BAIT1093 Introduction to Computer Security

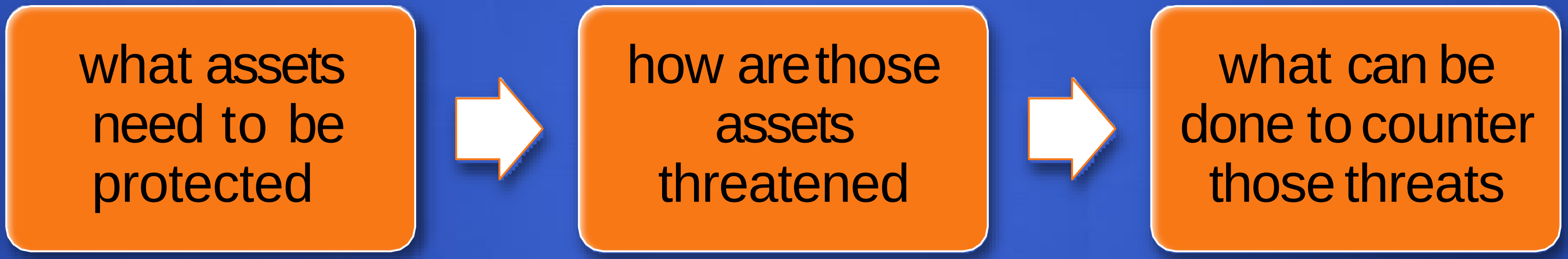
Chapter 7: IT Security Management and Risk Management

Topics

7.1 IT Security Management Overview
7.2 Organizational Context and Security Policy
7.3 Security Risk Assessment
7.4 Detailed Security Risk Analysis

7.1 IT Security Management Overview [1]

Formal process of answering the questions:


what assets need to be protected
how are those assets threatened
what can be done to counter those threats

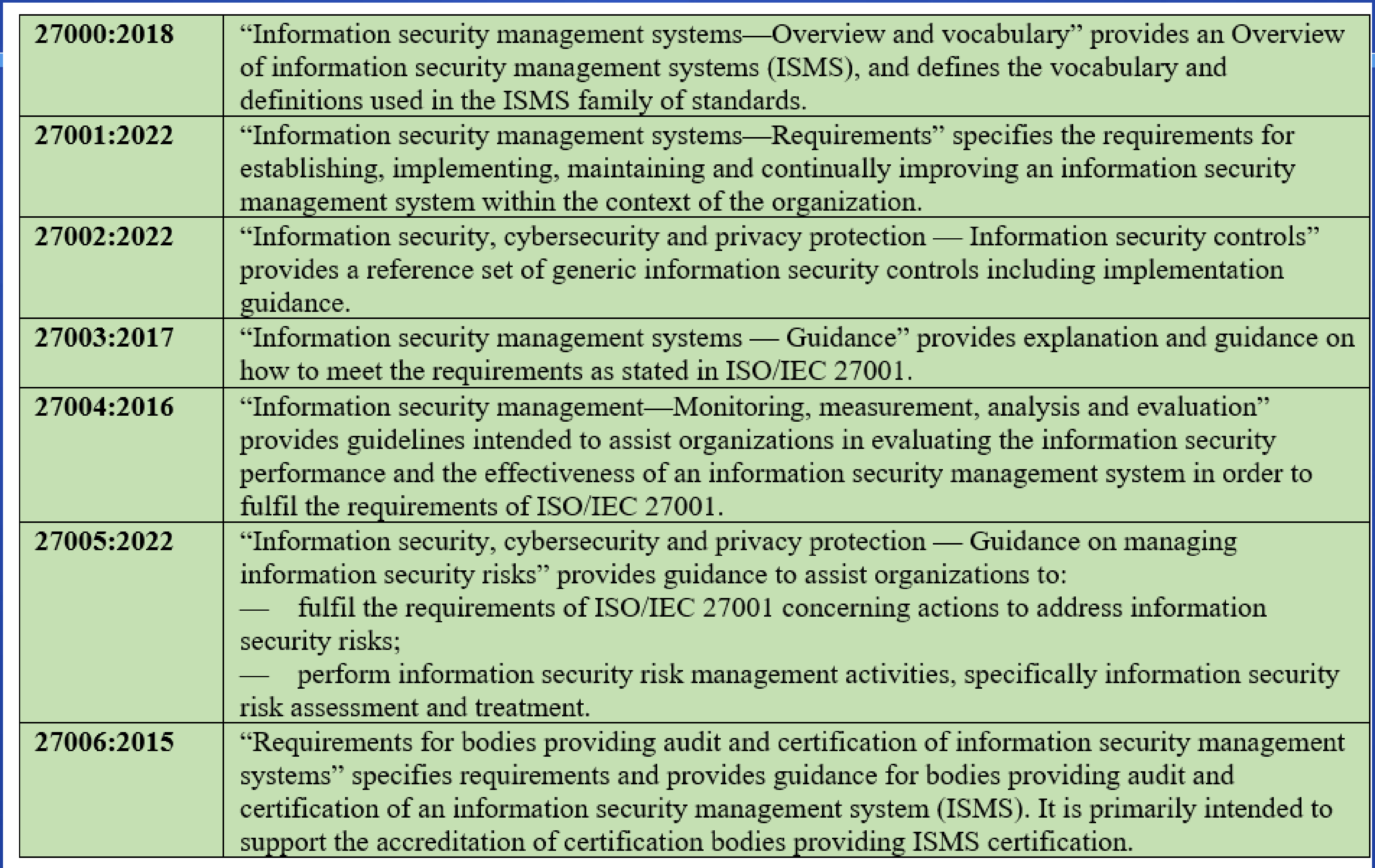
- ensures that critical assets are sufficiently protected in a cost-effective manner
- security risk assessment is needed for each asset in the organization that requires protection
- provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

7.1 IT Security Management Overview [1]

- The discipline of IT security management has evolved considerably, in response to the rapid growth of networked computer systems and the associated rise in risks to these systems.
- In the last decade, a number of national and international standards have been published. These represent a consensus on the best practice in the field.
- The International Standards Organization (ISO) has revised and consolidated a number of these standards into the ISO 27000 series.

7.1 IT Security Management Overview

ISO/IEC 27000 Series of Standards on IT Security Techniques (Source: https://www.iso.org/)



27000:2018	"Information security management systems—Overview and vocabulary" provides an Overview of information security management systems (ISMS), and defines the vocabulary and definitions used in the ISMS family of standards.
27001:2022	"Information security management systems—Requirements" specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
27002:2022	"Information security, cybersecurity and privacy protection — Information security controls" provides a reference set of generic information security controls including implementation guidance.
27003:2017	"Information security management systems — Guidance" provides explanation and guidance on how to meet the requirements as stated in ISO/IEC 27001.
27004:2016	"Information security management—Monitoring, measurement, analysis and evaluation" provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001.
27005:2022	"Information security, cybersecurity and privacy protection — Guidance on managing information security risks" provides guidance to assist organizations to: — fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks; — perform information security risk management activities, specifically information security risk assessment and treatment.
27006:2015	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS). It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

