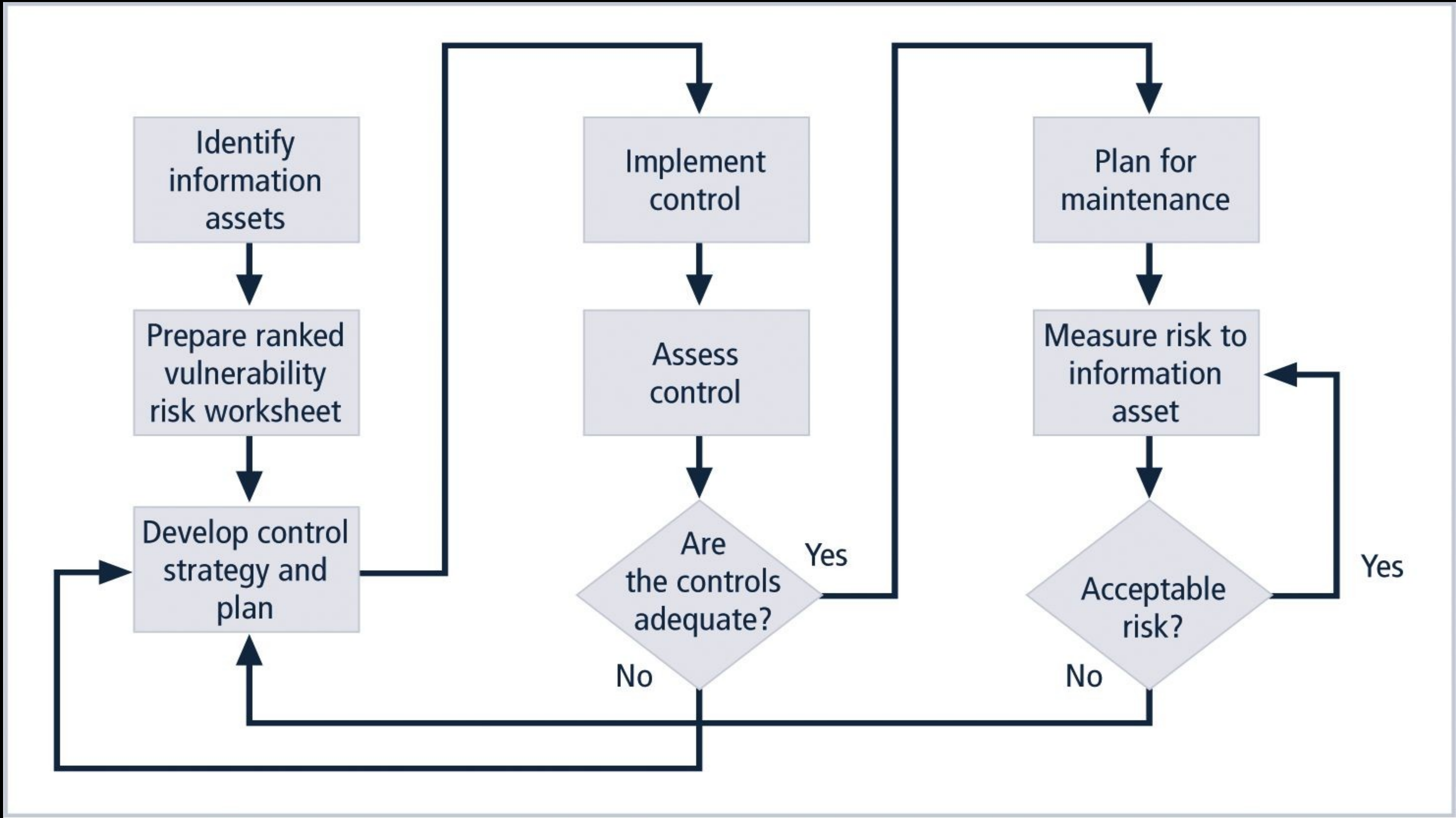
Identify information assets
Prepare ranked vulnerability risk worksheet
Develop control strategy and plan
Implement control
Assess control
Are the controls adequate?
Yes
No
Plan for maintenance
Measure risk to information asset
Acceptable risk?
Yes
No

