COMPUTER SECURITY

PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

Chapter 14

IT Security Management and Risk Assessment

IT Security Management Overview

formal process of answering the questions:

- 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

ISO/IEC 27000 Series of Standards on IT Security Techniques

27000:2009	"Information security management systems - Overview and vocabulary" provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2005	"Information security management systems – Requirements" specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2005	"Code of practice for information security management" provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	"Information security management system implementation guidance" details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	"Information security management – Measurement" provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2008	"Information security risk management" provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2007	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for these bodies.

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

IT Security Management Process

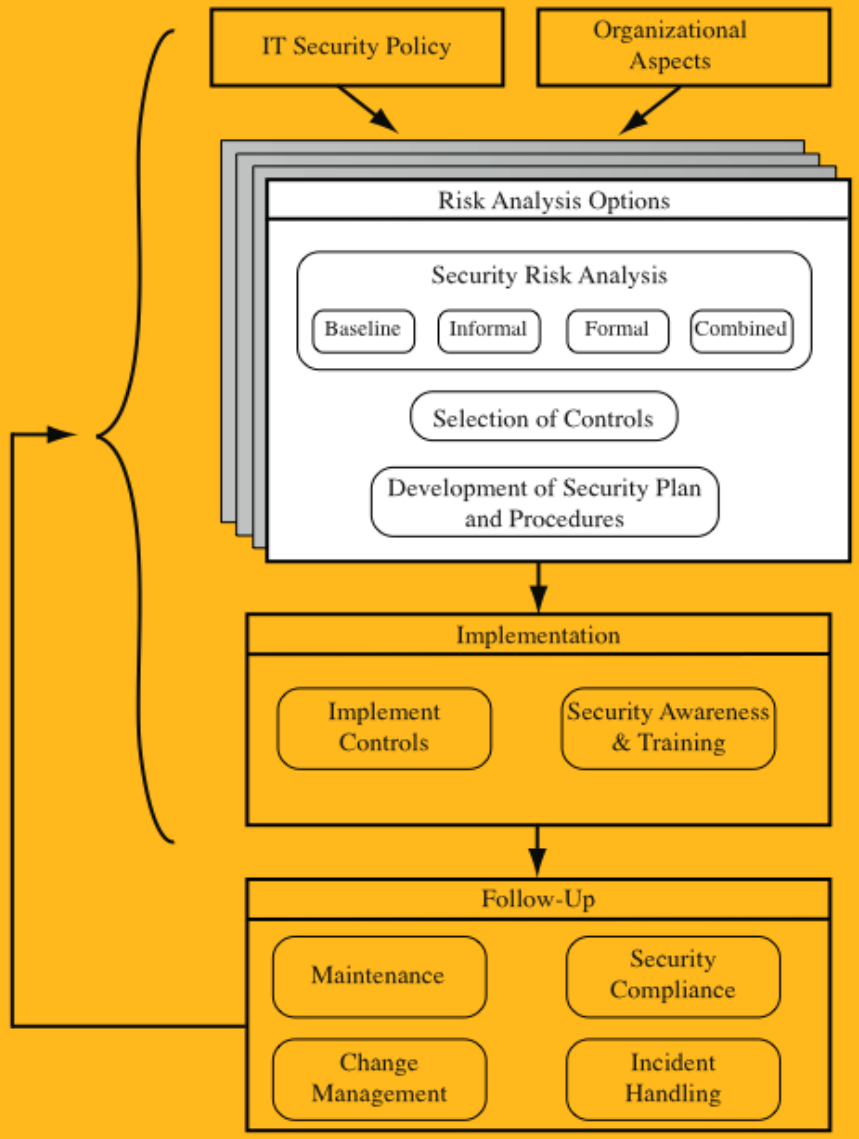


Figure 14.1 Overview of IT Security Management

Plan - Do - Check - Act

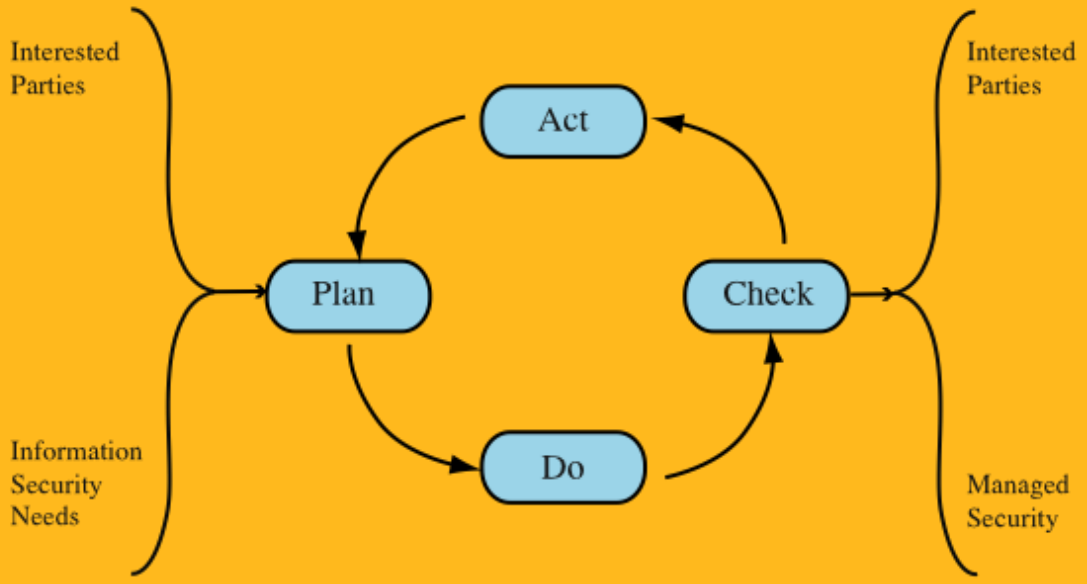


Figure 14.2 The Plan - Do - Check - Act Process Model

Organizational Context and Security Policy

- maintained and updated regularly
  - 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

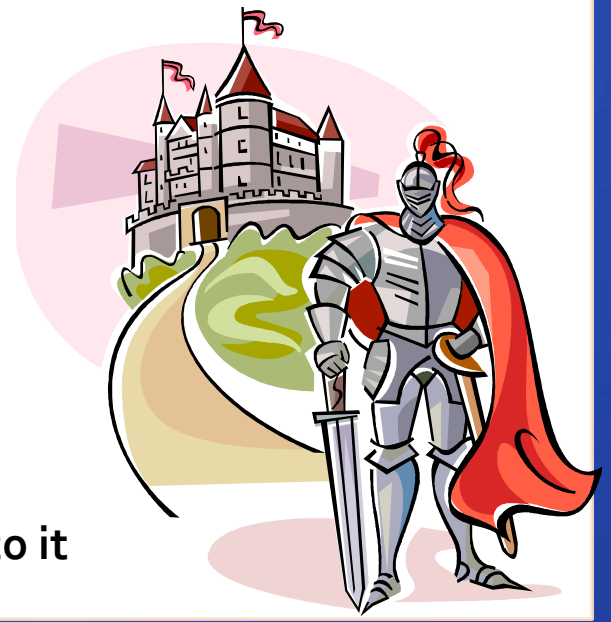
strategies - how to meet objectives

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

- IT security policy must be supported by senior management
- need IT security officer
  - 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

