TEL2813/IS2820 Security Management

Lecture 1

Jan 15, 2008

Contact

- James Joshi
- 706A, IS Building
- Phone: 412-624-9982
- E-mail: jjoshi@mail.sis.pitt.edu
- Web: http://www.sis.pitt.edu/~lersais/IS2820/Spring07/
- Office Hours: Monday: 1.00 – 3.00 p.m. or By appointments
- GSA: will be announced later

Course objective

- The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of security of an enterprise information system.

Course objective

- After the course, ability to to carry out
  - detailed analysis of enterprise security by performing various types of analysis
    - vulnerability analysis, penetration testing,
    - audit trail analysis,
    - system and network monitoring, and
    - Configuration management, etc.
  - Carry out the task of security risk management using various practical and theoretical tools.

Course objective

- After the course, ability to carry out
  - Design detailed enterprise wide security plans and policies, and deploy appropriate safeguards (models, mechanisms and tools) at all the levels due consideration to
    - the life-cycle of the enterprise information systems and networks,
    - legal and social environment
  - Be able to certify products according to IA standards (Common Criteria Evaluations)

Course content

- Introduction to Security Management
  - Security policies/models/mechanisms
  - Security Management Principles, Models and Practices
  - Security Planning/ Asset Protection
  - Security Programs and Disaster Recovery Plans
- Standards and Security Certification Issues
  - Rainbow Series, Common Criteria
  - Security Certification Process
- National/International Security Laws and Ethical Issues
- Security Analysis and Safeguards
  - Vulnerability analysis (Tools & Tech.)
  - Penetration testing
  - Risk Management
  - Protection Mechanisms and Incident handling
    - Access Control and Authentication architecture
    - Configuration Management
    - Auditing systems audit trail analysis
    - Network defense and countermeasures
      - Intrusion Detection Systems (SNORT)
      - Architectural configurations
      - Firewall configurations
      - Virtual private networks
      - Computer and network forensic
    - Privacy Protection
  - Case studies
    - Lab exercises

Course Material

- Recommended course material
  - Management of Information Security, M. E. Whitman, H. J. Mattord
  - Guide to Disaster Recovery, M. Erbschilde
  - Guide to Network Defense and Countermeasures, G. Holden
  - Real Digital Forensics: Computer Security and Incident Response, 1/e; Keith J. Jones, Richard Bejtlich, Curtis W. Rose
  - Computer Security: Art and Science, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003
  - Security in Computing, 2nd Edition, Charles P. Pfleeger, Prentice Hall
  - Software Security: Building Security In (by Gary McGraw)
  - The Art of Software Security Assessment : Identifying and Preventing Software Vulnerabilities (by Mark Dowd, John McDonald, Justin Schuh)

  - A list of papers and NIST/GAO documents for reading

Tentative Grading

- Assignments (50%)
  - Homework/Quiz/Paper review/Lab (35%)
  - Class Participation/Seminar attendance (5%)
  - 2-3 presentation (10%)
- Exams 20%
- Project 30%

Course Policies

- Your work MUST be your own
  - Zero tolerance for cheating/plagiarism
  - You get an F for the course if you cheat in anything however small – NO DISCUSSION
  - Discussing the problem is encouraged
- Homework
  - Penalty for late assignments (15% each day)
  - Ensure clarity in your answers – no credit will be given for vague answers
  - Homework is primarily the GSA’s responsibility
- Check webpage for everything!
  - You are responsible for checking the webpage for updates

Introduction

Introduction

- Information technology is critical to business and society
- Computer security is evolving into information security
- Information security is the responsibility of every member of an organization, but managers play a critical role

Introduction

- Information security involves three distinct communities of interest
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals

Communities of Interest

- InfoSec community:
  - protect information assets from threats
- IT community:
  - support business objectives by supplying appropriate information technology
- Business community:
  - policy and resources

What Is Security?

