Information Security Management

Chapter 2
Planning for Security

Webster University
Scott Granneman

“You got to be careful
if you don’t know where you’re going,
because you might not get there.”

-- Yogi Berra

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

Recognize the importance of planning
& describe the principal components
of organizational planning

Know and understand
the principal components of
infosec system implementation planning
as it functions
within the organizational planning scheme

Successful organizations utilize planning.

Why?

Planning involves:

- ✓ Employees
- ✓ Management
- ✓ Stockholders
- ✓ Other outside stakeholders
- ✓ Physical environment
- ✓ Political and legal environment
- ✓ Competitive environment
- ✓ Technological environment

Planning:

Is creating action steps toward goals,
& then controlling them

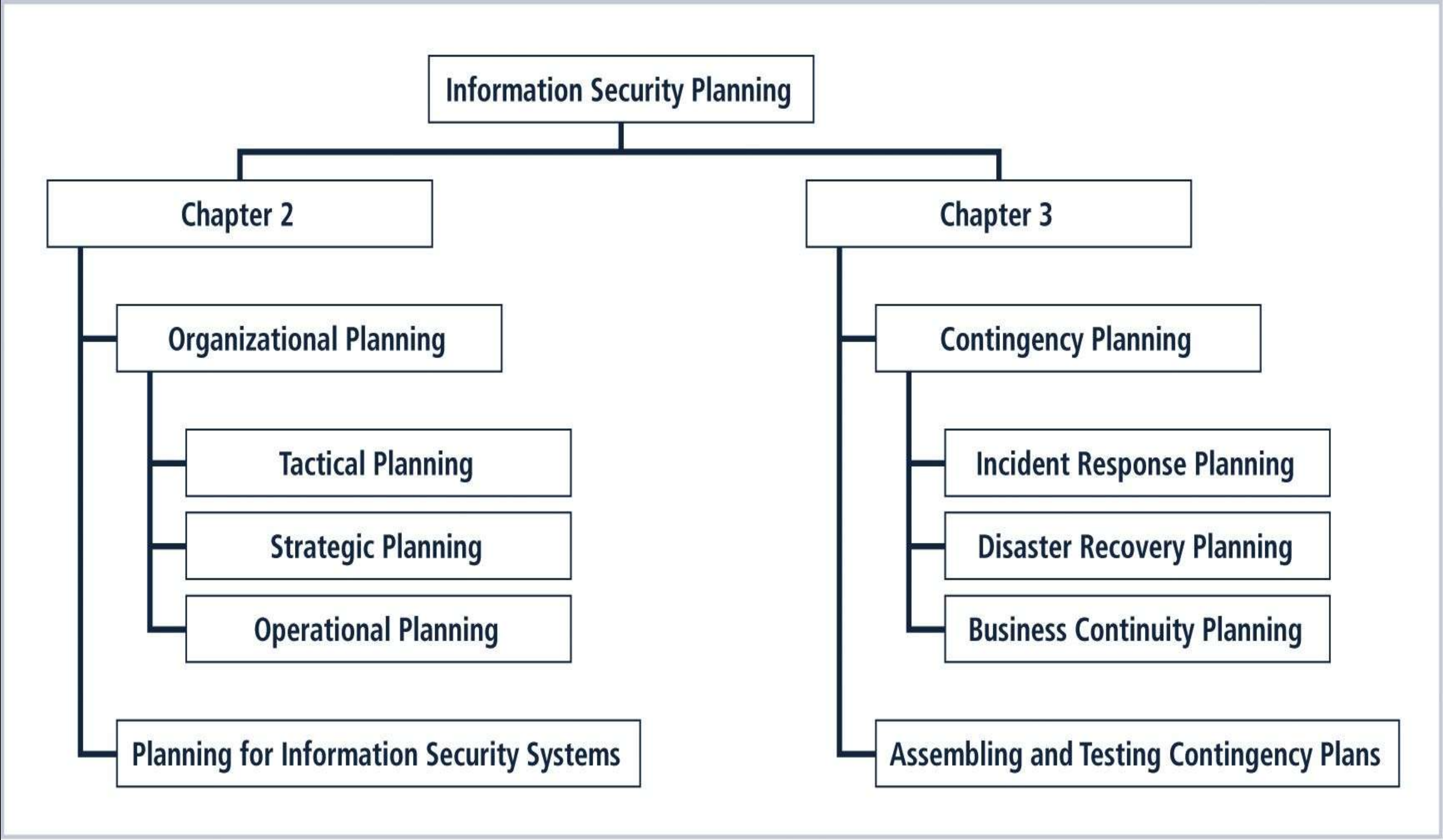
Provides direction
for the organization’s future

Top-down method of planning:

Organization’s leaders
choose the direction

Planning begins
with the general
& ends with the specific

InfoSec Planning



Information Security Planning

Chapter 2

Organizational Planning

Tactical Planning

Strategic Planning

Operational Planning

Planning for Information Security Systems

Chapter 3

Contingency Planning

Incident Response Planning

Disaster Recovery Planning

Business Continuity Planning

Assembling and Testing Contingency Plans

FIGURE 2-1 Information Security Planning

Strategic planning includes:

✓ Mission statement

✓ Vision statement

✓ Values statement

✓ Strategy

✓ Coordinated plans for sub units

Knowing how
the general org planning process works
helps in the
infosec planning process

Mission Statement

Declares the business of the organization
& its intended areas of operations

Explains what the organization does
& for whom

Example: Colostomo, Inc.
designs and manufactures
quality medical supplies
& associated equipment,
for use
in modern medical environments & homes

Vision statement

Expresses what the organization wants to become

Should be ambitious

Example: Colostomo
will be the preferred
manufacturer of choice
for every medical environment's
equipment needs,
with a Colostomo device
preferred by doctors & patients.

By establishing organizational principles
in a **values statement**,
an organization
makes its conduct standards clear.

“What do we put a premium on?
What drives us?”

Example: Colostomo values
commitment, honesty, integrity
& social responsibility among its employees,
& is committed to providing its services
in harmony with its corporate, social, legal,
& natural environments.