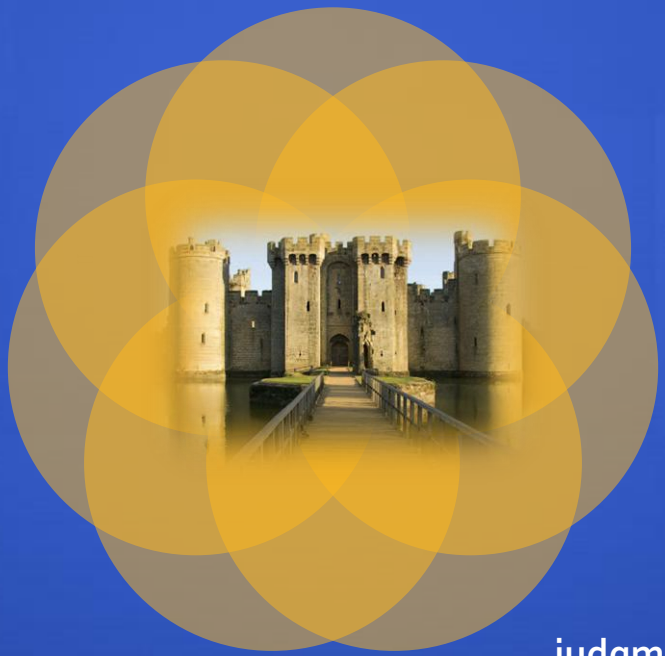
- goal is to implement agreed controls to provide protection against the most common threats
- forms a good base for further security measures
- use "industry best practice"
  - easy, cheap, can be replicated
  - gives no special consideration to variations in risk exposure
  - may give too much or too little security
- generally recommended 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

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

exploits knowledge and expertise of analyst



skewed by analyst's views, varies over time

fairly quick and cheap

some risks may be incorrectly assessed

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

Detailed Risk Analysis

most comprehensive approach

assess using formal structured process

- number of stages
- identify threats and vulnerabilities to assets
- identify likelihood of risk occurring and consequences

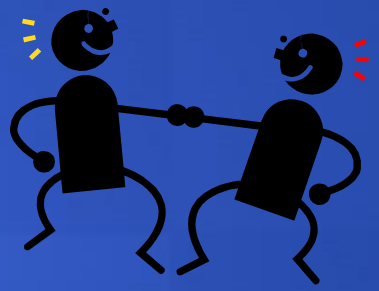
significant cost in time, resources, expertise

may be a legal requirement to use

suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- combines elements of other approaches
  - initial baseline on all systems
  - informal analysis to identify critical risks
  - formal assessment on these systems



- results in the development of a strategic picture of the IT resources and where major risks are likely to occur
- ensures that a basic level of security protection is implemented early
- for most organizations this approach is the most cost effective
- use is highly recommended

Detailed Security Risk Analysis

provides the most accurate evaluation of an organization's IT system's security risks