7.1 IT Security Management Overview [1]

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

7.1 IT Security Management Overview [1]

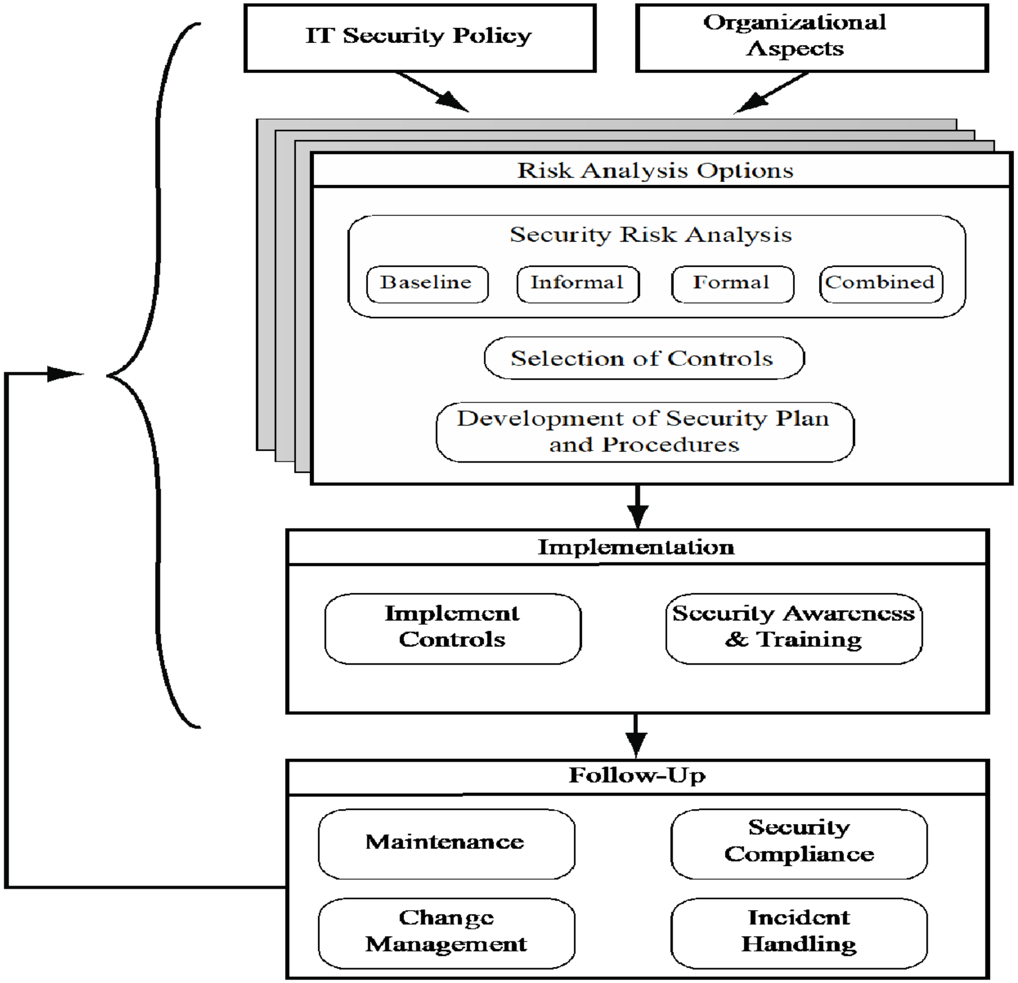


Figure 14.1 Overview of IT Security Management

focus on the internal details relating to the **risk assessment** process

7.1 IT Security Management Overview [1]

- IT management is not something undertaken just once. Rather it is a cyclic process that must be repeated constantly in order to keep pace with the rapid changes in both IT technology and the risk environment.
- The iterative nature of this process is a key focus of [ISO27001], and is specifically applied to the security risk management process in [ISO27005].

7.1 IT Security Management Overview [1]

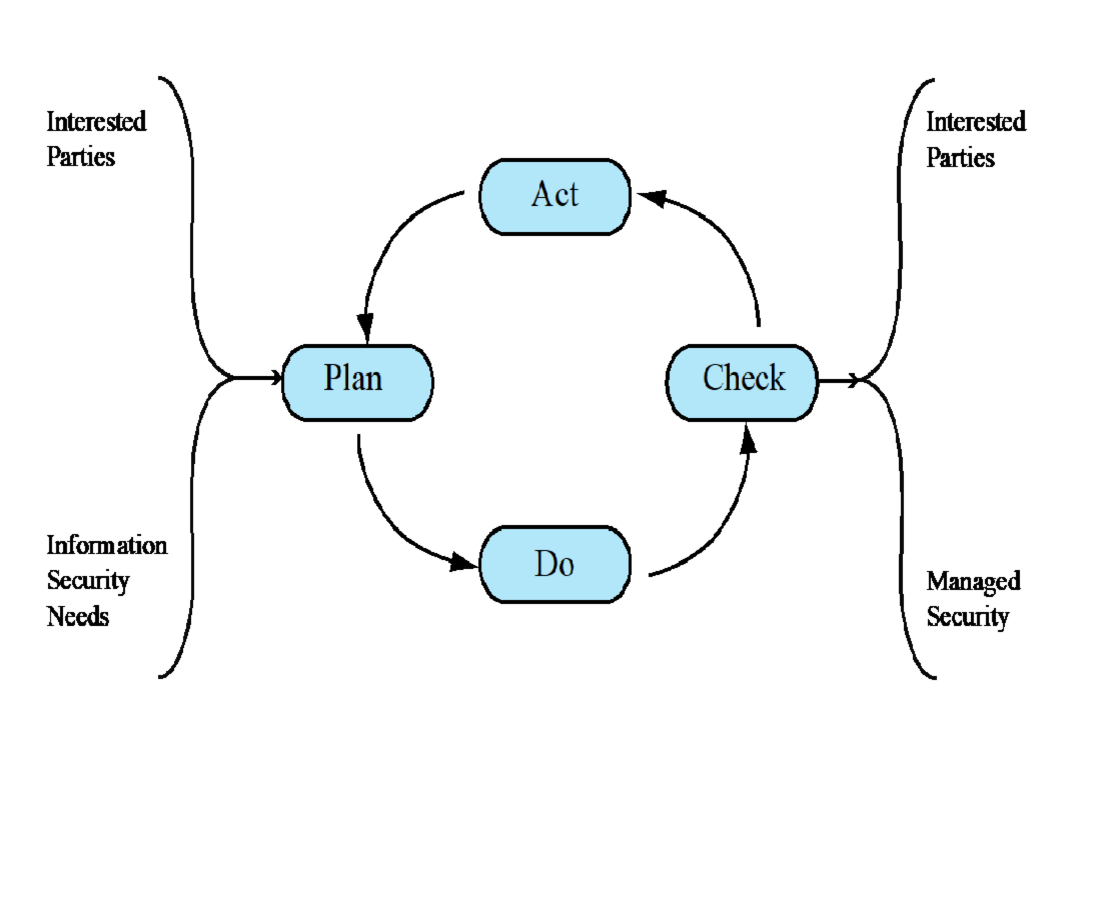


Figure 14.2 The Plan - Do - Check - Act Process Model

This standard details a model process for managing information security that comprises the following steps:

1) **Plan: establish security policy, objectives, processes and procedures;** perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.

2) **Do: implement the risk treatment plan.**

3) **Check: monitor and maintain the risk treatment plan.**

4) **Act: maintain and improve the information security risk management** process in response to incidents, review, or identified changes.

