Information Security Management

Chapter 1
Introduction to the Management of Information Security

Webster University
Scott Granneman

“If this is the information superhighway,
it’s going through
a lot of bad, bad neighborhoods.”

-- Dorian Berger, 1997

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

Recognize the importance of information technology & understand who is responsible for protecting an organization's information assets

Know & understand the definition & key characteristics of information security

Know & understand the definition & key characteristics of leadership & management

Recognize the characteristics that differentiate information security management from general management

Obvious, but often unsaid, things:

Information technology is critical to business and society
… & always has been
(what happens if it’s not available?)

Computer security is evolving into information security

Information security is the responsibility of every member of an organization, but managers play a critical role

Information security involves
3 distinct communities of interest:

Information security
managers & professionals

Information technology
managers & professionals

Non-technical business
managers & professionals

Communities of interest:

InfoSec community:
protect information assets from threats

IT community:
support business objectives by supplying appropriate information technology

Business community:
articulate & communicate policy
& allocate resources

InfoSec includes
information security management,
computer security,
data security,
& network security.

Policy is central to all infosec efforts.

Components of InfoSec

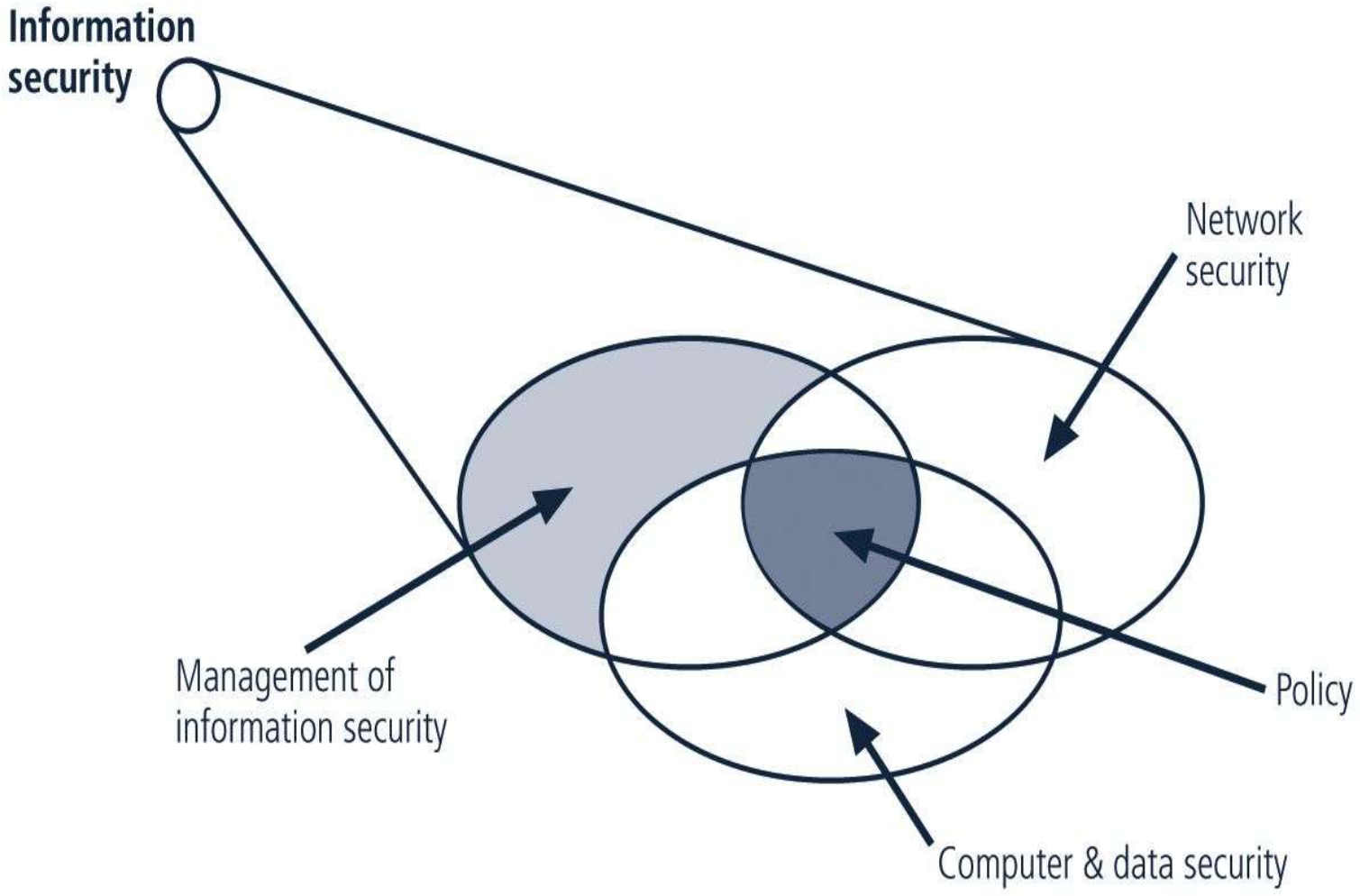

FIGURE 1-1 Components of Information Security

The C.I.A. triangle is made up of:

Confidentiality

Integrity

Availability

(Over time the list of characteristics has expanded, but these 3 remain central)

CIA +

Confidentiality

Integrity

Availability

Privacy

Identification

Authentication

Authorization

Accountability