- “The quality or state of being secure—to be free from danger”

- Security is achieved using several strategies simultaneously

Security and Control

- Examples
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security

- Controls
  - Physical Controls
  - Technical Controls
  - Administrative
  - Prevention – Detection – Recovery
  - Deterrence, Corrective

InfoSec Components

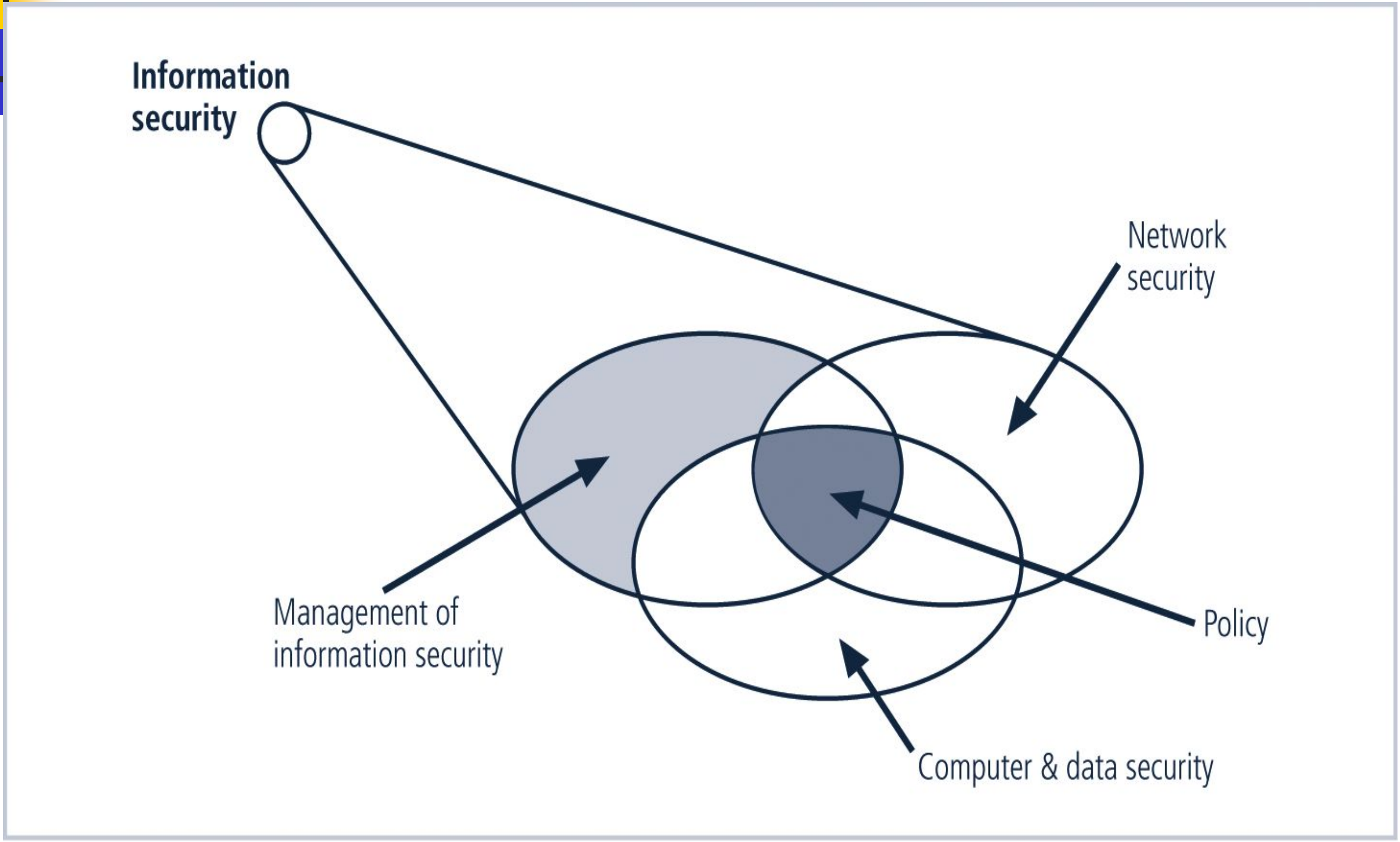


FIGURE 1-1 Components of Information Security

CIA Triangle

- The C.I.A. triangle is made up of
  - Confidentiality
  - Integrity
  - Availability
- Over time the list of characteristics has expanded, but these three remain central
- CNSS model is based on CIA