7.1 IT Security Management Overview [1]

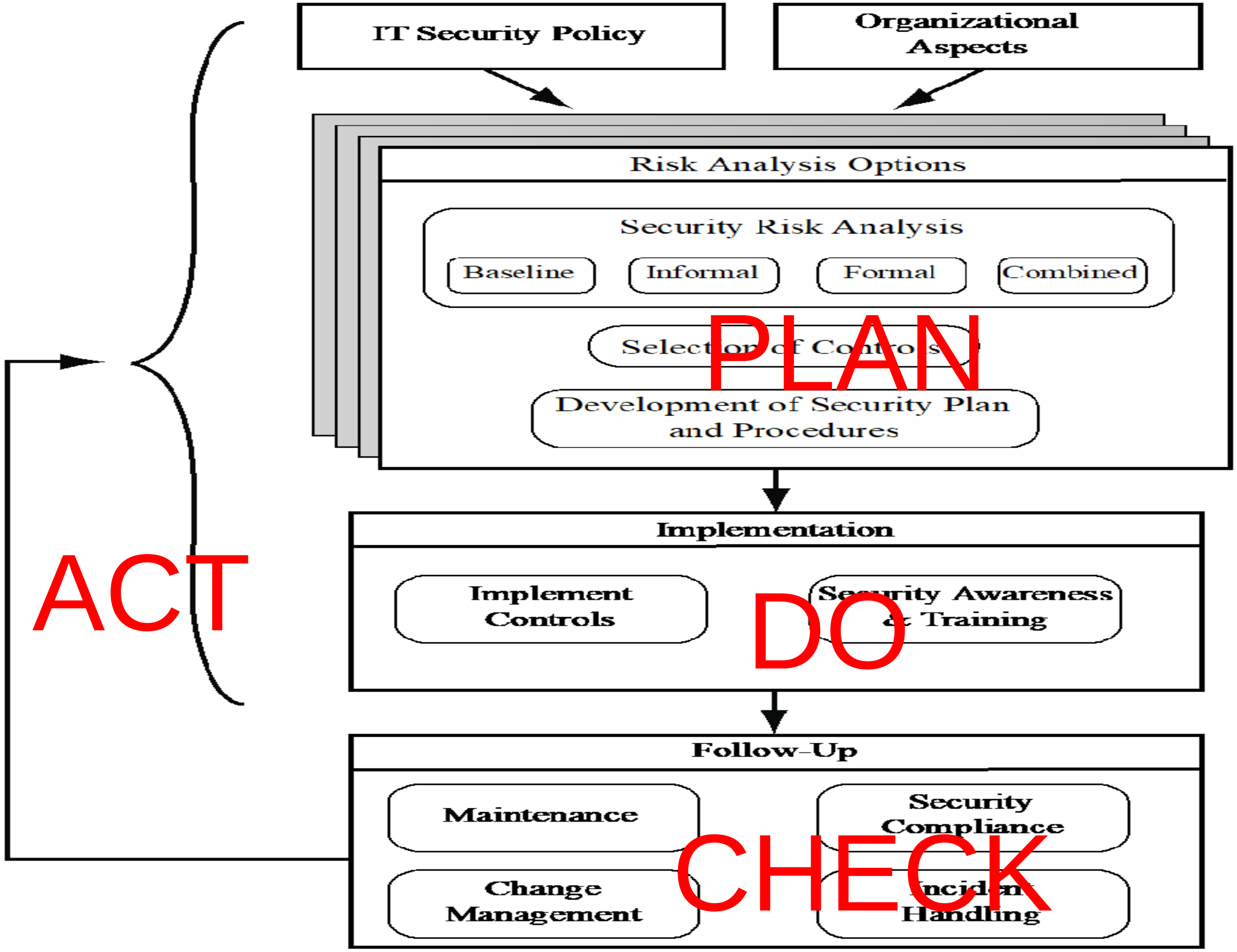


Figure 14.1 Overview of IT Security Management

7.2 Organizational Context and Security Policy [1]

first examine organization's IT security:

objectives - IT security outcomes to be achieved

strategies - how to meet objectives

policies - identify what needs to be done

- maintained and updated regularly
  - periodic security reviews
  - reflect changing technical/ risk environments
- examine role and importance of IT systems in organization

7.2 Organizational Context and Security Policy [1]

Security Policy

Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements (confidentiality, integrity, availability,
- accountability, authenticity, and reliability)
- 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

7.2 Organizational Context and Security Policy [1]

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 IT security 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

7.3 Security Risk Assessment [1]

Critical component of IT security 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

7.3 Security Risk Assessment [1]

Baseline Approach

- Aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and industry best practice.
- The goal of the baseline approach is to implement generally agreed controls to provide protection against the most common threats.
- The baseline approach forms a good base from which further security measures can be determined.

7.3 Security Risk Assessment [1]

Baseline Approach

- Advantage:
  - does not require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems.
- Disadvantage:
  - no special consideration is given to variations in the organization’s risk exposure based on who they are and how their systems are used.
  - there is a chance that the baseline level may be set either too high or too low

7.3 Security Risk Assessment [1]

Baseline Approach

- Suitable baseline recommendations and checklists may be obtained from a range of organizations, including:
  - Various national and international standards organizations
  - Security-related organizations such as the CERT, NSA, and so on
  - Industry sector councils
- The use of the baseline approach alone would generally be recommended only for small organizations without the resources to implement more structured approaches.

7.3 Security Risk Assessment [1]

Informal Approach

- involves conducting some form of informal, pragmatic risk analysis for the organization’s IT systems.
- does not involve the use of a formal, structured process, but rather exploits the knowledge and expertise of the individuals performing this analysis.
- These may either be internal experts, if available, or, alternatively, external consultants.

7.3 Security Risk Assessment [1]

Informal Approach

- Advantages:
  - No additional skills is required while performing the analysis
  - Can be performed quickly and cheaply.
  - Organization’s systems are being examined, specific vulnerabilities and risks are identified → more accurate and targeted controls may be used where baseline approach would not address.
- Disadvantages:
  - some risks may not be considered appropriately, potentially leaving the organization vulnerable
  - results may be skewed or inconsistent by the views and prejudices of the individuals performing the analysis → not justifying the proposed expenditure for suggested controls

7.3 Security Risk Assessment [1]

Informal Approach

- The use of the informal approach would generally be recommended for small to medium-sized organizations where the IT systems are not necessarily essential to meeting the organization’s business objectives and where additional expenditure on risk analysis cannot be justified.

7.3 Security Risk Assessment [1]

Detailed Risk Analysis

- conduct a detailed risk assessment of the organization’s IT systems, using a formal structured process. ← most comprehensive approach
- involves a number of stages
  - identification of assets
  - identification of threats and vulnerabilities to those assets
  - determination of the likelihood of the risk occurring + the consequences → the risk the organization is exposed to
- Appropriate controls → to address the risks identified.

7.3 Security Risk Assessment [1]

Detailed Risk Analysis

- Advantages:
  - More detailed examination of the security risks of an organization’s IT system
  - Provides strong justification for expenditure on the controls to be implemented
  - It also provides the best information for continuing to manage the security of these systems as they evolve and change

7.3 Security Risk Assessment [1]

Detailed Risk Analysis

- Disadvantages:
  - Involve significant cost in time, resources, and expertise
  - May also result in delays in providing suitable levels of protection
- is often a legal requirement for some government organizations and businesses providing key services to them.
- for organizations providing key national infrastructure.
- for large organizations with IT systems critical to their business objectives

7.3 Security Risk Assessment [1]

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

7.3 Security Risk Assessment [1]

Combined Approach

- 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

7.3 Security Risk Assessment [1]

Combined Approach

- Advantages:
  - initial high-level analysis to determine where further resources need to be expended, rather than facing a full detailed risk analysis of all systems → easier to convince management.
  - The use of the baseline and informal analyses ensures that a basic level of security protection is implemented early
  - Most cost effective and therefore, highly recommended

7.3 Security Risk Assessment [1]

Combined Approach

- Disadvantages:
  - If the initial high-level analysis is inaccurate, then some systems for which a detailed risk analysis should be performed may remain vulnerable for some time. Nonetheless, the use of the baseline approach should
  - ensure a basic minimum security level on such systems.