Confidentiality of information ensures that only those with sufficient privileges may access certain information.

To protect confidentiality of information, a number of measures may be used, including:

✓ Information classification
✓ Secure document storage
✓ Application of general security policies
✓ Education of information custodians & end users

Integrity is the quality or state of being whole, complete, & uncorrupted.

The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state.

Corruption can occur while information is being compiled, stored, or transmitted.

Availability is making information
accessible to user access
without interference or obstruction
in the required format.

A user in this definition may be either
a person
or another computer system.

Availability means
availability to authorized users.

Privacy

Information is to be used
only
for purposes known to the data owner.

This does not focus
on freedom from observation,
but rather
that information will be used
only
in ways known to the owner.

Information systems possess
the characteristic of **identification**
when they are able
to recognize individual users.

Identification and authentication
are essential to establishing
the level of access or authorization
that an individual is granted.

Authentication occurs
when a control provides proof
that a user possesses
the identity that he or she claims.

After the identity of a user
is authenticated,
a process called **authorization**
provides assurance that the user
(whether a person or a computer)
has been specifically & explicitly authorized
by the proper authority
to access, update, or delete
the contents of an information asset.

The characteristic of **accountability**
exists when a control
provides assurance
that every activity undertaken
can be attributed
to a named person or automated process.

To review ... CIA +

Confidentiality

Integrity

Availability

Privacy

Identification

Authentication

Authorization

Accountability

Think about your home computer.

How do you secure it?

How do you guarantee
confidentiality, integrity, & availability?