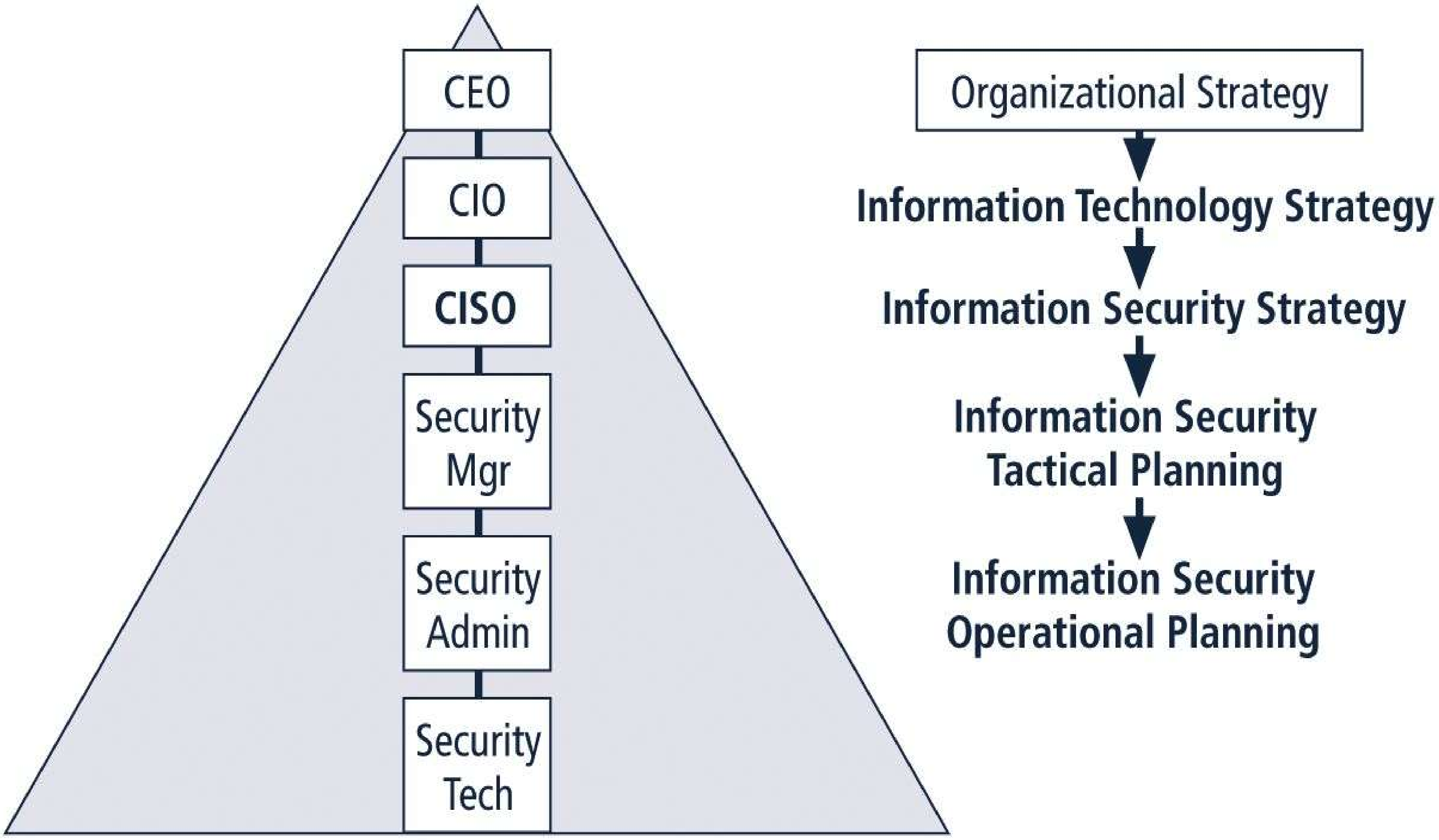
The mission,
vision,
& values statements
together
provide the foundation for planning

Strategy is the basis
for long-term direction

Strategic planning:

✓ Guides organizational efforts
✓ Focuses resources
on clearly defined goals

"… strategic planning
is a disciplined effort
to produce fundamental decisions & actions
that shape & guide what an organization is,
what it does, & why it does it,
with a focus on the future."



CEO

CIO

CISO

Security Mgr

Security Admin

Security Tech

Organizational Strategy

Information Technology Strategy

Information Security Strategy

Information Security Tactical Planning

Information Security Operational Planning

FIGURE 2-3 Top-Down Strategic Planning for Information Security

To plan, an organization:

✓ Develops a general strategy
✓ Creates specific strategic plans for major divisions

Each level of division translates those objectives into more specific objectives for the level below

In order to execute this broad strategy, executives must define individual managerial responsibilities