7.4 Detailed Security Risk Analysis [1]

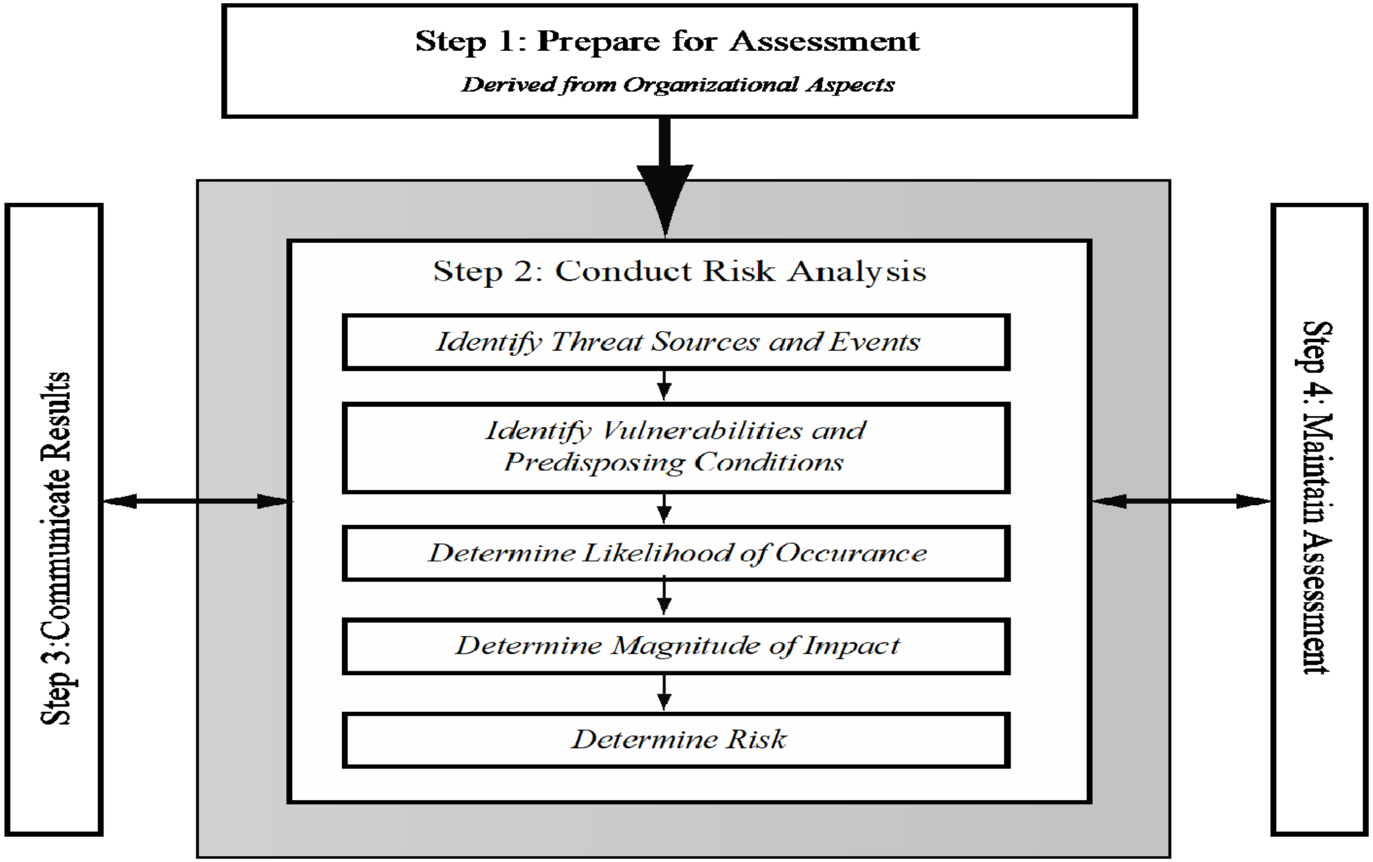

Step 1: Prepare for Assessment
Derived from Organizational Aspects
Step 2: Conduct Risk Analysis
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurance
Determine Magnitude of Impact
Determine Risk
Step 3:Communicate Results
Step 4: Maintain Assessment

Figure 14.3 Risk Assessment Process

7.4 Detailed Security Risk Analysis [1]

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

7.4 Detailed Security Risk Analysis [1]

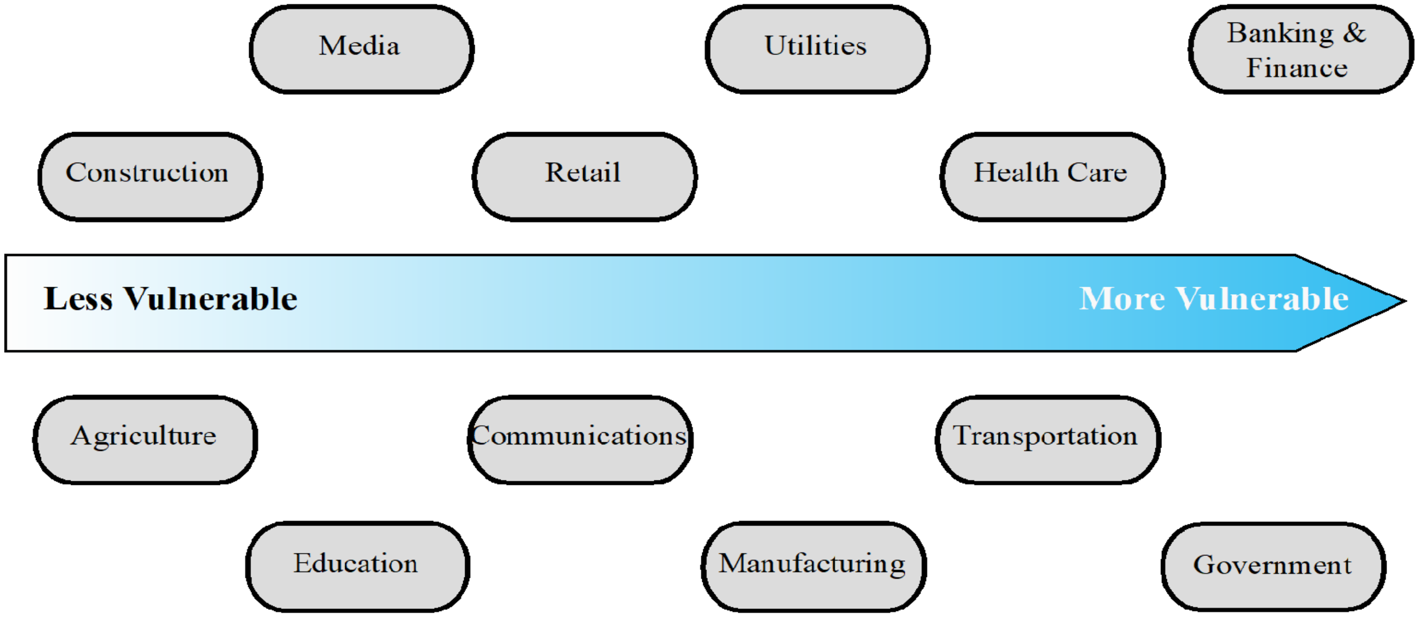


Figure 14.4 Generic Organizational Risk Context

7.4 Detailed Security Risk Analysis [1]

Asset Identification

- Last component of the first step 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

“anything that needs to be protected” because it has value to the organization and contributes to the successful attainment of the organization’s objectives