FIGURE 8-3 Risk Control Cycle

Controlling risk by means of
avoidance, mitigation, or transference
may be accomplished
by implementing controls or safeguards

Controls can be grouped for discussion
by 1 of 4 categories:

- ✓ Control function
- ✓ Architectural layer
- ✓ Strategy layer
- ✓ InfoSec principle

Preventive controls

Stop attempts to exploit a vulnerability
by implementing enforcement
of an organizational policy
or a security principle

Use a technical procedure,
or some combination
of technical means & enforcement methods

Detective controls

Warn organizations
of violations of security principles,
organizational policies,
or attempts to exploit vulnerabilities

Use techniques such as
audit trails,
intrusion detection,
& configuration monitoring

Some controls apply
to one or more layers
of an organization’s technical architecture

Possible architectural layers
include the following:

✓ Organizational policy
✓ External networks
✓ Extranets
✓ Demilitarized zones
✓ Intranets
✓ Network devices that interface network zones
✓ Systems
✓ Applications

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

✓ Avoidance
✓ Mitigation
✓ Transference

Note that the acceptance strategy
is not an option
since it involves the absence of controls

Risk controls operate
within one or more
of the commonly accepted
information security principles:

✓ Confidentiality
✓ Integrity
✓ Availability
✓ Authentication
✓ Authorization
✓ Accountability
✓ Privacy

Before deciding on the strategy
for a specific vulnerability,
all readily accessible information
about the consequences of the vulnerability
must be explored

“What are the advantages
of implementing a control
as opposed to the disadvantages
of implementing the control?”

Number of ways
to determine advantage or disadvantage
of a specific control

Primary means are based
on the value of information assets
that control is designed to protect

Economic Feasibility:
criterion most commonly used
when evaluating a project
that implements
infosec controls & safeguards

Organizations are urged
to begin a cost benefit analysis (CBA),
or economic feasibility study.
by evaluating

✓ Worth of the information assets to be protected
✓ Loss in value
if those information assets are compromised

Just as it is difficult
to determine the value of information,
it is difficult to determine
the cost of safeguarding it

Some of the items
that affect the cost
of a control or safeguard include:

✓ Cost of development or acquisition
of hardware, software, and services
✓ Training fees
✓ Cost of implementation
✓ Service costs
✓ Cost of maintenance

Benefit is the value to the organization
of using controls
to prevent losses
associated with a specific vulnerability

Usually determined by:

✓ Valuing the information asset or assets
exposed by vulnerability
✓ Determining how much of that value is at risk
& how much risk there is for the asset

This is expressed as
the **annualized loss expectancy** (ALE)

Asset valuation is the process
of assigning financial value or worth
to each information asset

Value of information
differs within organizations
& between organizations

Based on information characteristics &
perceived value of that information

Valuation of assets involves estimation
of real & perceived costs
associated with:

design,
development,
installation,
maintenance,
protection,
recovery,
& defense against loss & litigation

Some of the components of asset valuation include:

✓ Value retained from the cost
of creating the information asset
✓ Value retained from past maintenance
of the information asset
✓ Value implied by the cost of replacing the information
✓ Value from providing the information
✓ Value acquired from the cost
of protecting the information
✓ Value to owners
✓ Value of intellectual property
✓ Value to adversaries
✓ Loss of productivity
while the information assets are unavailable
✓ Loss of revenue
while information assets are unavailable

Organization must be able to place a dollar value on each information assets it owns, based on:

✓ How much did it cost to create or acquire?

✓ How much would it cost to recreate or recover?

✓ How much does it cost to maintain?

✓ How much is it worth to the organization?

✓ How much is it worth to the competition?

Potential loss is that
which could occur
from the exploitation of vulnerability
or a threat occurrence

The questions that must be asked include:

✓ What loss could occur,
& what financial impact would it have?

✓ What would it cost to recover from the attack,
in addition to the financial impact of damage?

✓ What is the single loss expectancy for each risk?