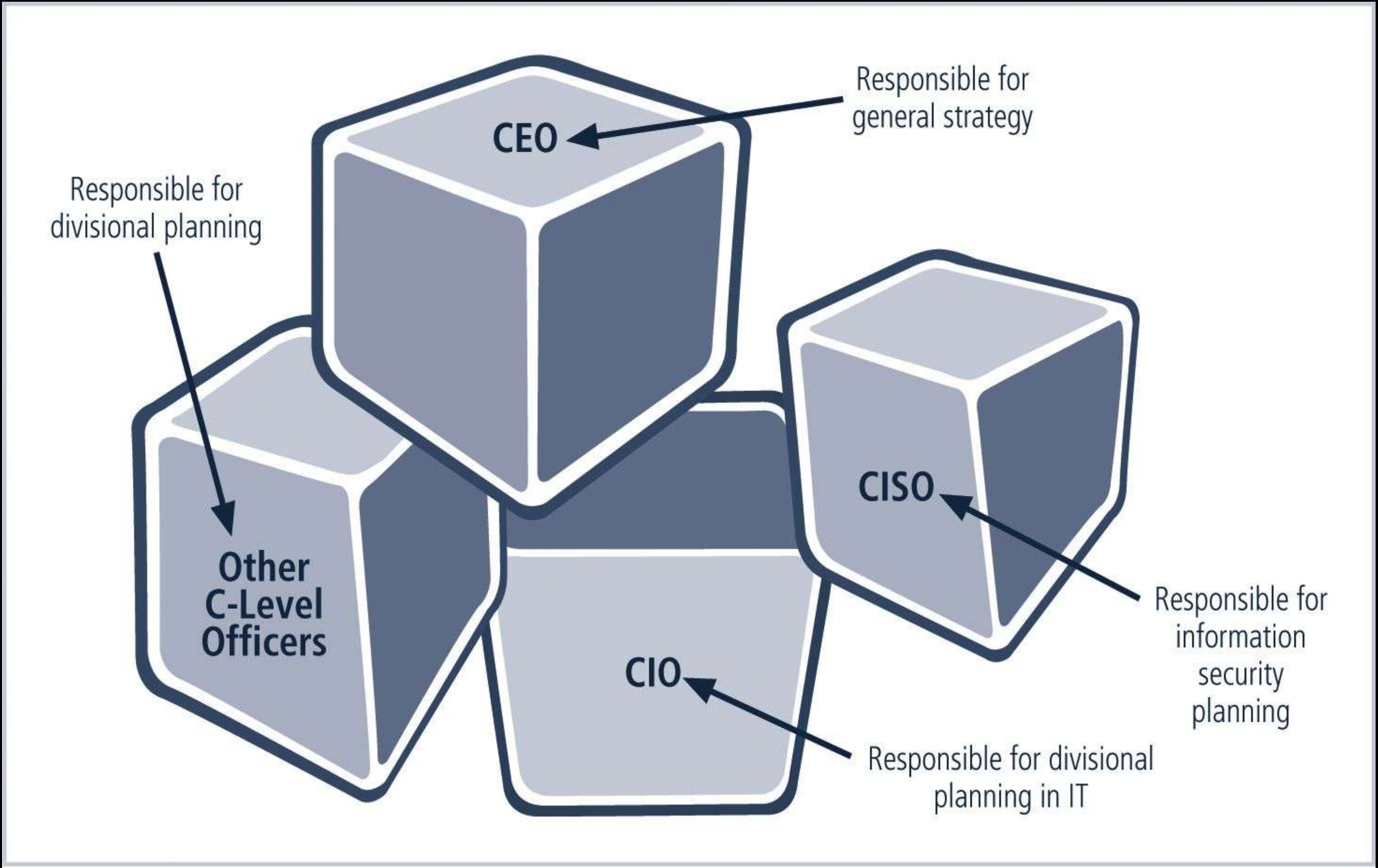

Responsible for general strategy
CEO
Responsible for divisional planning
Other C-Level Officers
CISO
Responsible for information security planning
CIO
Responsible for divisional planning in IT

FIGURE 2-4 Planning for the Organization

Strategic goals are then translated
into tasks with
specific,
measurable,
achievable,
reasonably high &
time-bound
objectives
(SMART)

Strategic planning then begins
a transformation from general
to specific objectives

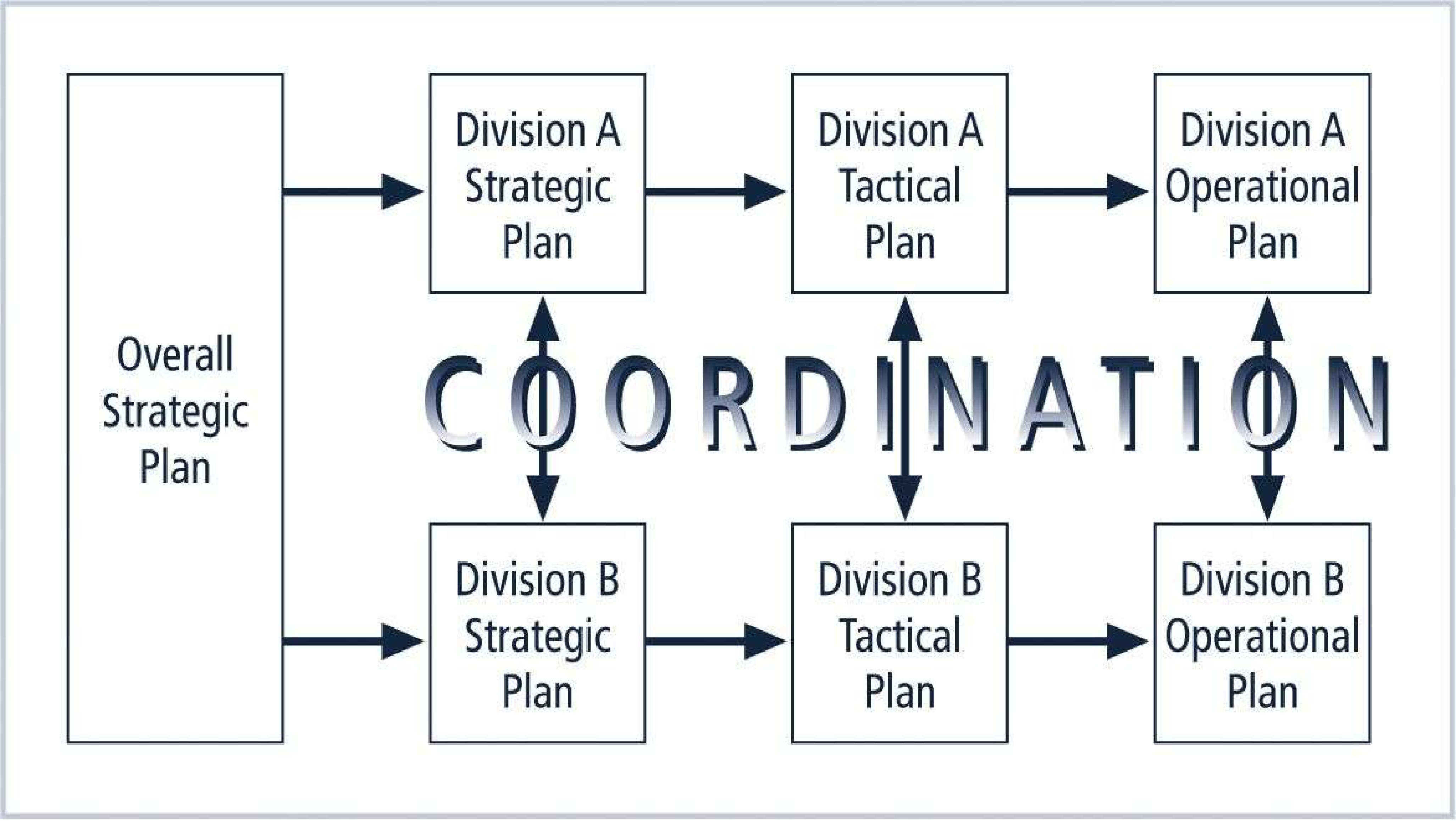

Overall Strategic Plan
Division A Strategic Plan
Division A Tactical Plan
Division A Operational Plan
COORDINATION
Division B Strategic Plan
Division B Tactical Plan
Division B Operational Plan

FIGURE 2-5 Planning Levels

Typical Strategic Plan Elements

✓ Introduction by senior executive
✓ Executive Summary
✓ Mission Statement & Vision Statement
✓ Organizational Profile & History
✓ Strategic Issues & Core Values
✓ Program Goals & Objectives
✓ Management/Operations Goals & Objectives

Appendices (optional):
strengths, **w**eaknesses, **o**pportunities and **t**hreats
(SWOT) analyses,
surveys, budgets, & so on

Tactical Planning

Shorter focus than strategic planning

Usually one to three years

Breaks applicable strategic goals
into a series of incremental objectives

So what is it?