7.4 Detailed Security Risk Analysis [1]

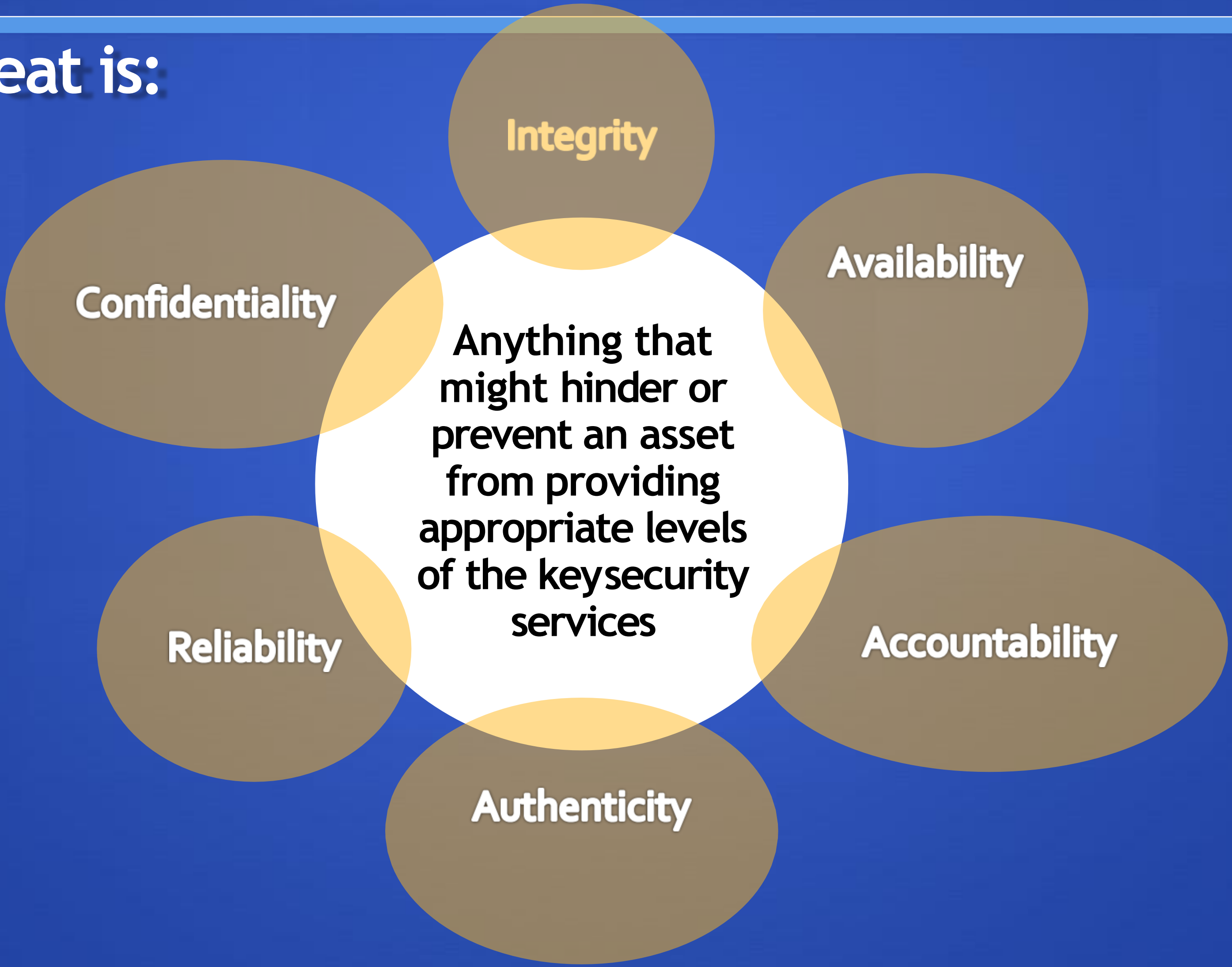
Terminology

- Asset: A system resource or capability of value to its owner that requires protection
- Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat
- Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner

7.4 Detailed Security Risk Analysis [1]

Threat Identification

- A threat is:



Anything that might hinder or prevent an asset from providing appropriate levels of the keysecurity services

Integrity

Availability

Accountability

Authenticity

Reliability

Confidentiality

7.4 Detailed Security Risk Analysis [1]

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

7.4 Detailed Security Risk Analysis [1]

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems orprocesses
  - determines applicability and significance of threat to organization
- need combination of threat and vulnerability to create a risk to anasset
- outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

7.4 Detailed Security Risk Analysis [1]

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

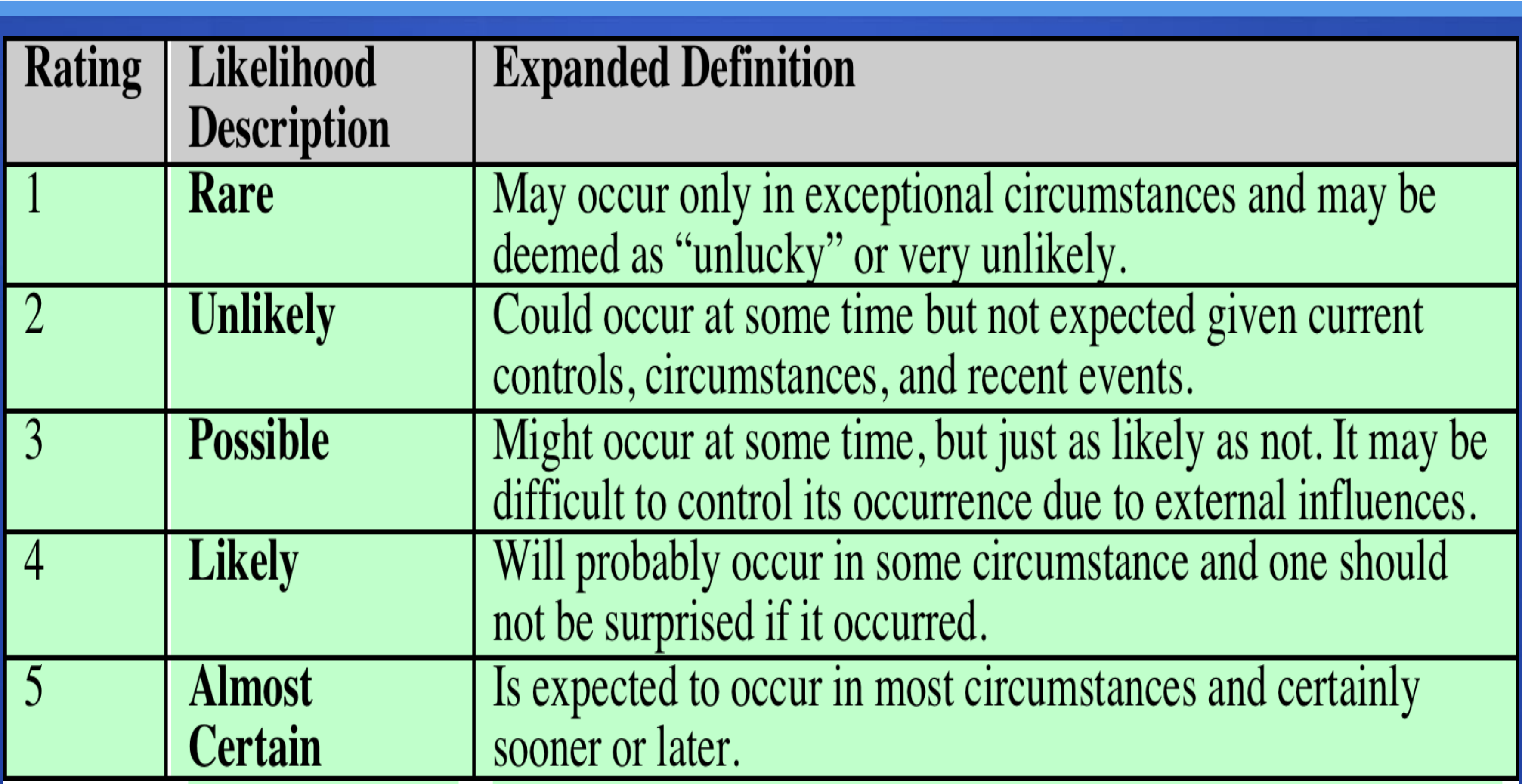
7.4 Detailed Security Risk Analysis [1]

Analyze Existing Controls

- existing controls used to attempt to minimize threats need to be identified
- security controls include (to be covered in detail in Chap 8):
  - management
  - operational
  - technical processes and procedures
- use checklists of existing controls and interview key organizational staff to solicit information