Single loss expectancy (SLE): calculation of value associated with most likely loss from an attack

Based on asset value
& expected percentage of loss
that would occur from a particular attack:

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

Where EF = the percentage loss
that would occur
from a given vulnerability being exploited

This information is usually estimated

In most cases,
probability of a threat occurring
is the probability of loss from an attack
within a given time frame

Commonly referred to as the ARO,
or **annualized rate of occurrence**

CBA determines
whether or not a control alternative
is worth its associated cost

CBAs may be calculated:

Before a control or safeguard
is implemented to determine
if the control is worth implementing

OR

After controls have been implemented
& have been functioning for a time:
CBA = ALE(prior) – ALE(post) – ACS

The CBA formula for
CBA = ALE(prior) – ALE(post) – ACS

ALE(prior to control)
is the annualized loss expectancy
of the risk
before the implementation of the control

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

ACS is the annual cost of the safeguard

Organizational feasibility analysis
examines how well
proposed InfoSec alternatives
will contribute to operation of an organization
by looking at
user acceptance & support,
management acceptance & support,
& overall requirements
of organization’s stakeholders

Technical feasibility examines
whether or not the organization has or can acquire
the technology to implement
& support the alternatives

Political feasibility defines
what can & cannot occur
based on the consensus & relationships
between the communities of interest

Benchmarking:

✓ Seeking out & studying practices of other organizations that produce desired results

✓ Measuring differences between how organizations conduct business

When benchmarking, an organization typically uses 1 of 2 measures to compare practices:

✓ **Metrics-based** measures are comparisons based on numerical standards

✓ **Process-based** measures are generally less focused on numbers & are more strategic

In the field of InfoSec,
2 categories of benchmarks are used:

1. Standards of due care & due diligence
2. Best practices

Within best practices,
the **gold standard**
is a subcategory of practices
that are typically viewed as
“the best of the best”

For legal reasons,
an organization may be forced to adopt
a certain minimum level of security

When organizations adopt levels of security
for legal defense, they may need to show
that they have done what any prudent
organization would do in similar
circumstances; i.e., **due care**

Due diligence demonstrates
that the organization is persistent
in ensuring implemented standards
continue to provide
required levels of protection

Best business practices: security efforts
that seek to provide
a superior level of performance

Are among the best in the industry,
balancing access to information
with adequate protection,
while maintaining a solid degree
of fiscal responsibility

Companies with best practices
may not be the best in every area

May simply have established
an extremely high quality
or successful security effort in one or more areas

Even the best business practices
are not sufficient for some organizations

These organizations aspire
to set the standard
by implementing
the most protective, supportive,
& yet fiscally responsible standards they can

The **gold standard** is
a defining level of performance
that demonstrates
a company’s industrial leadership, quality,
& concern for the protection of information

Seeking the gold standard
is a method of striving for excellence

When considering best practices for adoption, address the following questions:

Does your organization resemble the organization that implemented the best practice?

Is your organization in a similar industry?

Does your organization face similar challenges?

Is your organizational structure similar to the organization that implemented the best practice?

Can your organization expend resources that are in line with the requirements of the best practice?

Is your organization in a similar threat environment as the one cited in the best practice?

Problems with benchmarking & best practices

✓ Organizations don’t talk to each other

✓ No two organizations are identical

✓ Best practices are a moving target

✓ Simply knowing
what was going on a few years ago
does not necessarily indicate what to do next

Baselining is
the analysis of measures
against established standards

In InfoSec,
baselining is the comparison
of security activities & events
against
the organization’s future performance

The information gathered
for an organization’s first risk assessment
becomes the baseline for future comparisons

Risk appetite defines
the quantity & nature of risk
that organizations are willing to accept,
as they evaluate the trade-offs
between perfect security
& unlimited accessibility

Reasoned approach to risk
is one that
balances expense
against possible losses if exploited

When vulnerabilities have been controlled as much as possible, there is often remaining risk that has not been completely accounted for: **residual risk**

Residual risk
=
Risk from a threat
less the effect of
threat-reducing safeguards
+
Risk from a vulnerability
less the effect of
vulnerability-reducing safeguards
+
Risk to an asset
less the effect of
asset value-reducing safeguards

The significance of residual risk
must be judged
within the context
of an organization’s risk appetite