NSTISSC Security Model

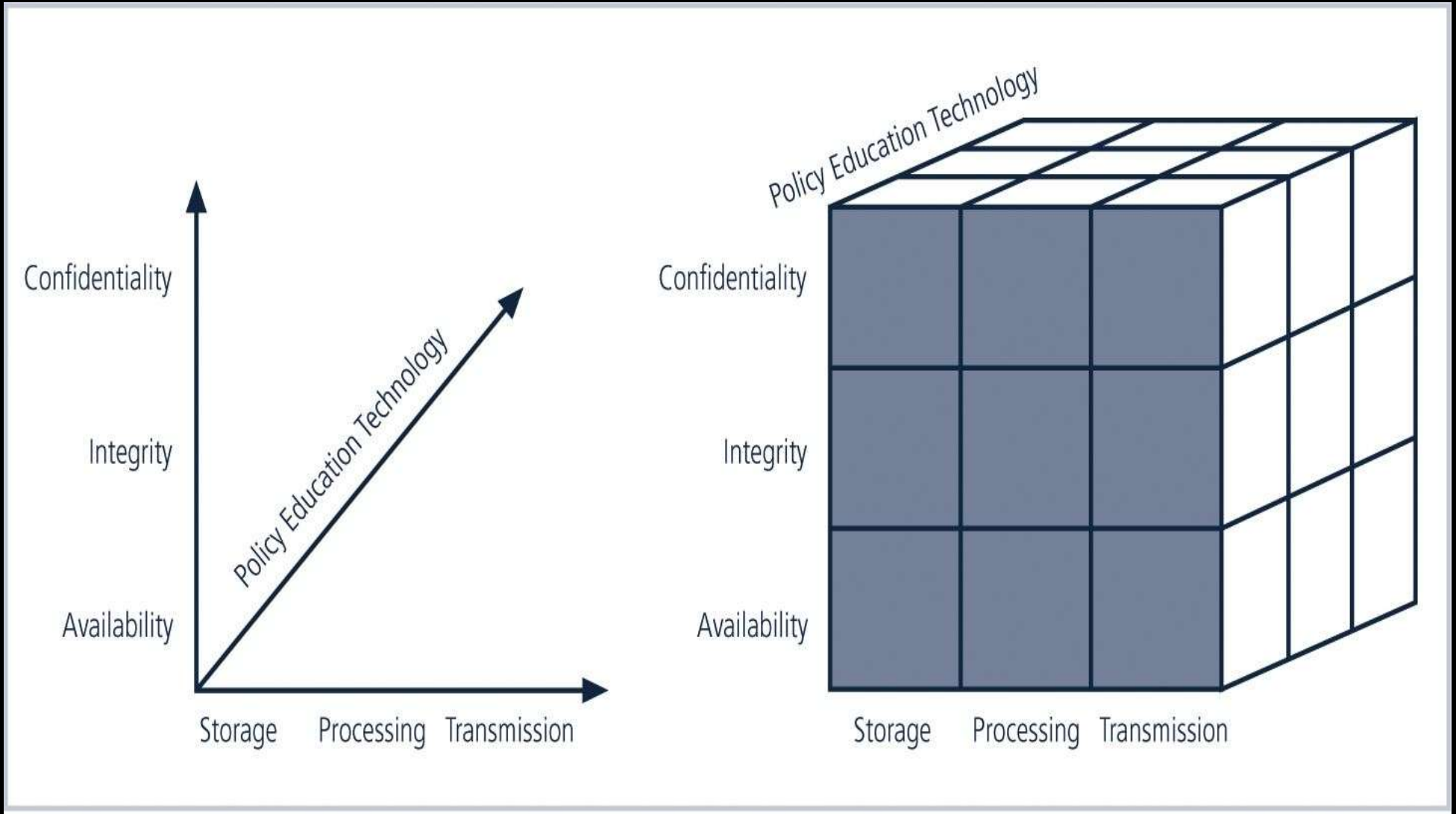

FIGURE 1-2 NSTISSC Security Model

Two well-known approaches to management:

Traditional management theory using principles of planning, organizing, staffing, directing, & controlling (POSDC).

Popular management theory using principles of management into planning, organizing, leading, & controlling (POLC).

