Week 9

IT SECURITY MANAGEMENT & RISK ASSESSMENT

IT SECURITY CONTROLS, PLANS, AND PROCEDURES

Chapter 14

IT Security Management and Risk Assessment

IT Security Management Overview

Ensures that critical assets are sufficiently protected in a cost-effective manner

Security risk assessment is needed for each asset in the organization that requires protection

Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

IT Security Management

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

Determining organizational IT security objectives, strategies, and policies	Determining organizational IT security requirements	Identifying and analyzing security threats to IT assets within the organization	Identifying and analyzing risks	Specifying appropriate safeguards	Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization	Developing and implementing a security awareness program	Detecting and reacting to incidents

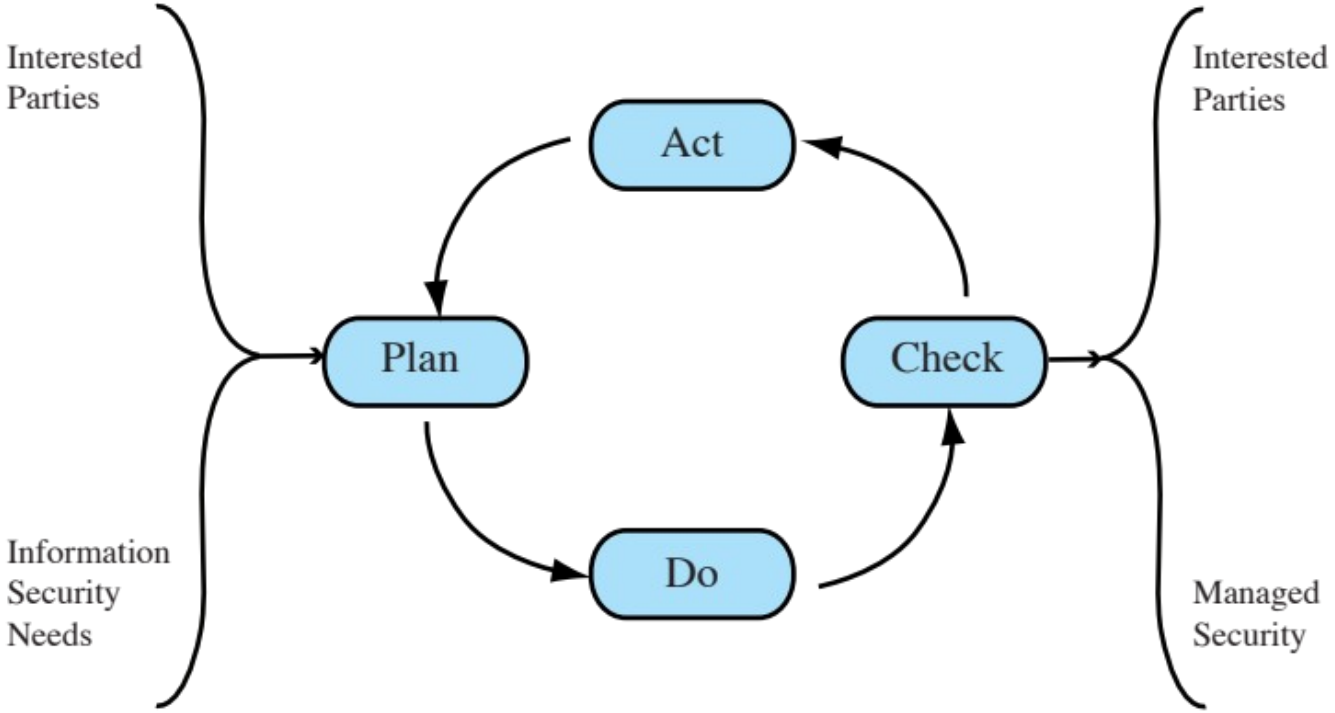


Figure 14.2 The Plan - Do - Check - Act Process Model

Plan-Do-Check-Act

Organizational Context and Security Policy

Maintained and updated regularly

- Using periodic security reviews
- Reflect changing technical/risk environments

Examine role and importance of IT systems in organization

First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy

Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of responsibilities
- Risk management approach
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when policy reviewed, and change control to it