NSTISSC Security Model (4011)

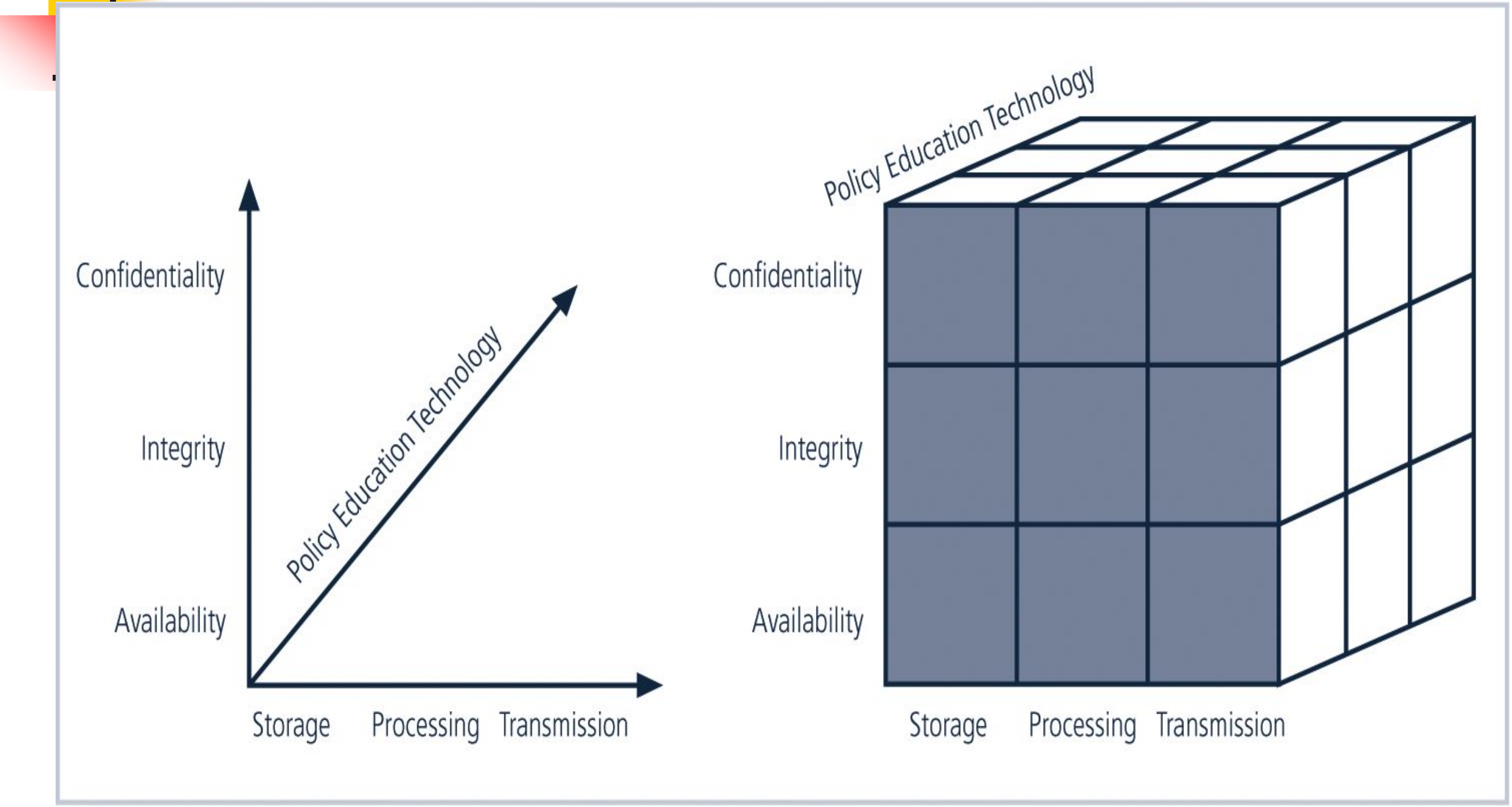


FIGURE 1-2 NSTISSC Security Model

Key Concepts: Confidentiality

- Confidentiality
  - only those with sufficient privileges may access certain information
- Confidentiality model
  - Bell-LaPadula
    - No write down & No read up
  - TCSEC/TNI (Orange, Red Book)