If strategic planning determines
where I want to go,
tactical planning determines
the best steps used to get there.

Operational Planning

Used by managers & employees
to organize the
ongoing, day-to-day performance of tasks

Includes
clearly identified coordination activities
across department boundaries such as:

✓ Communications requirements
✓ Weekly meetings
✓ Summaries
✓ Progress reports

Strategic plan:
Take that hill by Monday night.

Tactical plan:
Call in an airstrike
& then attack from the south
with 10 men.

Operational plan:
Check the weather forecast.
Test the radio. Replenish ammunition.
Get rations.

Tips for planning:

✓ Create a compelling vision statement
that frames the evolving plan,
& acts as a magnet for people
who want to make a difference

✓ Embrace the use
of balanced scorecard approach
(everyone judges using the same measures)

✓ Deploy a draft high level plan early,
& ask for input from stakeholders
in the organization

✓ Make the evolving plan visible

More tips for planning
(or for having a good meeting ☺):

✓ Make the process invigorating for everyone

✓ Be persistent

✓ Make the process continuous

✓ Provide meaning

✓ Be yourself

✓ Lighten up & have some fun

Planning for InfoSec Implementation

The CIO & CISO play important roles
in translating overall strategic planning
into tactical and operational
infosec plans & information security

CISO plays a more active role
in the development
of the planning details
than does the CIO

CISO Job Description

✓ Creates strategic infosec plan
with a vision for the future of infosec at Company X

✓ Understands fundamental business activities
performed by Company X

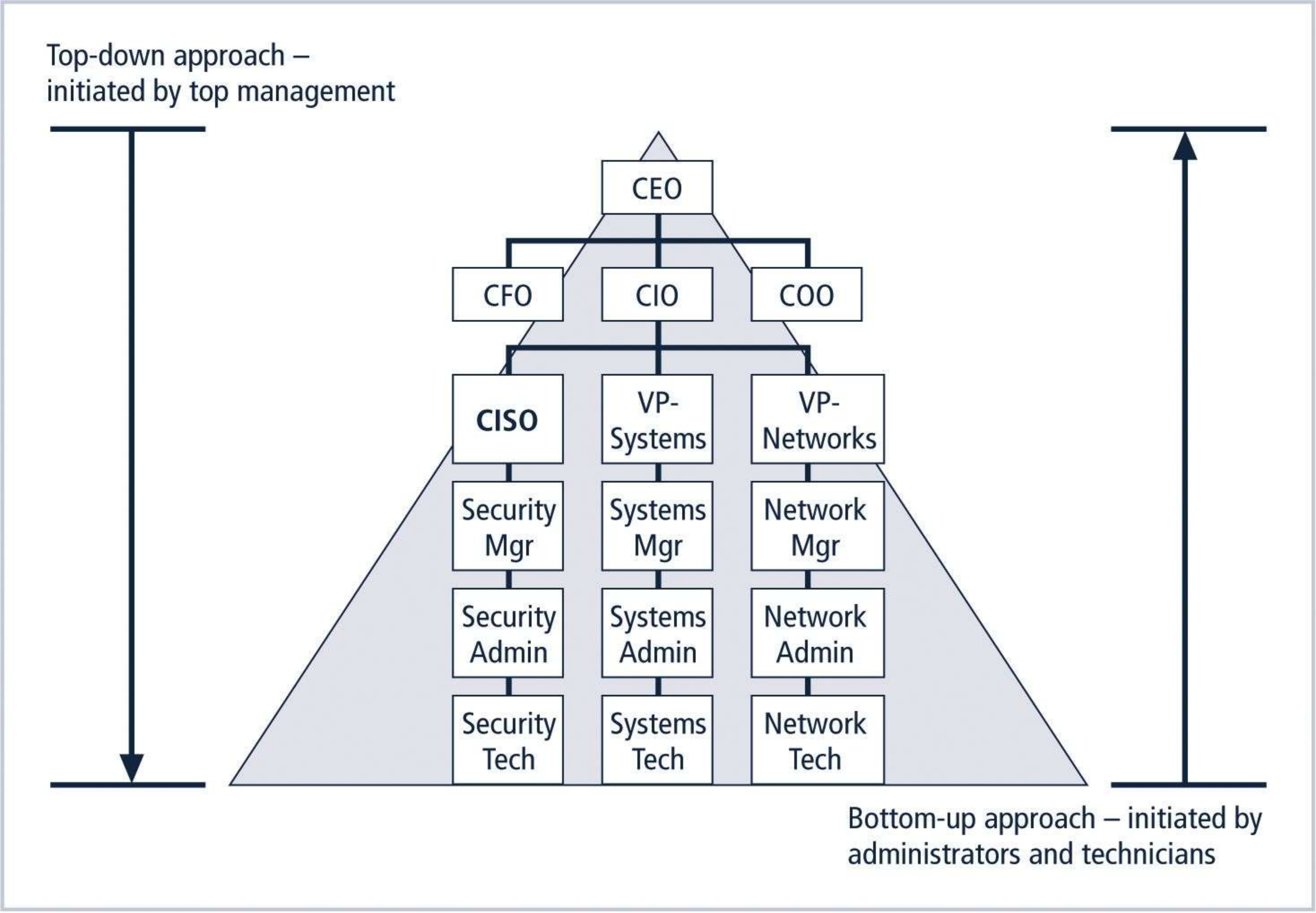
✓ Based on this understanding,
suggests appropriate infosec solutions
that uniquely protect these activities

✓ Develops action plans, schedules, status reports,
budgets, & other top management communications
intended to improve
the status of infosec at Company X

Once plan has been translated
into IT and infosec objectives
& tactical & operational plans infosec,
implementation can begin

Implementation of information security
can be accomplished in two ways:

Bottom-up OR Top-down



Top-down approach – initiated by top management

CEO

CFO

CIO

COO

CISO

VP-Systems

VP-Networks

Security Mgr

Systems Mgr

Network Mgr

Security Admin

Systems Admin

Network Admin

Security Tech

Systems Tech

Network Tech

Bottom-up approach – initiated by administrators and technicians

FIGURE 2-7 Approaches to Security Implementation

The Systems Development Life Cycle (SDLC)

A methodology
for the design & implementation
of an information system

SDLC-based projects may be
initiated by events or planned

At the end of each phase,
a review occurs
– a **feasibility analysis** –
when reviewers determine
if the project should be continued,
discontinued, outsourced, or postponed.