highest cost

initially focused on addressing defense security concerns

often mandated by government organizations and associated businesses

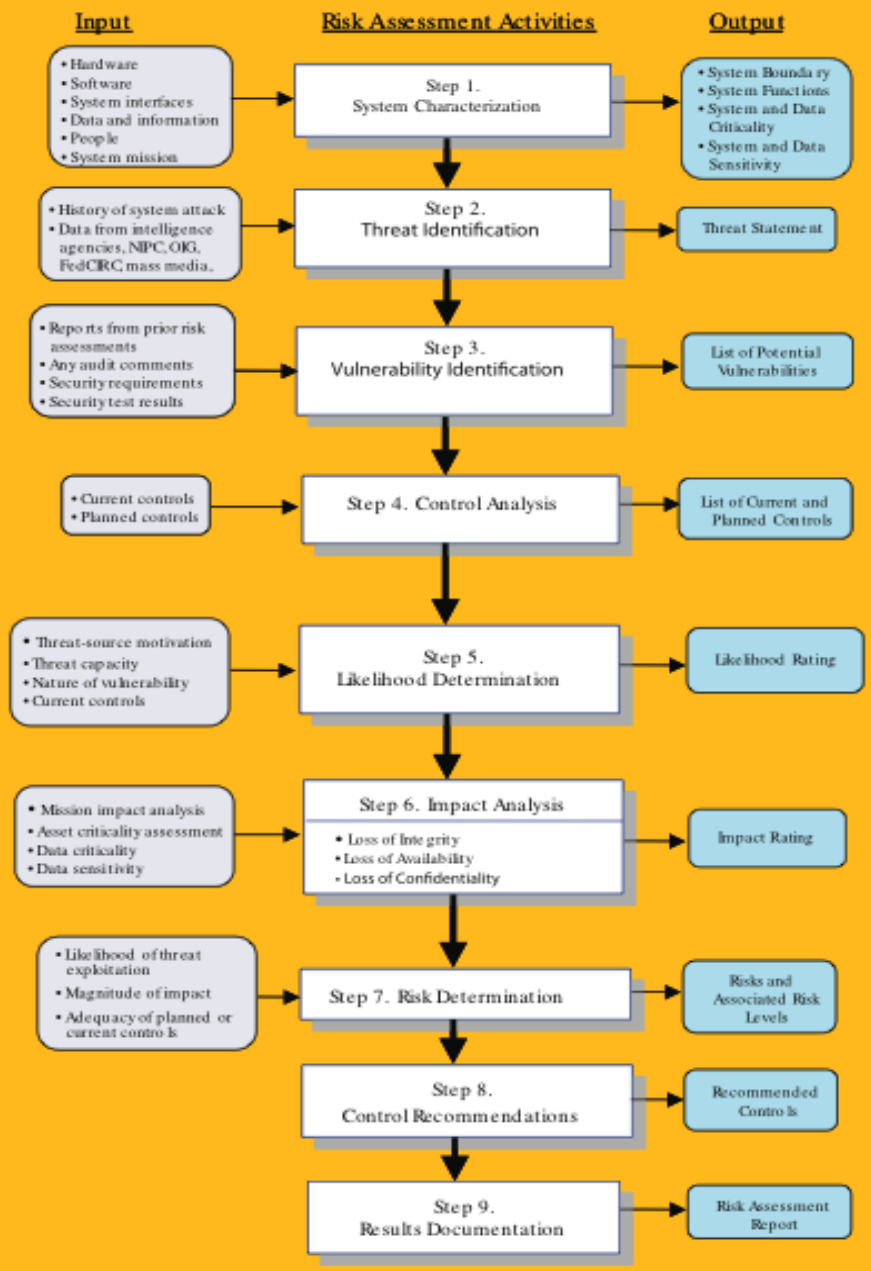


Figure 14.3 Risk Assessment Methodology

Figure 14.3

Risk Assessment Methodology

Establishing the Context

- initial step
  - determine the basic parameters of the risk assessment
  - identify the assets to be examined
- explore 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