The goal of InfoSec
is not to bring residual risk to zero,
but to bring it in line
with an organization’s risk appetite

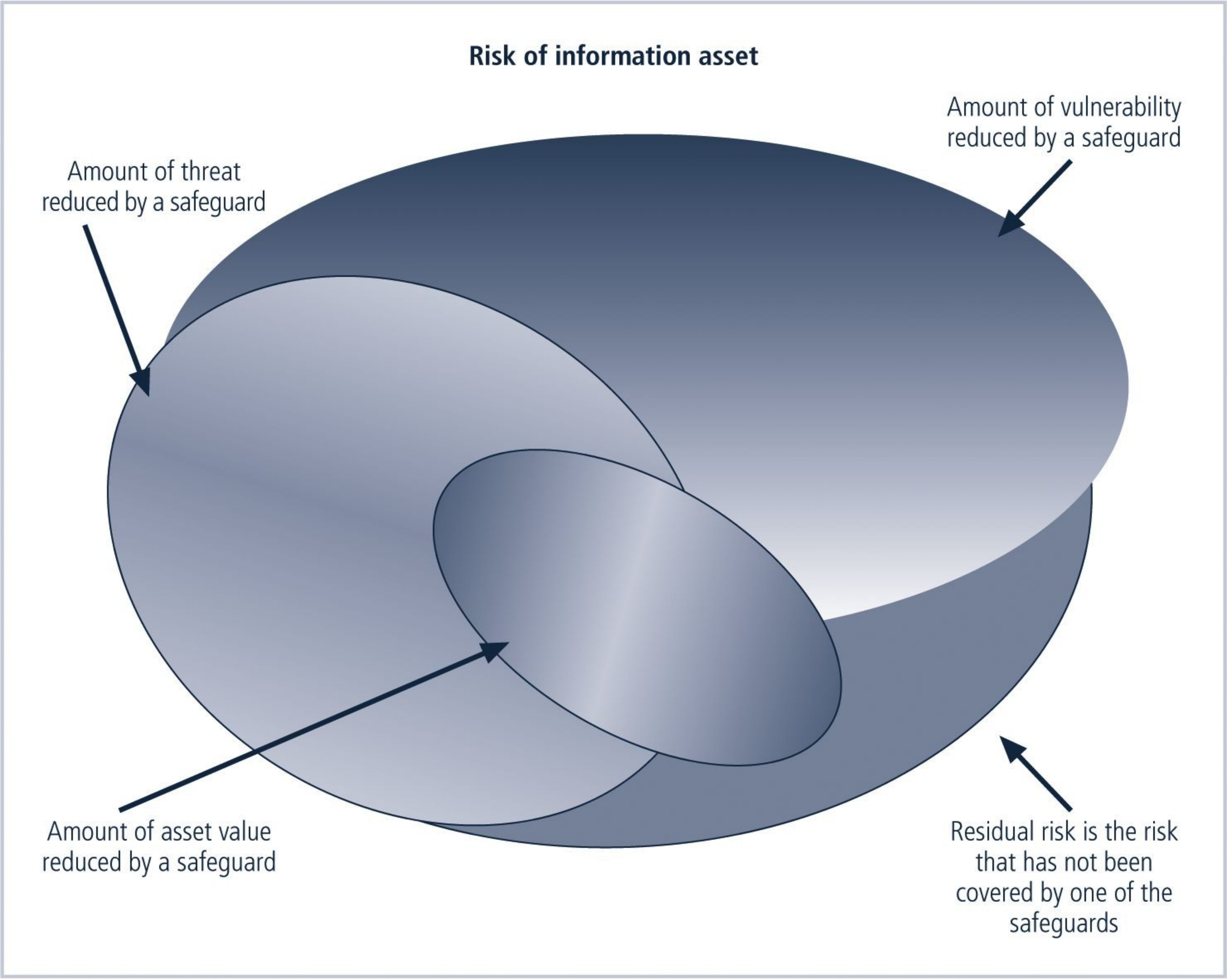
Risk of information asset
Amount of vulnerability reduced by a safeguard
Amount of threat reduced by a safeguard
Amount of asset value reduced by a safeguard
Residual risk is the risk that has not been covered by one of the safeguards