Assess various approaches
to understand
the economic, technical, & bahavioral
feasibility of the process to be performed.

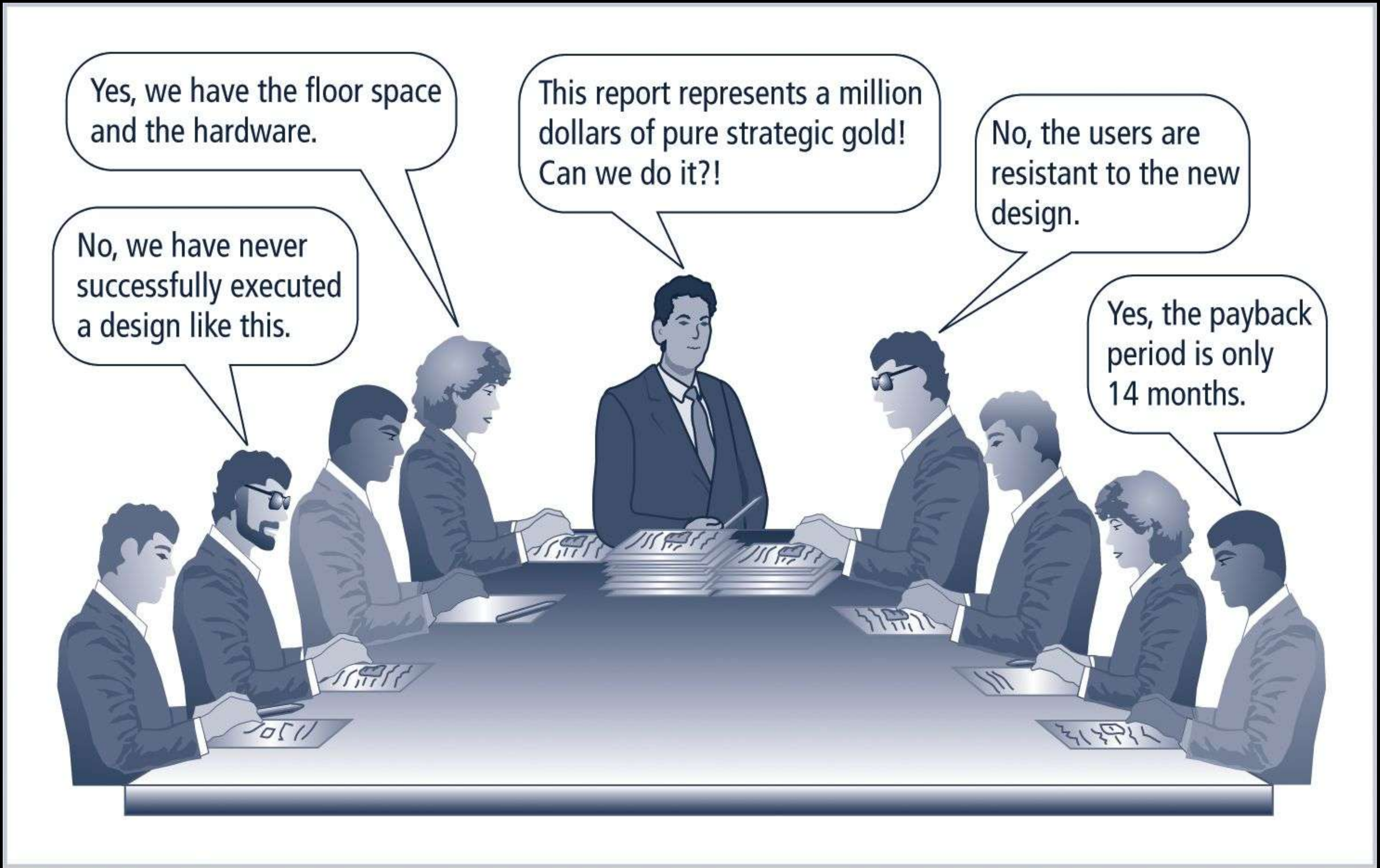
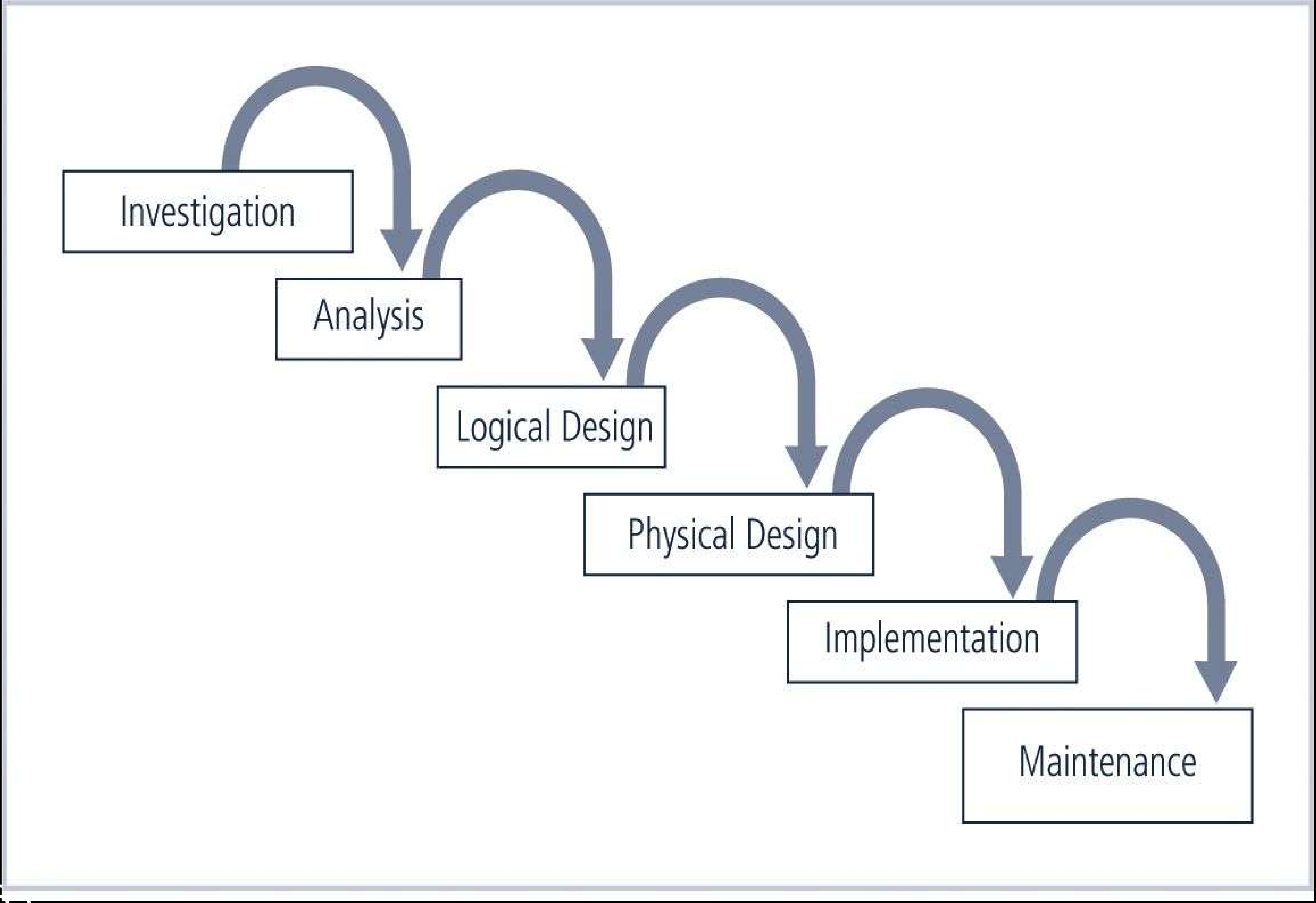