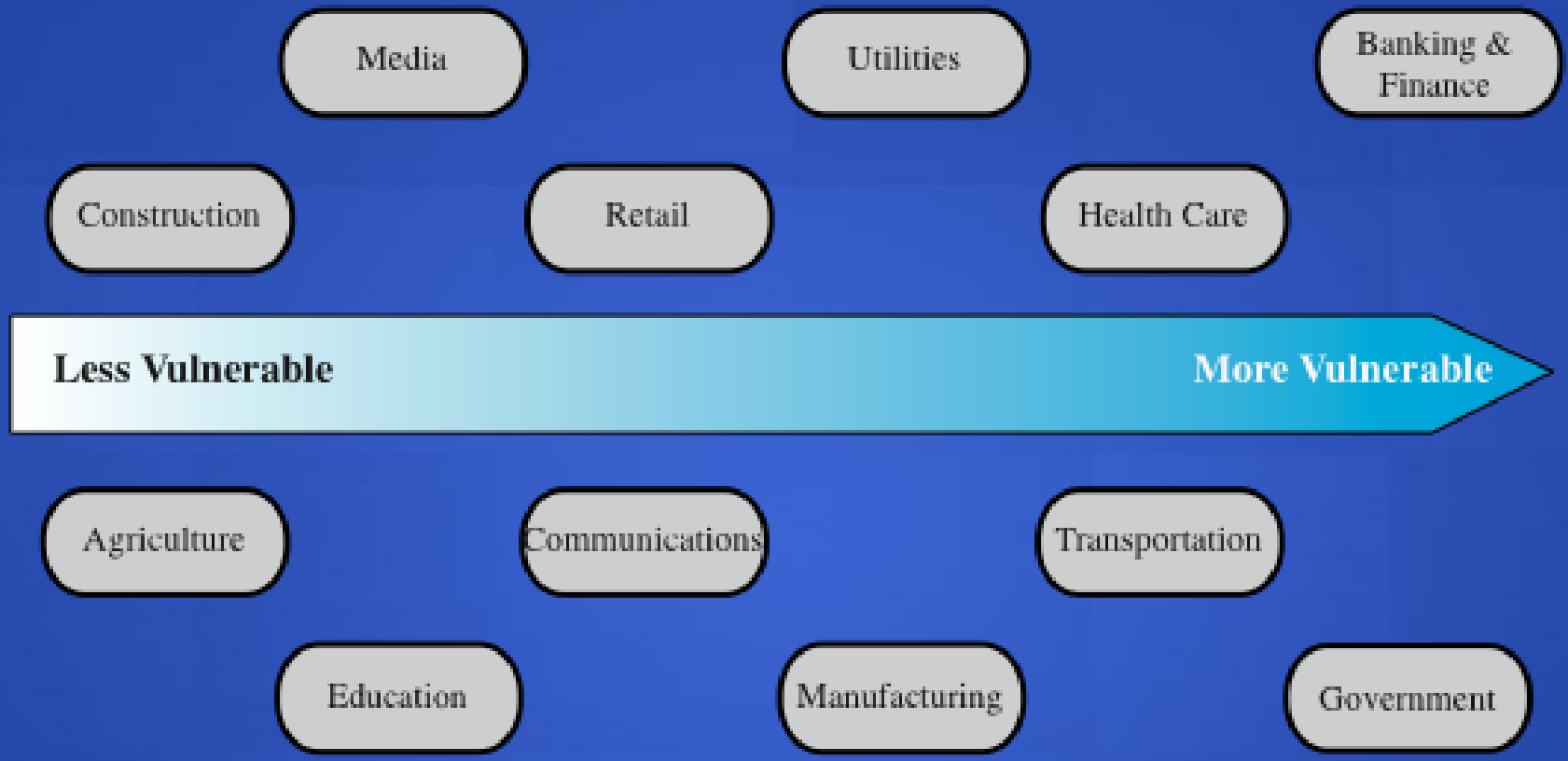


Figure 14.4 Generic Organizational Risk Context

Asset Identification

- last component is to identify assets to examine

asset

- "anything that needs to be protected"
- has value to organization to meet its objectives
- tangible or intangible
- whose compromise or loss would seriously impact the operation of the organization

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

Terminology

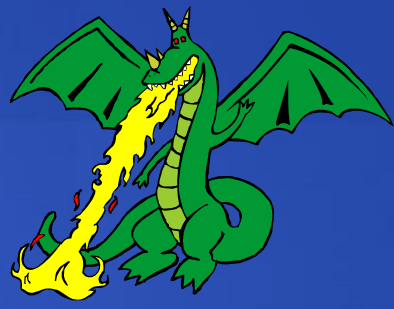
asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification



integrity

reliability

availability

anything that might hinder or prevent an asset from providing appropriate levels of the key security services

confidentiality

accountability

authenticity

Threat Sources

- threats may be
  - natural "acts of God"
  - man-made
  - accidental or deliberate

evaluation of human threat sources should consider:

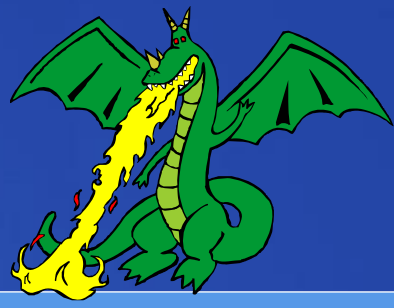
- motivation
- capability
- resources
- probability of attack
- deterrence

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

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

Risk Likelihood

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.

Table 14.2 Risk Likelihood

Table 14.3

Risk Consequences

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

Table 14.4
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.