7.4 Detailed Security Risk Analysis [1]

Analyze Risks → 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

7.4 Detailed Security Risk Analysis [1]

Risk Consequence

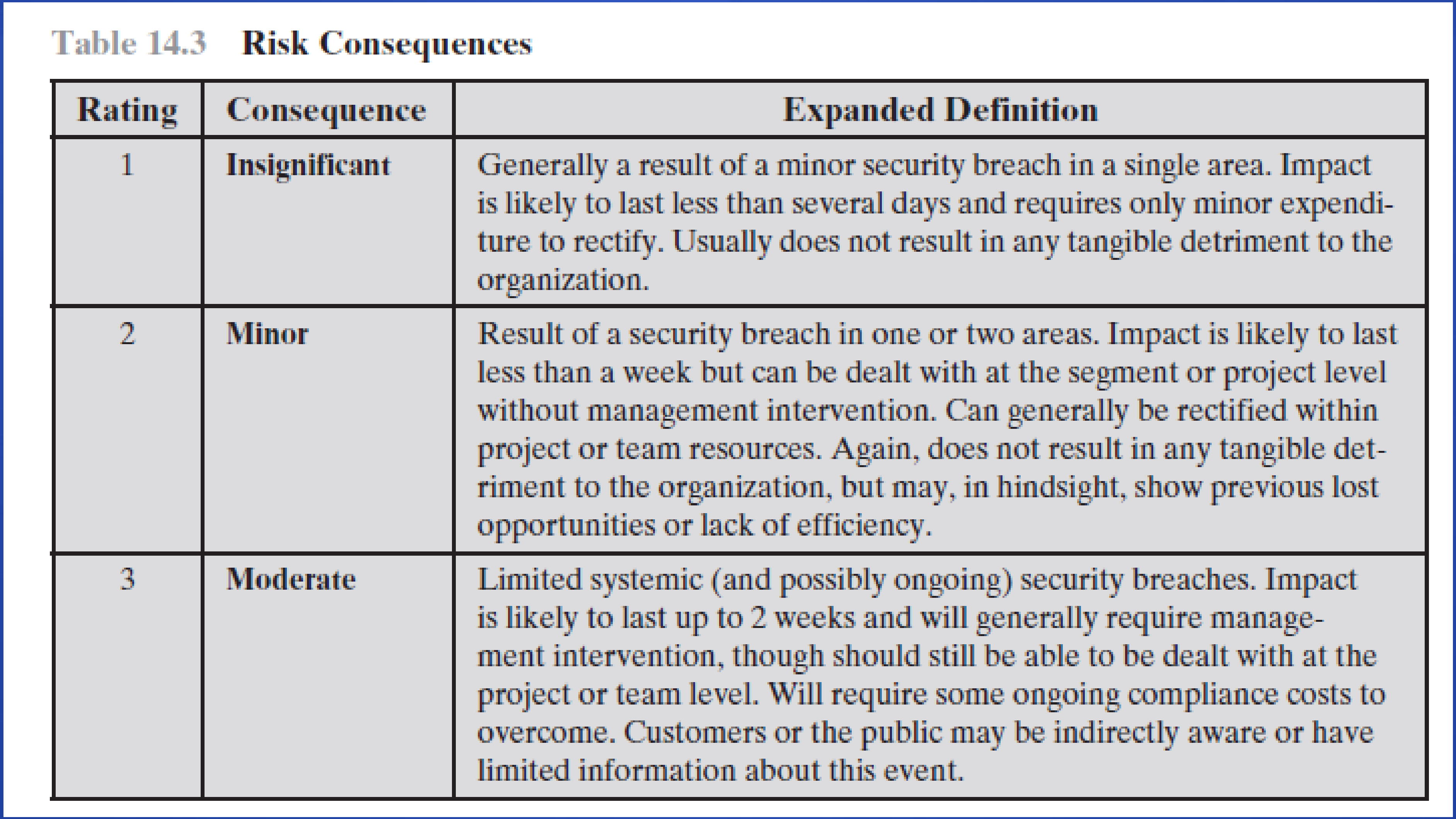


Table 14.3 **Risk Consequences**

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.

7.4 Detailed Security Risk Analysis [1]

Risk Consequence

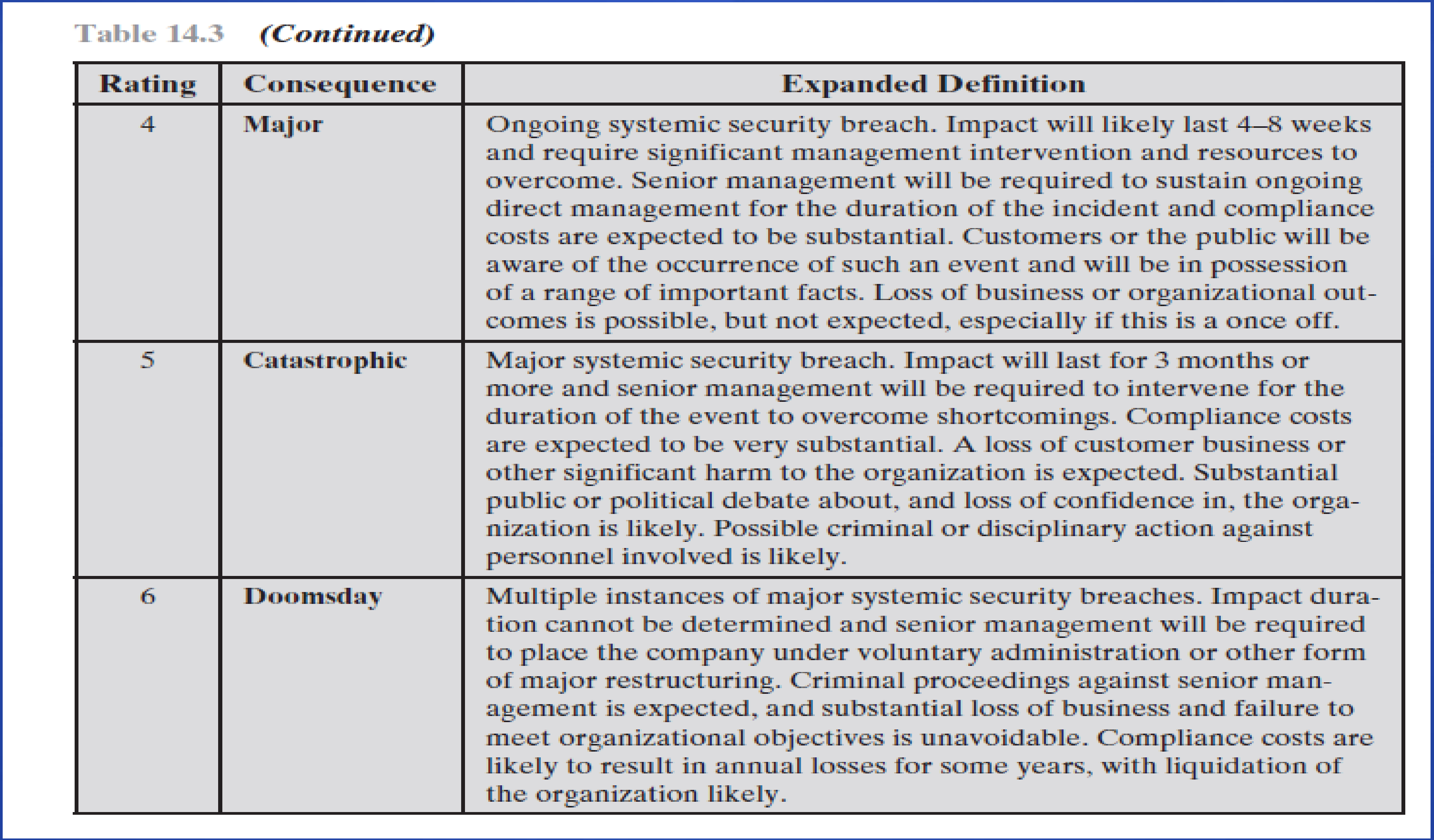
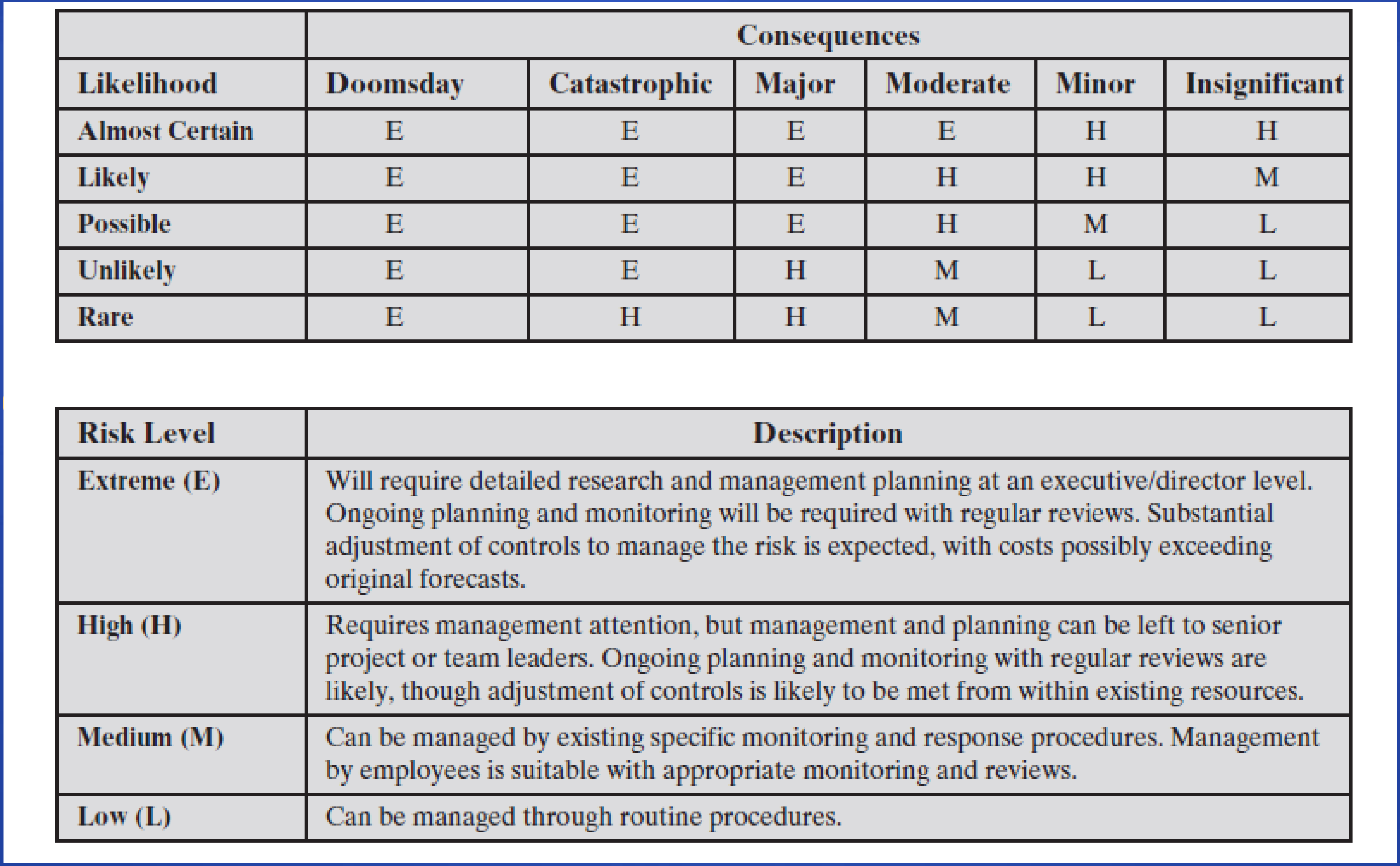