- Some threats
  - Hackers
  - Masqueraders
  - Unauthorized users
  - Unprotected download of files
  - LANS
  - Trojan horses

Key Concepts: Integrity

- Integrity
  - Integrity is the quality or state of being whole, complete, and uncorrupted
- Integrity model
  - Biba/low water mark
    - No write up & No read down
  - Clark-Wilson
    - Separation of duty
  - Lipner
- Other issues
  - Origin integrity
  - Data integrity

Key Concepts: Availability

- Availability
  - making information accessible to user access without interference or obstruction
- Survivability
  - Ensuring availability in presence of attacks

Key Concepts: privacy

- 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

Key Concepts: Identification

- Identification
  - 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

Key Concepts: Authentication & Authorization

- Authentication
  - Authentication occurs when a control provides proof that a user possesses the identity that he or she claims
- Authorization
  - authorization provides assurance that the user has been specifically and explicitly authorized by the proper authority to access the contents of an information asset

Key Concepts: Accountability; Assurance

- Accountability
  - The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process
- Assurance
  - Assurance that all security objectives are met

What Is Management?

- A process of achieving objectives using a given set of resources
- To manage the information security process, first understand core principles of management
- A manager is
  - "someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals"

Managerial Roles

- Informational role: Collecting, processing, and using information to achieve the objective
- Interpersonal role: Interacting with superiors, subordinates, outside stakeholders, and other
- Decisional role: Selecting from alternative approaches and resolving conflicts, dilemmas, or challenges

Differences Between Leadership and Management

- The leader influences employees so that they are willing to accomplish objectives
- He or she is expected to lead by example and demonstrate personal traits that instill a desire in others to follow
- Leadership provides purpose, direction, and motivation to those that follow
- A manager administers the resources of the organization, budgets, authorizes expenditure

Characteristics of a Leader

1. Bearing
2. Courage
3. Decisiveness
4. Dependability
5. Endurance
6. Enthusiasm
7. Initiative
8. Integrity
9. Judgment
10. Justice
11. Knowledge
12. Loyalty
13. Tact
14. Unselfishness

Used by US military

What Makes a Good Leader? Action plan

1. Know yourself and seek self-improvement
2. Be technically and tactically proficient
3. Seek responsibility and take responsibility for your actions
4. Make sound and timely decisions
5. Set the example
6. Know your [subordinates] and look out for their well-being
7. Keep your subordinates informed
8. Develop a sense of responsibility in your subordinates
9. Ensure the task is understood, supervised, and accomplished
10. Build the team
11. Employ your team in accordance with its capabilities