Table 14.5

Risk Register

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

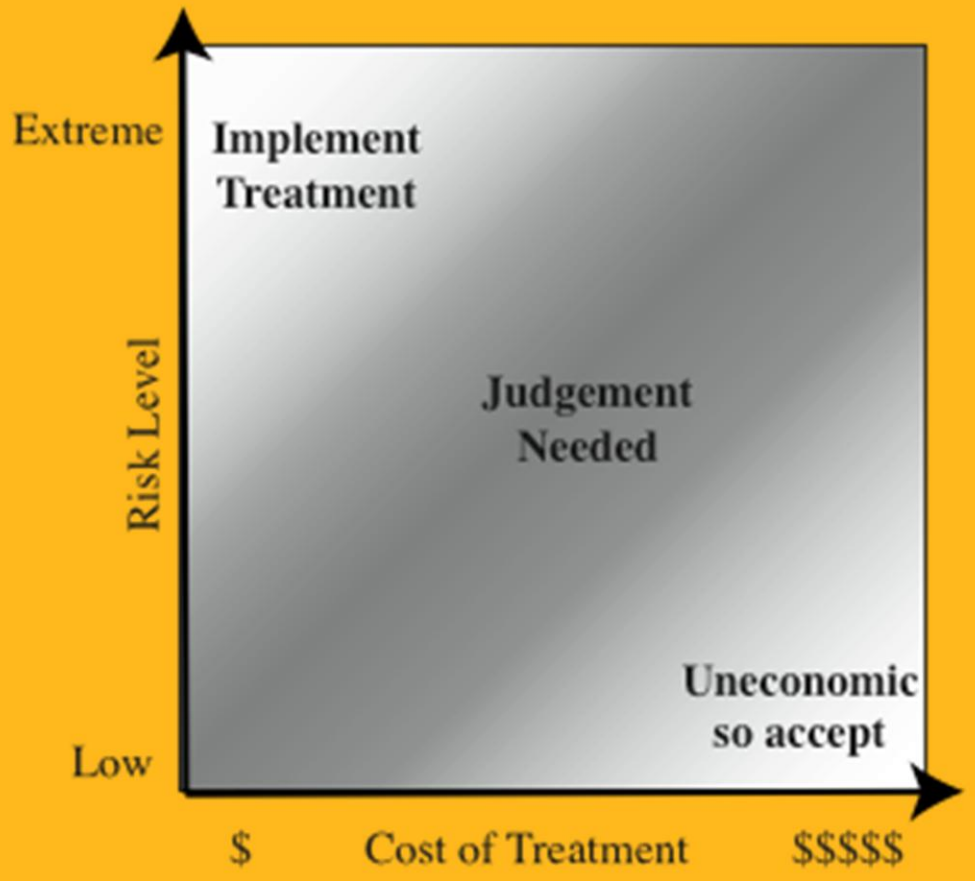


Figure 14.5 Judgment About Risk Treatment

Risk Treatment Alternatives

Case Study: Silver Star Mines

- fictional operation of global mining company
- large IT infrastructure
  - both common and specific software
  - some directly relate to health and safety
  - formerly isolated systems now networked
- decided on combined approach
- subject to legal/regulatory requirements
- management accepts moderate or low risk

Assets

- reliability and integrity of SCADA nodes and net
- integrity of stored file and database information
- availability, integrity of financial system
- availability, integrity of procurement system
- availability, integrity of maintenance/production system
- availability, integrity and confidentiality of mail services

Silver Star Mines
Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls and servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost Certain	Minor	High	6

Summary

- IT security management
  - overview
  - best practice
- organizational context and security policy
- security risk assessment
  - baseline approach
  - informal approach
  - detailed risk analysis
  - combined approach
- Case Study: Silver Star Mines
- detailed security risk analysis
  - context and system characterization
  - risk assessment methodology
  - identification of threats/risks/vulnerabilities
- risk alternatives
  - risk acceptance
  - risk avoidance
  - risk transfer
  - reduce consequence
  - reduce likelihood