Table 14.3 *(Continued)*

Rating	Consequence	Expanded Definition
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.

7.4 Detailed Security Risk Analysis [1]

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 is 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 is 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.

7.4 Detailed Security Risk Analysis [1]

Risk Register

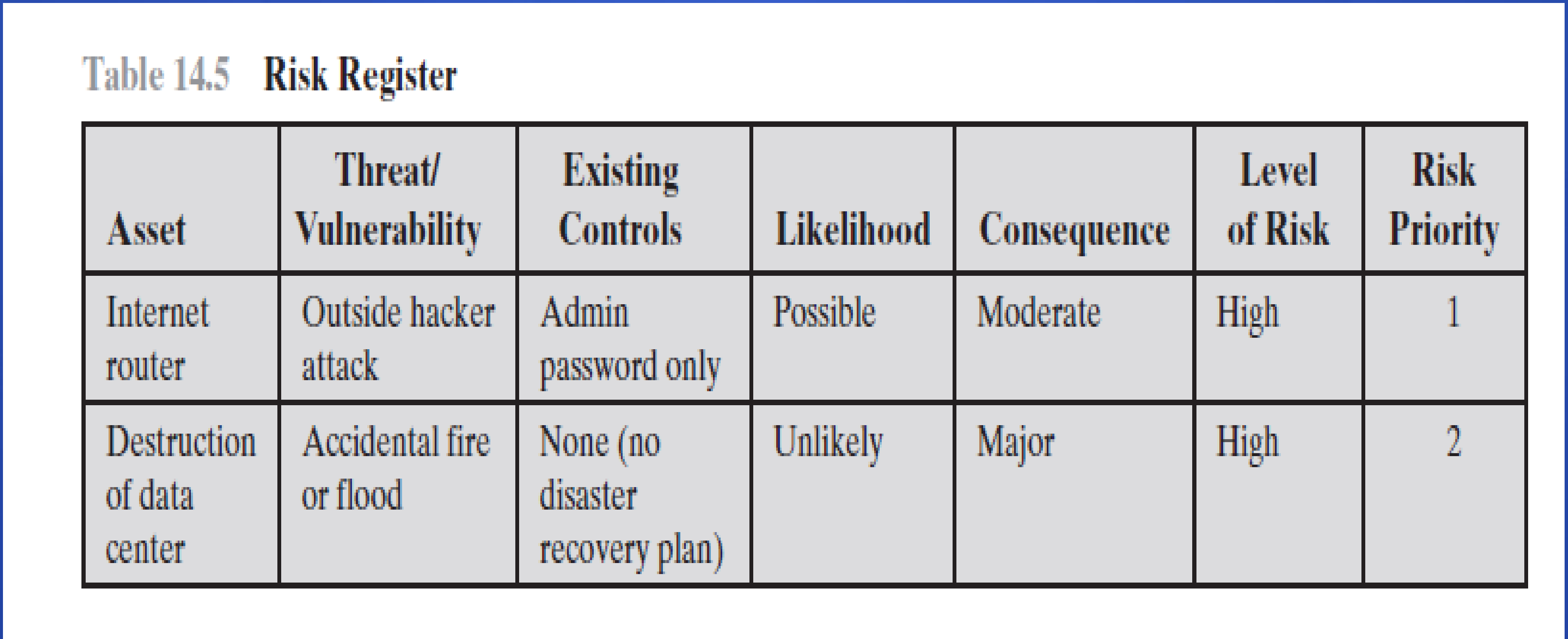


Table 14.5 **Risk Register**

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

7.4 Detailed Security Risk Analysis [1]

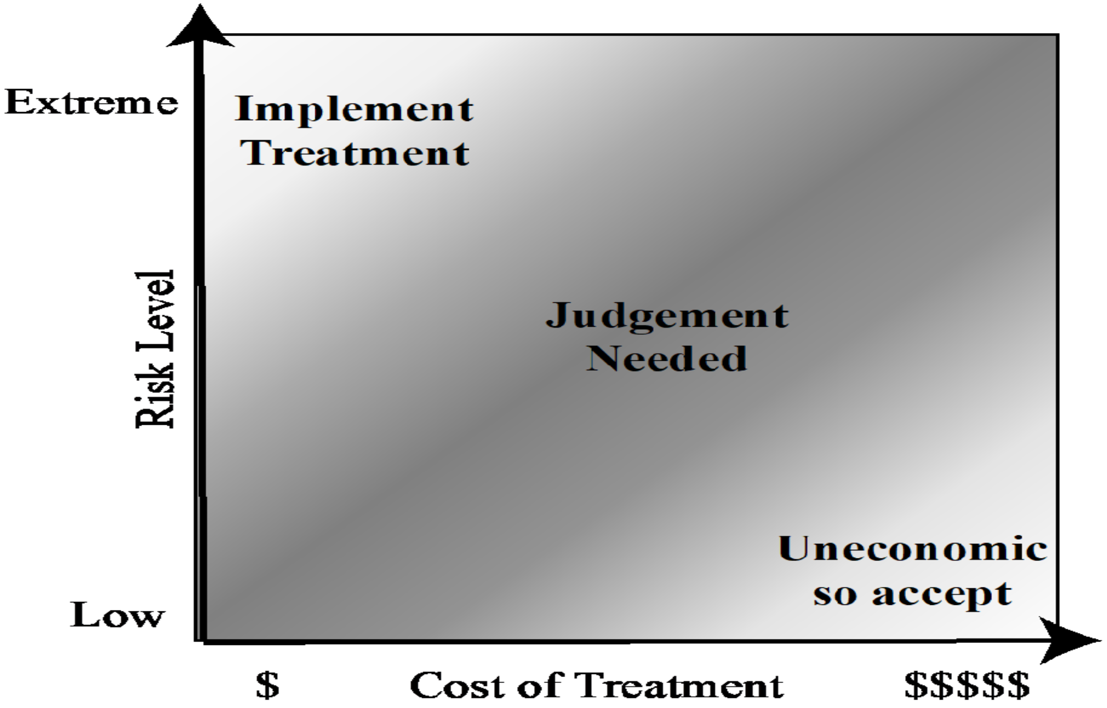
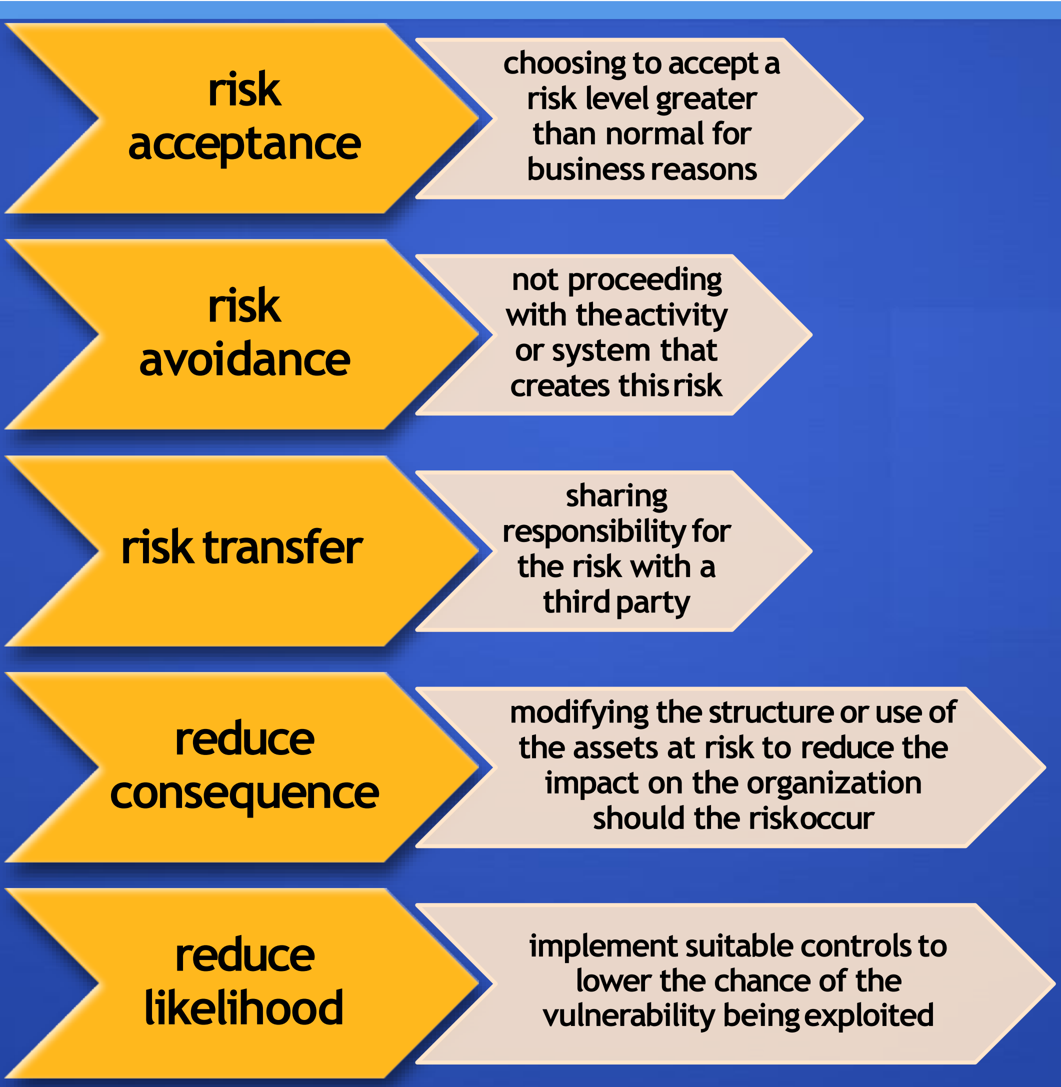


Figure 14.5 Judgment About Risk Treatment

7.4 Detailed Security Risk Analysis [1]

RiskTreatment Alternatives