FIGURE 8-4 Residual Risk

When risk management program
has been completed,
series of proposed controls are prepared

Each justified by one or more
feasibility or rationalization approaches

At minimum,
each information asset-threat pair
should have a documented control strategy
that clearly identifies
any residual risk remaining
after the proposed strategy
has been executed

Some organizations document
outcome of control strategy
for each information asset-threat pair
in an **action plan**,
which can include concrete tasks,
each with accountability
assigned to an organizational unit
or to an individual

Quantitative assessment
performs asset valuation
with actual values or estimates

An organization could determine
that it cannot put specific numbers
on these values

Organizations could use
qualitative assessments instead,
using scales instead of specific estimates

Operationally Critical Threat, Asset, & Vulnerability Evaluation^SM (OCTAVE^SM) Method:

Defines essential components
of a comprehensive, systematic, context-driven,
self-directed InfoSec risk evaluation

By following OCTAVE Method,
organization can make
information-protection decisions
based on risks
to confidentiality, integrity, & availability
of critical information technology assets

Operational or business units & IT department
work together
to address InfoSec needs of the organization

Phases of The OCTAVE Method

Phase 1: Build Asset-Based Threat Profiles

Organizational evaluation

Key areas of expertise within organization
are examined to elicit important knowledge about:

✓ Information assets
✓ Threats to those assets
✓ Security requirements of assets
✓ What organization is currently doing
to protect its information assets
✓ Weaknesses in organizational policies & practice

more ... →

Phase 2: Identify Infrastructure Vulnerabilities

Evaluation of information infrastructure

Key operational components
of information technology infrastructure
are examined for weaknesses
(technology vulnerabilities)
that can lead to unauthorized action

more … →

Phase 3: Develop Security Strategy & Plans

Risks are analyzed in this phase

Information generated by
organizational & information infrastructure evaluations
(Phases 1 & 2)
is analyzed to:

✓ Identify risks to organization

✓ Evaluate risks based on
their impact to the organization’s mission

✓ Organization protection strategy
& risk mitigation plans
for the highest priority risks are developed

The OCTAVE Method:

Self directed

Requires analysis team
to conduct evaluation & analyze information

Basic tasks of the team are to:

✓ Facilitate Phase 1’s
knowledge elicitation workshops
✓ Gather any necessary supporting data
✓ Analyze threat & risk information
✓ Develop a protection strategy for the organization
✓ Develop mitigation plans to address risks
to the organization’s critical assets

more … →

Uses workshop-based approach for gathering information & making decisions

Relies upon the following major catalogs of information:

✓ Catalog of practices:
collection of good strategic
& operational security practices

✓ Threat profile:
range of major sources of threats
that an organization needs to consider

✓ Catalog of vulnerabilities:
collection of vulnerabilities
based on platform & application

Each phase of the OCTAVE Method contains two or more processes

Each process is made of activities

Phase 1: Build Asset-Based Threat Profiles

Process 1:
Identify Senior Management Knowledge

Process 2:
Identify Operational Area Management Knowledge

Process 3: Identify Staff Knowledge

Process 4: Create Threat Profiles

more … →

Phase 2: Identify Infrastructure Vulnerabilities

Process 5: Identify Key Components

Process 6: Evaluate Selected Components

Phase 3: Develop Security Strategy & Plans

Process 7: Conduct Risk Analysis

Process 8: Develop Protection Strategy

Preparing for the OCTAVE Method

✓ Obtain senior management sponsorship of OCTAVE

✓ Select analysis team members

✓ Train analysis team

✓ Select operational areas to participate in OCTAVE

✓ Select participants

✓ Coordinate logistics

✓ Brief all participants

For more information,
download the
Octave$^{\text{SM}}$ method implementation guide

http://www.cert.org/octave/omig.html

Summary

Introduction

Risk Control Strategies

Risk Control Strategy Selection

Categories of Controls

Feasibility Studies & Cost-Benefit Analysis

Risk Management Discussion Points

Recommended Risk Control Practices

The OCTAVE Method

Thank you!

Scott Granneman