The Planning-Controlling Link

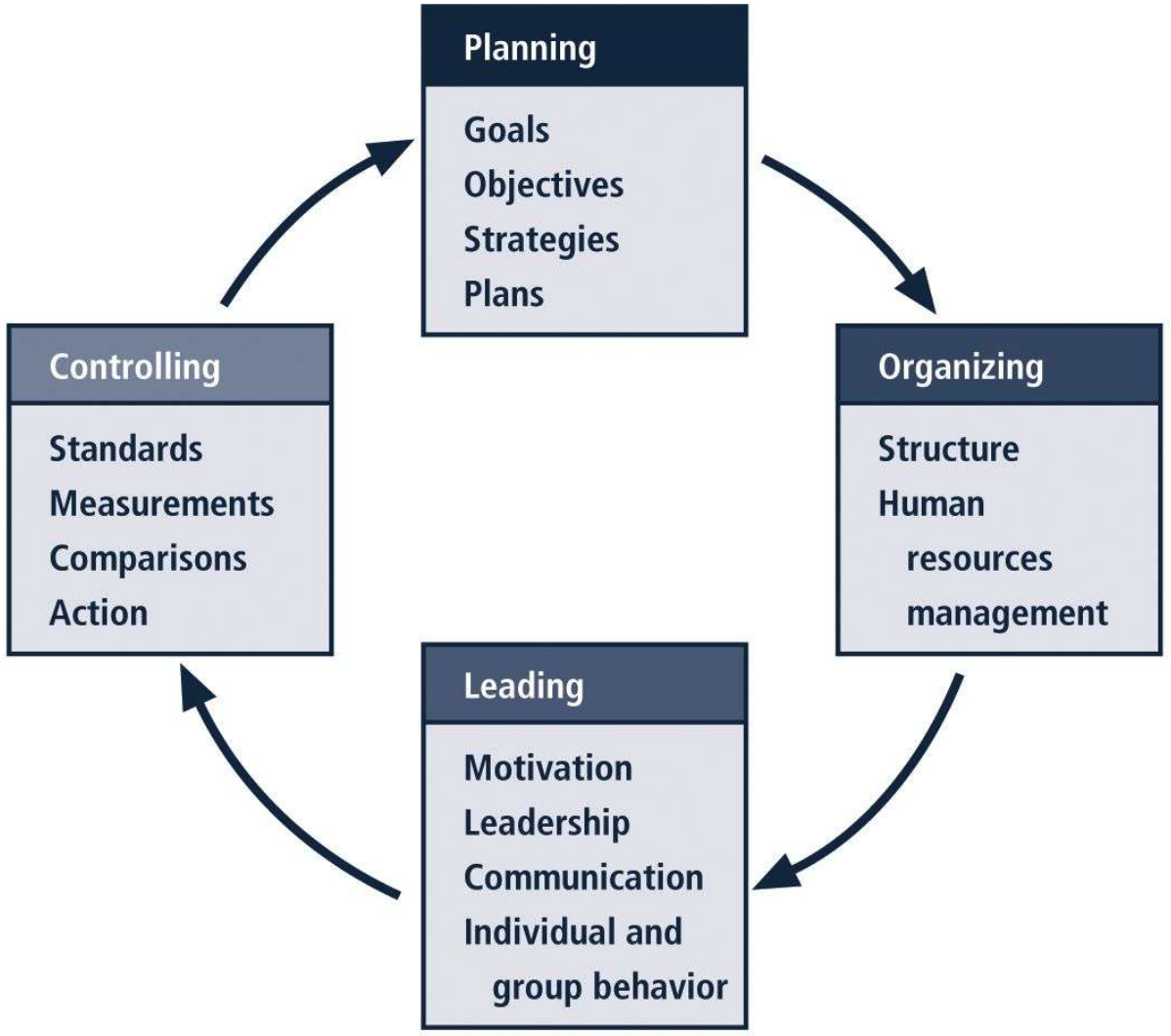

FIGURE 1-3 The Planning-Controlling Link[8]

Planning is the process that develops, creates, & implements strategies for the accomplishment of objectives.

Three levels of planning:

1. Strategic
2. Tactical
3. Operational

In general,
planning begins
with the strategic plan
for the whole organization.

To do this successfully,
an organization must thoroughly define
its goals & objectives.

Organization:
structuring of resources
to support
the accomplishment of objectives.

Organizing tasks requires determining:

✓ What is to be done
✓ In what order
✓ By whom
✓ By which methods
✓ When

Leadership encourages
the implementation
of the planning and organizing functions,
including supervising
employee behavior, performance,
attendance, & attitude.

Leadership generally addresses
the direction and motivation
of the human resource.

Control is monitoring progress
toward completion
& making necessary adjustments
to achieve the desired objectives.

Controlling function determines
what must be monitored as well
using specific control tools
to gather and evaluate information.

Four categories of control tools:

Information

Financial

Operational

Behavioral

The Control Process

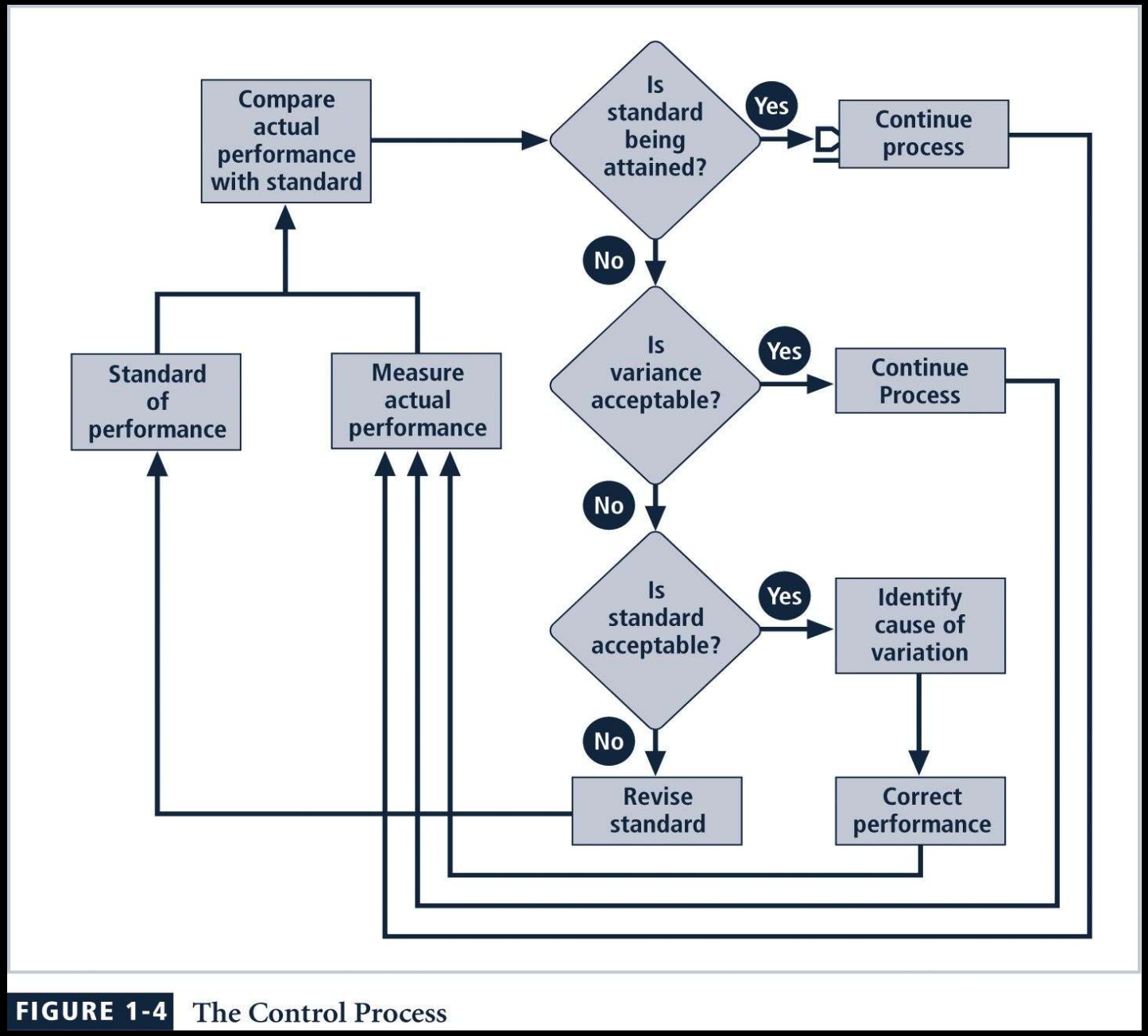

FIGURE 1-4 The Control Process

How to Solve Problems

Step 1:
Recognize & define the problem

Step 2:
Gather facts & make assumptions

Step 3: Develop possible solutions

Step 4:
Analyze & compare possible solutions

Step 5:
Select, implement, & evaluate a solution

Feasibility Analyses

Economic feasibility assesses
costs & benefits of a solution

Technological feasibility assesses
an organization's ability
to acquire & manage a solution

Behavioral feasibility assesses
whether members of an organization
will support a solution

Operational feasibility assesses
if an organization can integrate a solution

Extended characteristics or principles of infosec management (AKA, the 6 P’s)

Planning

Policy

Programs

Protection

People

Project Management

1. Planning
as part of InfoSec management
is an extension
of the basic planning model
discussed earlier in this chapter.

Included in the InfoSec planning model
are activities necessary to support
the design, creation, and implementation
of information security strategies
as they exist
within the IT planning environment.

Several types of InfoSec plans exist:

Incident response

Business continuity

Disaster recovery

Policy

Personnel

Technology rollout

Risk management

Security program,
including education, training, & awareness

2. Policy:
set of organizational guidelines
that dictates certain behavior
within the organization.

In InfoSec, there are
3 general categories of policy:

1. General program policy
(Enterprise Security Policy)

2. An issue-specific security policy (ISSP)

3. System-specific policies (SSSPs)

3. Programs:
specific entities managed
in the information security domain.

One such entity:
security education training & awareness
(SETA)
program.

Other programs that may emerge include
the physical security program,
complete with fire, physical access,
gates, guards, & so on.

4. **Protection**:

Risk management activities,
including risk assessment and control,
as well as protection mechanisms,
technologies, & tools.

Each of these mechanisms
represents some aspect
of the management of specific controls
in the overall information security plan.

5. People
are the most critical link
in the information security program.

It is imperative
that managers continuously recognize
the crucial role that people play.

Includes information security personnel
and the security of personnel, as well as
aspects of the SETA program.

6. Project management discipline
should be present throughout
all elements
of the information security program.

This involves:

✓ Identifying and controlling
the resources applied to the project

✓ Measuring progress
& adjusting the process
as progress is made toward the goal

In summation:

Communities of interest

CIA+

Planning, Organizing, Leading, Controlling

Principles of infosec management
(the 6 P’s)

Thank you!

Scott Granneman