risk acceptance

choosing to accept a risk level greater than normal for business reasons

risk avoidance

not proceeding with theactivity or system that creates thisrisk

risk transfer

sharing responsibility for the risk with a third party

reduce consequence

modifying the structure or use of the assets at risk to reduce the impact on the organization should the riskoccur

reduce likelihood

implement suitable controls to lower the chance of the vulnerability beingexploited

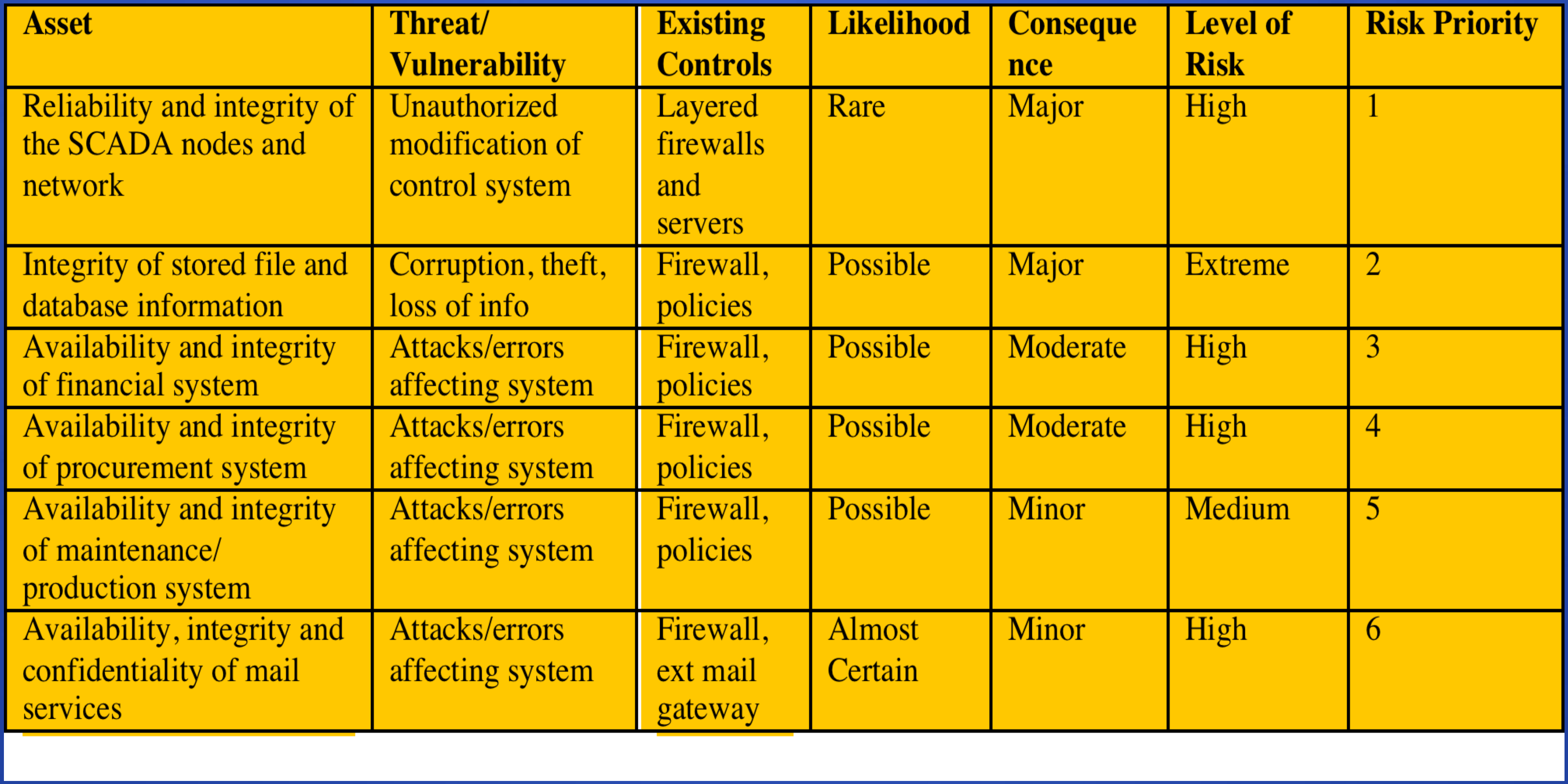
Case Study: Silver Star Mines

- 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

Main References

[1] William Stallings and Lawrie Brown. 2018. Computer Security: Principles and Practice. Pearson.