Management Support / Sponsorship

IT security policy must be supported by senior management

Need IT security officer

- To provide consistent overall supervision
- Liaison with senior management
- Maintenance of IT security objectives, strategies, policies
- Handle incidents
- Management of IT security awareness and training programs
- Interaction with IT project security officers

Large organizations need separate IT project security officers associated with major projects and systems

- Manage security policies within their area

Security Risk Assessment

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

Goal is to implement agreed controls to provide protection against the most common threats

Forms a good base for further security measures

Use “industry best practice”

- Easy, cheap, can be replicated
- Gives no special consideration to variations in risk exposure
- May give too much or too little security

Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

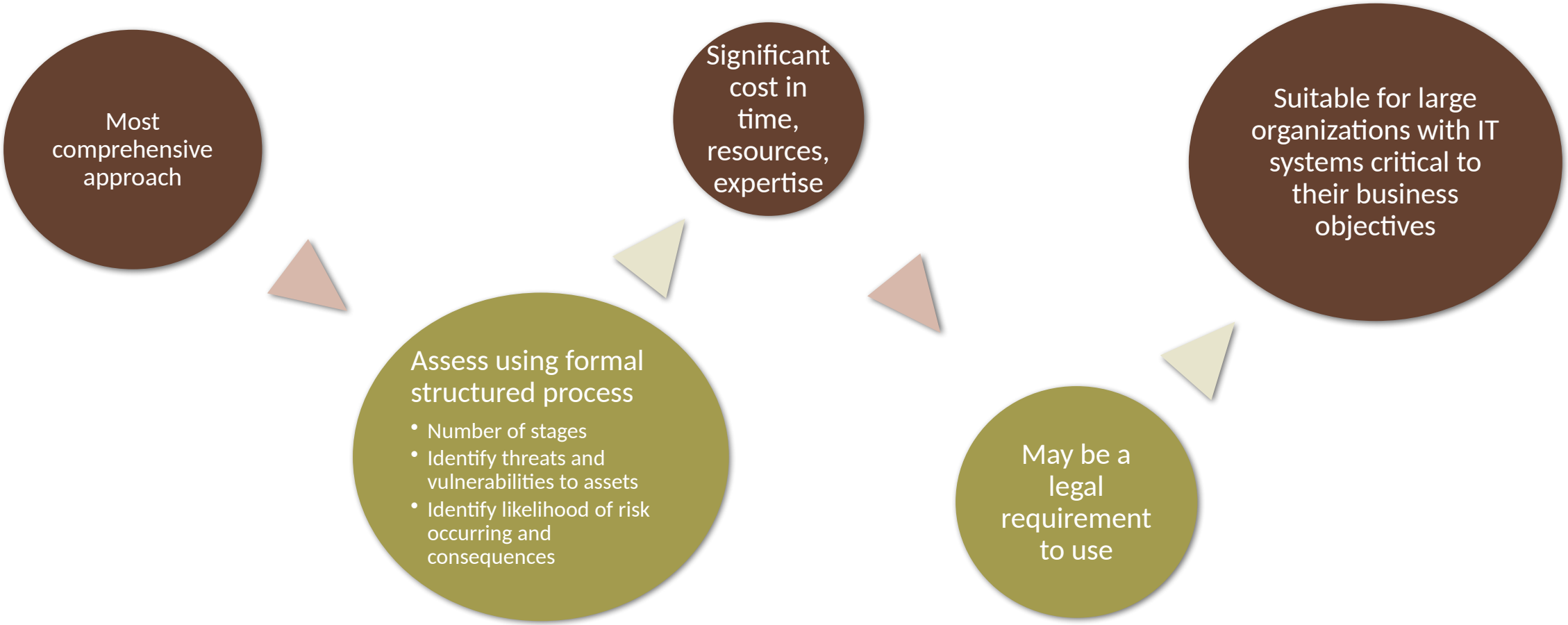
Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis



Combined Approach

Combines elements of the baseline, informal, and detailed risk analysis approaches

Aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time

Approach starts with the implementation of suitable baseline security recommendations on all systems

Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment

A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements

Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted

Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

Risk Assessment

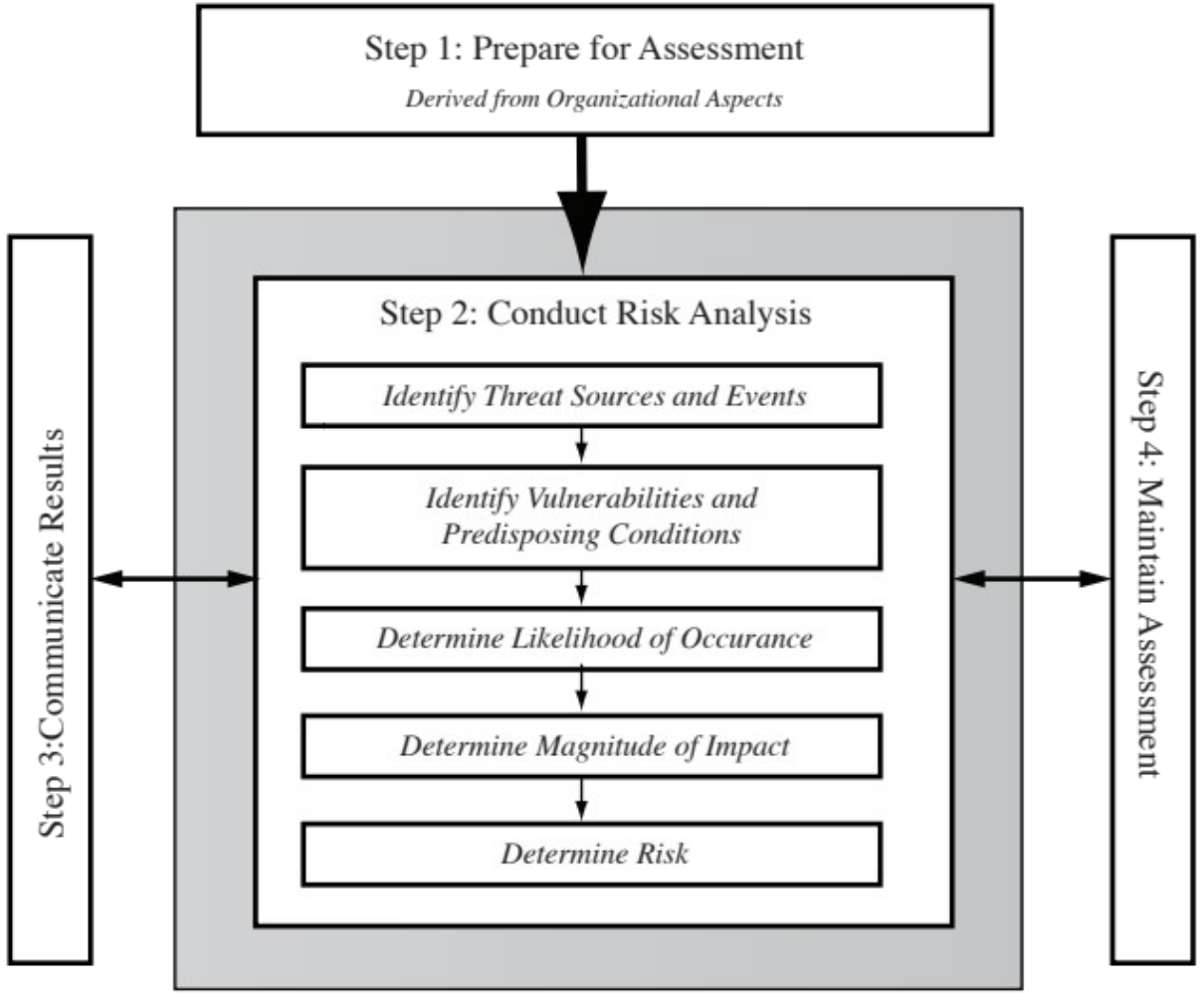


Figure 14.3 Risk Assessment Process

Establishing Context

- Initial step
- Determine the basic parameters of the risk assessment
- Identify the assets to be examined
- Explores political and social environment in which the organization operates
- Legal and regulatory constraints
- Provide baseline for organization’s risk exposure
- Risk appetite
- The level of risk the organization views as acceptable