Yes, we have the floor space and the hardware.
No, we have never successfully executed a design like this.
This report represents a million dollars of pure strategic gold! Can we do it?!
No, the users are resistant to the new design.
Yes, the payback period is only 14 months.

FIGURE 2-8 Feasibility Analysis

Phases of An SDLC



1: Investigation

Identifies problem to be solved

Begins with the
objectives, constraints, & scope
of the project

A preliminary cost/benefit analysis
is developed to evaluate
perceived benefits & appropriate costs
for those benefits

2: Analysis

Begins with information
from the Investigation phase

Assesses the organization’s readiness,
its current systems status,
& its capability to implement & then support
the proposed system(s)

Analysts determine
what the new system is expected to do,
& how it will interact with existing systems

3: Logical Design

Information obtained from analysis phase
is used to create a proposed solution
for the problem

A system and/or application
is selected based on the business need

The logical design is the
implementation independent blueprint
for the desired solution

4: Physical Design

During the physical design phase,
the team selects specific technologies

The selected components
are evaluated further
as a make-or-buy decision

A final design is chosen
that optimally integrates
required components

5: Implementation

Develop any software that is not purchased,
& create integration capability

Customized elements
are tested & documented

Users are trained
& supporting documentation is created

Once all components
have been tested individually,
they are installed & tested as a whole

6: Maintenance

Tasks necessary to support & modify
the system for the remainder of its useful life

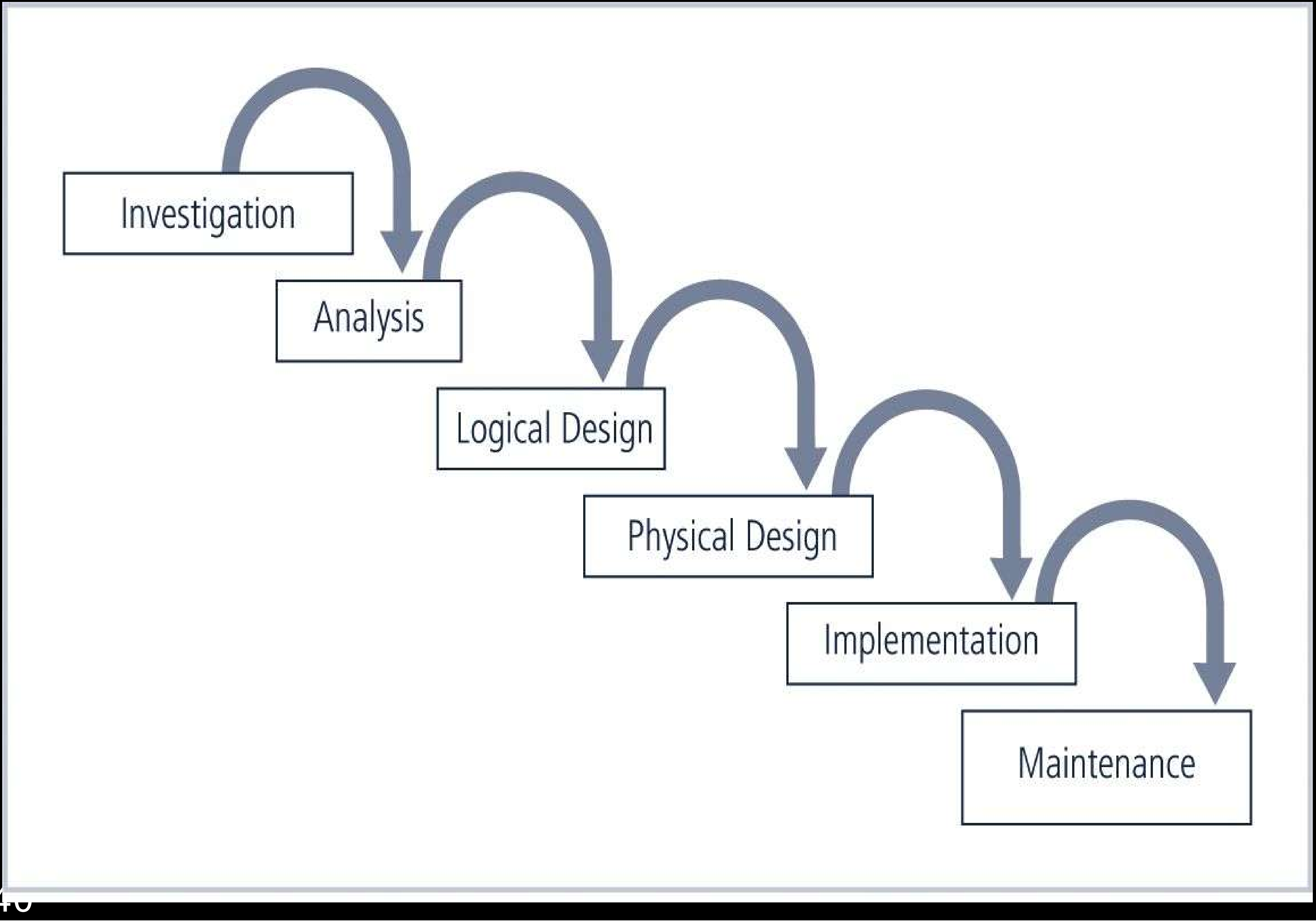
System is tested periodically
for compliance with specifications