Risk Context

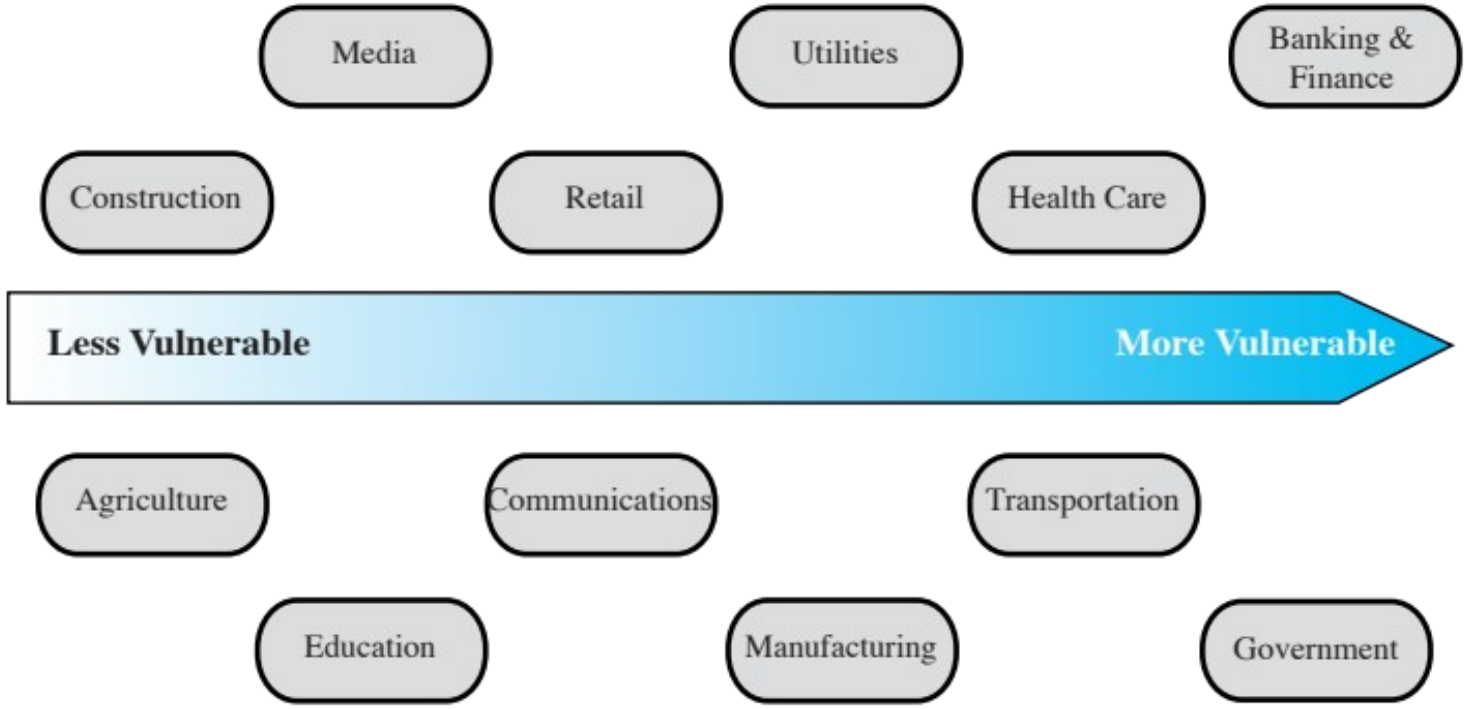


Figure 14.4 Generic Organizational Risk Context

Asset Identification

Last component is to identify assets to examine

Draw on expertise of people in relevant areas of organization to identify key assets

- Identify and interview such personnel

Asset

- "anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives

Threat Identification

Threat Sources

Threats may be

- Natural “acts of God”
- Man-made
- Accidental or deliberate

Any previous experience of attacks seen by the organization also needs to be considered

Evaluation of human threat sources should consider:

- Motivation
- Capability
- Resources
- Probability of attack
- Deterrence

Vulnerability Identification

Identify exploitable flaws or weaknesses in organization's IT systems or processes

- Determines applicability and significance of threat to organization

Need combination of threat and vulnerability to create a risk to an asset

Outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

Analyze Risks

Specify likelihood of occurrence of each identified threat to asset given existing controls

Specify consequence should threat occur

Derive overall risk rating for each threat

- Risk = probability threat occurs x cost to organization

Hard to determine accurate probabilities and realistic cost consequences

Use qualitative, not quantitative, ratings

Analyze Existing Controls

Existing controls used to attempt to minimize threats need to be identified

Security controls include:

- Management
- Operational
- Technical processes and procedures
- Use checklists of existing controls and interview key organizational staff to solicit information

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Risk Likelihood

Risk Level Determination and Meaning

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Register (example)

Judgements about Risk Treatment

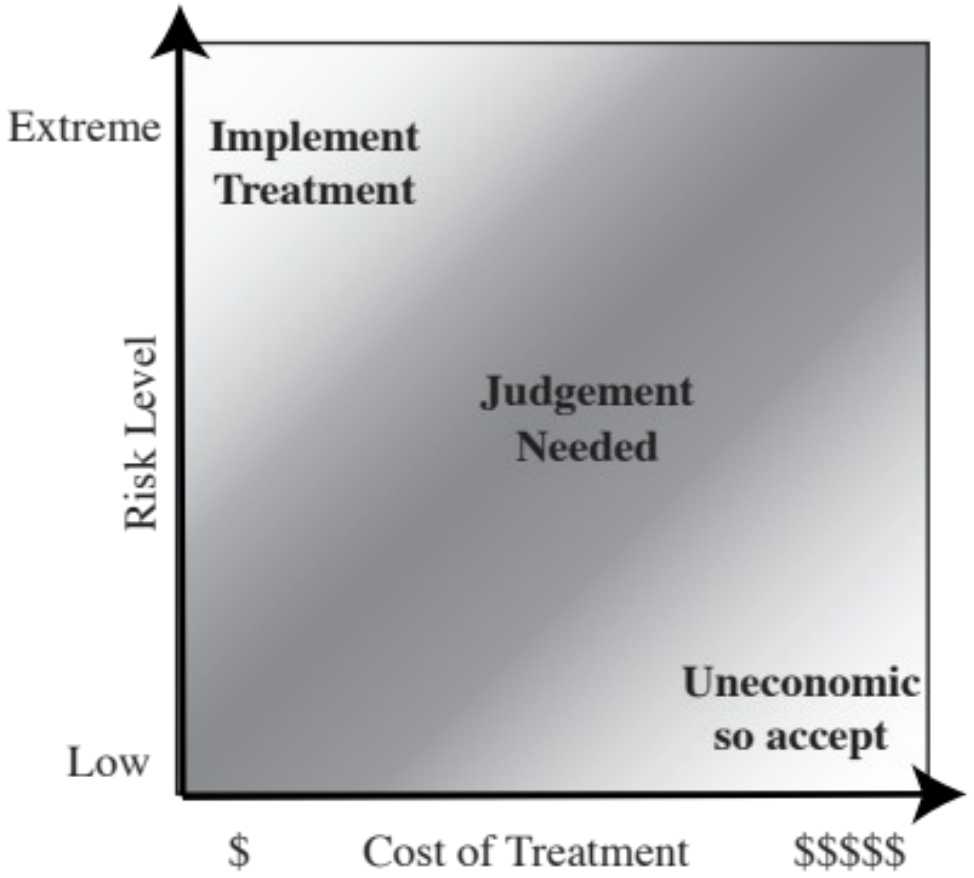


Figure 14.5 Judgment About Risk Treatment

Supervisory Control and Data Acquisition

https://www.youtube.com/watch?v=sphvkkybTt0