Feasibility of
continuance versus discontinuance
is evaluated

Upgrades, updates, & patches are managed

When current system
can no longer support the organization’s mission,
it’s terminated &
a new systems development project is undertaken

To review … Phases of An SDLC



Security Systems Development Life Cycle (SecSDLC)

May differ in several specifics,
but overall methodology is similar to SDLC

SecSDLC process involves:

✓ Identification of specific threats
& the risks that they represent

✓ Subsequent design & implementation
of specific controls to counter those threats
& assist in the management of the risk
those threats pose to the organization

1. SecSDLC: Investigation

Often begins as directive from management
specifying the process, outcomes, & goals
of the project and its budget

Frequently begins with
the affirmation or creation of security policies

Teams assemble to analyze problems,
define scope, specify goals, & identify constraints

Feasibility analysis determines
whether the organization has
resources & commitment
to conduct a successful security analysis & design

2. SecSDLC: Analysis

A preliminary analysis
of existing security policies or programs
is prepared along with
known threats & current controls

Includes an analysis of
relevant legal issues
that could affect the design
of the security solution

Risk management begins in this stage

Risk Management: process of identifying, assessing, & evaluating levels of risk facing the organization

Specifically, the threats to the information stored and processed by the organization

To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations

In this context, a threat is an object, person, or other entity that represents a constant danger to an asset

Some key terms

Attack: deliberate act that exploits
a vulnerability to achieve
the compromise of a controlled system

Accomplished by a **threat agent**
that damages or steals
an organization’s information or physical asset

Exploit: technique or mechanism
used to compromise a system

Vulnerability: identified weakness
of a controlled system
in which necessary controls
are not present or are no longer effective

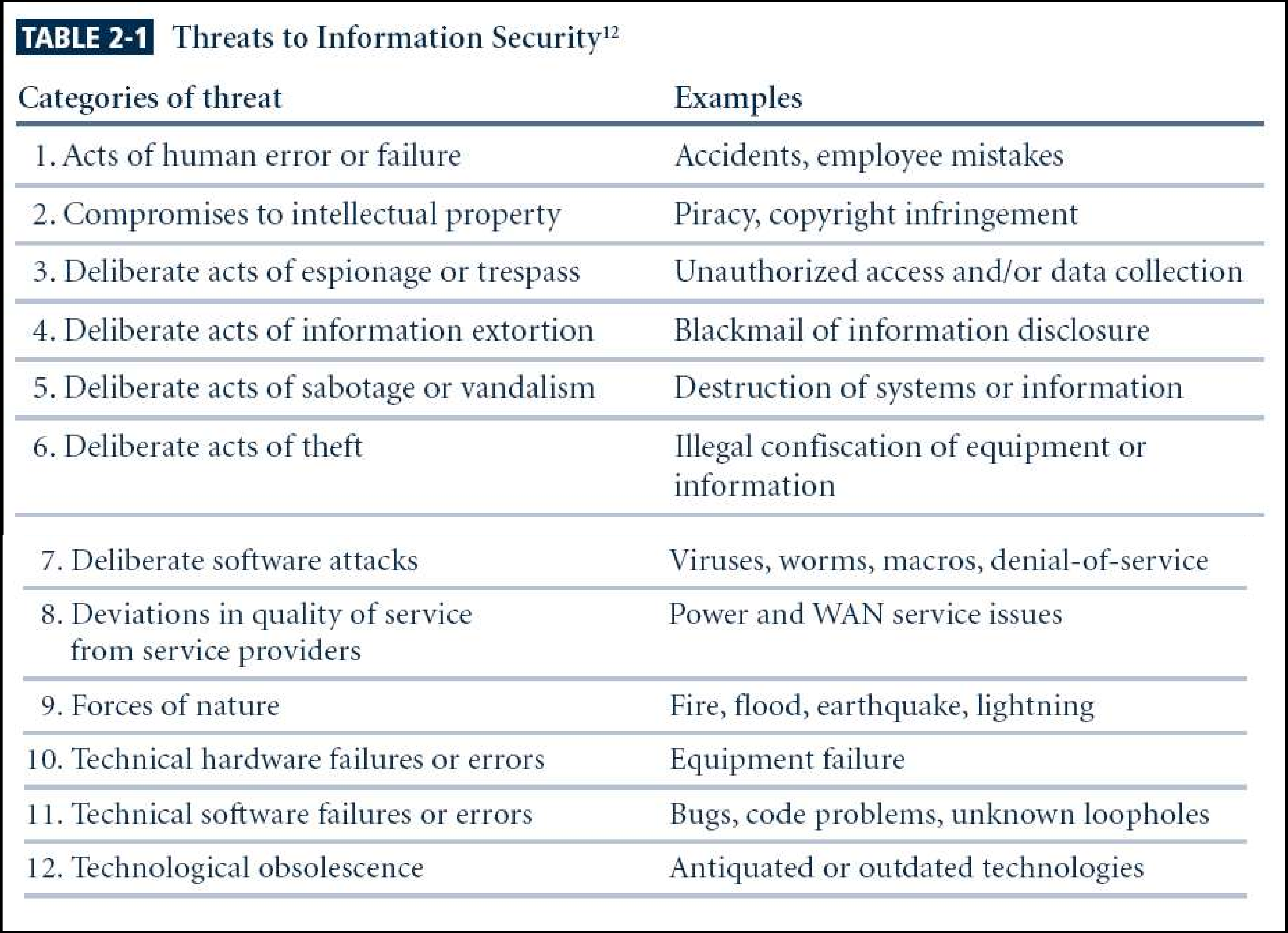


TABLE 2-1 Threats to Information Security[12]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Some common attacks

Malicious code

Hoaxes

Back doors

Password crack

Brute force

Dictionary

Denial-of-service (DoS) & distributed denial-of-service (DDoS)

Spoofing

Man-in-the-middle

Spam

Mail bombing

Sniffer

Social engineering

Buffer overflow

Timing

Risk management

Use some method of prioritizing risk
posed by each category of threat
& its related methods of attack

To manage risk,
you must identify & assess
the value of your information assets

Risk assessment assigns
comparative risk rating or score
to each specific information asset

Risk management
identifies vulnerabilities
in an organization’s information systems
& takes carefully reasoned steps
to assure
the confidentiality, integrity, and availability
of all the components
in an organization’s information system

SecSDLC: Design

Design phase actually consists of two distinct phases:

3. Logical design phase:
team members create & develop
a blueprint for security,
& examine & implement key policies

4. Physical design phase:
team members evaluate
the technology needed
to support the security blueprint,
generate alternative solutions,
& agree upon a final design

Security models

Security managers often use
established security models
to guide the design process

Security models provide frameworks
for ensuring that
all areas of security are addressed

Organizations can
adapt or adopt a framework to meet
their own information security needs

A critical design element
of the infosec program
is the infosec **policy**

Management must define
3 types of security policy:

1. General or security program policy
2. Issue-specific security policies
3. Systems-specific security policies

Another integral part
of the InfoSec program is the
security education and training program

SETA program consists of 3 elements:

1. security education
2. security training
3. security awareness

Purpose of SETA is to enhance security by:

✓ Improving awareness
✓ Developing skills & knowledge
✓ Building in-depth knowledge

Attention turns to the **design**
of the controls & safeguards
used to protect information
from attacks by threats

Three categories of controls:

1. Managerial
2. Operational
3. Technical

Managerial controls

Address the design & implementation
of the security planning process
& security program management

Management controls also address:

✓ Risk management
✓ Security control reviews

Operational controls

Cover management functions
& lower level planning, including:

✓ Disaster recovery
✓ Incident response planning
✓ Operational controls also address:
✓ Personnel security
✓ Physical security
✓ Protection of production inputs & outputs

Technical controls

Address those tactical & technical issues related to designing & implementing security in the organization

Technologies necessary to protect information are examined & selected

Contingency Planning

“What if …?”

Essential preparedness documents provide contingency planning (CP) to prepare, react & recover from circumstances that threaten the organization:

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

Physical Security addresses
the design, implementation, & maintenance
of countermeasures
that protect the physical resources
of an organization

Physical resources include:

✓ People
✓ Hardware
✓ Supporting information system elements

5. SecSDLC Implementation

Security solutions are
acquired, tested, implemented, & tested again

Personnel issues are evaluated
& specific training & education programs conducted

Perhaps most important element
of implementation phase
is management of project plan:

1. Planning project
2. Supervising tasks & action steps within project
3. Wrapping up project

InfoSec project team should consist of individuals experienced
in one or multiple
technical & non-technical areas, including:

✓ Champion
✓ Team leader
✓ Security policy developers
✓ Risk assessment specialists
✓ Security professionals
✓ Systems administrators
✓ End users

Staffing the infosec function

Each organization should examine the options
for staffing of the infosec function

Decide how to position & name
the security function

Plan for proper staffing of infosec function

Understand impact of infosec across every IT role

Integrate solid infosec concepts
into personnel management practices
of the organization

It takes a wide range of professionals
to support a diverse infosec program:

✓ Chief Information Officer (CIO)
✓ Chief Information Security Officer (CISO)
✓ Security managers
✓ Security technicians
✓ Data owners
✓ Data custodians
✓ Data users

Many organizations
seek professional certification
so that they can more easily identify
the proficiency of job applicants:

✓ CISSP
✓ SSCP
✓ GIAC
✓ SCP
✓ ICSA
✓ Security +
✓ CISM

6. SecSDLS Maintenance

Once infosec program is implemented,
it must be operated, properly managed,
& kept up to date
by means of established procedures

If the program
is not adjusting adequately
to the changes
in the internal or external environment,
it may be necessary
to begin the cycle again

While a systems management model
is designed to manage & operate systems,
a maintenance model
is intended to focus organizational effort
on system maintenance:

✓ External monitoring
✓ Internal monitoring
✓ Planning & risk assessment
✓ Vulnerability assessment & remediation
✓ Readiness & review
✓ Vulnerability assessment

One issue planned in the SecSDLC
is the systems management model

ISO management model
contains five areas:

1. Fault management
2. Configuration & name management
3. Accounting management
4. Performance management
5. Security management

Security Management Model

Fault Management involves
identifying & addressing faults

Configuration and Change Management
involve administration of components
involved in the security program
& administration of changes

Accounting and Auditing Management
involves chargeback accounting
& systems monitoring

Performance Management
determines if security systems
are effectively doing their jobs

Security Program Management

Once an infosec program is functional,
it must be operated and managed

In order to assist
in the actual management of infosec programs,
a formal management standard
can provide some insight
into the processes & procedures needed

This could be based on
the BS7799/ISO17799 model
or the NIST models described earlier

SDLC & the SecSDLC
both use the same 6 phases.

1. Investigation
2. Analysis
3. Logical design
4. Physical design
5. Implementation
6. Maintenance

Table 2-2 in our textbook
lists the steps unique to the SecSDLC.

Summary

Components of organizational planning

Planning for infosec implementation (especially strategic planning)

Systems Development Life Cycle (SDLC)

↓

Security Systems Development Life Cycle (SecSDLC)

Assignments for next week:

1. Find an example of corporate mission, vision, & values statements on the web.
How many mention security?

2. Find your organization’s mission, vision, & values statement.
Does it mention security?

3. Find 3 stories in the news that mention threats to infosec.

Thank you!