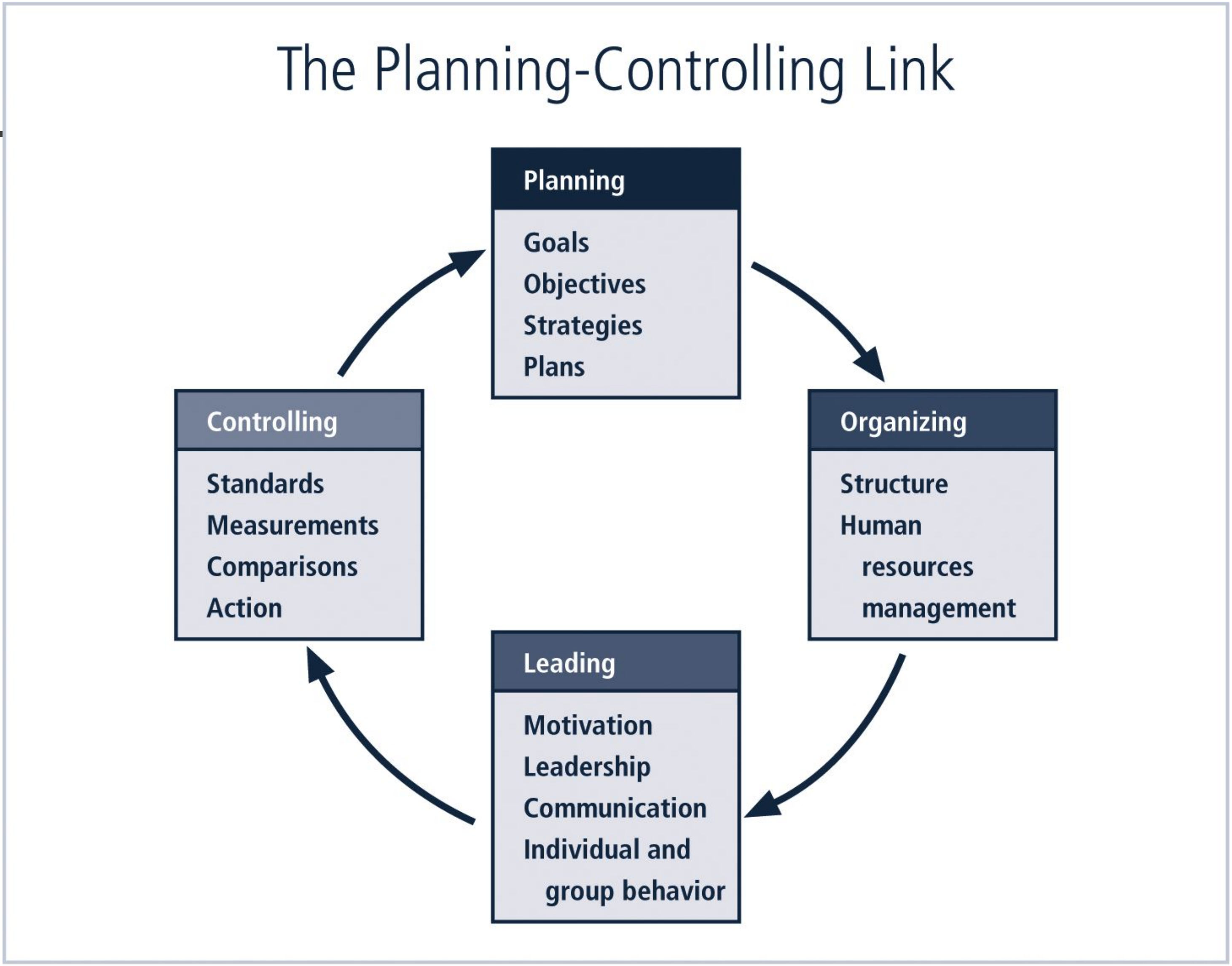
Leadership quality and types

- A leader must:
  - BE a person of strong and honorable character
  - KNOW you, the details of your situation, the standards to which you work, human nature, and your team
  - DO by providing purpose, direction, and motivation to your team
- Three basic behavioral types of leaders:
  - Autocratic
  - Democratic
  - Laissez-faire

Characteristics of Management

- Two well-known approaches to management:
  - Traditional management theory using principles of planning, organizing, staffing, directing, and controlling (POSDC)
  - Popular management theory using principles of management into planning, organizing, leading, and controlling (POLC)

The Planning–Controlling Link



The Planning-Controlling Link

Planning

Goals
Objectives
Strategies
Plans

Organizing

Structure
Human resources management

Leading

Motivation
Leadership
Communication
Individual and group behavior

Controlling

Standards
Measurements
Comparisons
Action

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

Planning & Organization

- Planning: process that develops, creates, and implements strategies for the accomplishment of objectives
- Three levels of planning
  - Strategic
  - Tactical
  - Operational
- Organization: structuring of resources to support the accomplishment of objectives

Leadership

- Encourages the implementation of
  - the planning and organizing functions,
    - Includes supervising employee behavior, performance, attendance, and attitude
- Leadership generally addresses the direction and motivation of the human resource

Control

- Control:
  - Monitoring progress toward completion
  - Making necessary adjustments to achieve the desired objectives
- Controlling function determines what must be monitored as well as using specific control tools to gather and evaluate information

Control Tools

- Four categories:
  - Information
    - Information flows/ communications
  - Financial
    - Guide use of monetary resources (ROI,CBA,..)
  - Operational
    - PERT, Gantt, process flow
  - Behavioral
    - Human resources

The Control Process

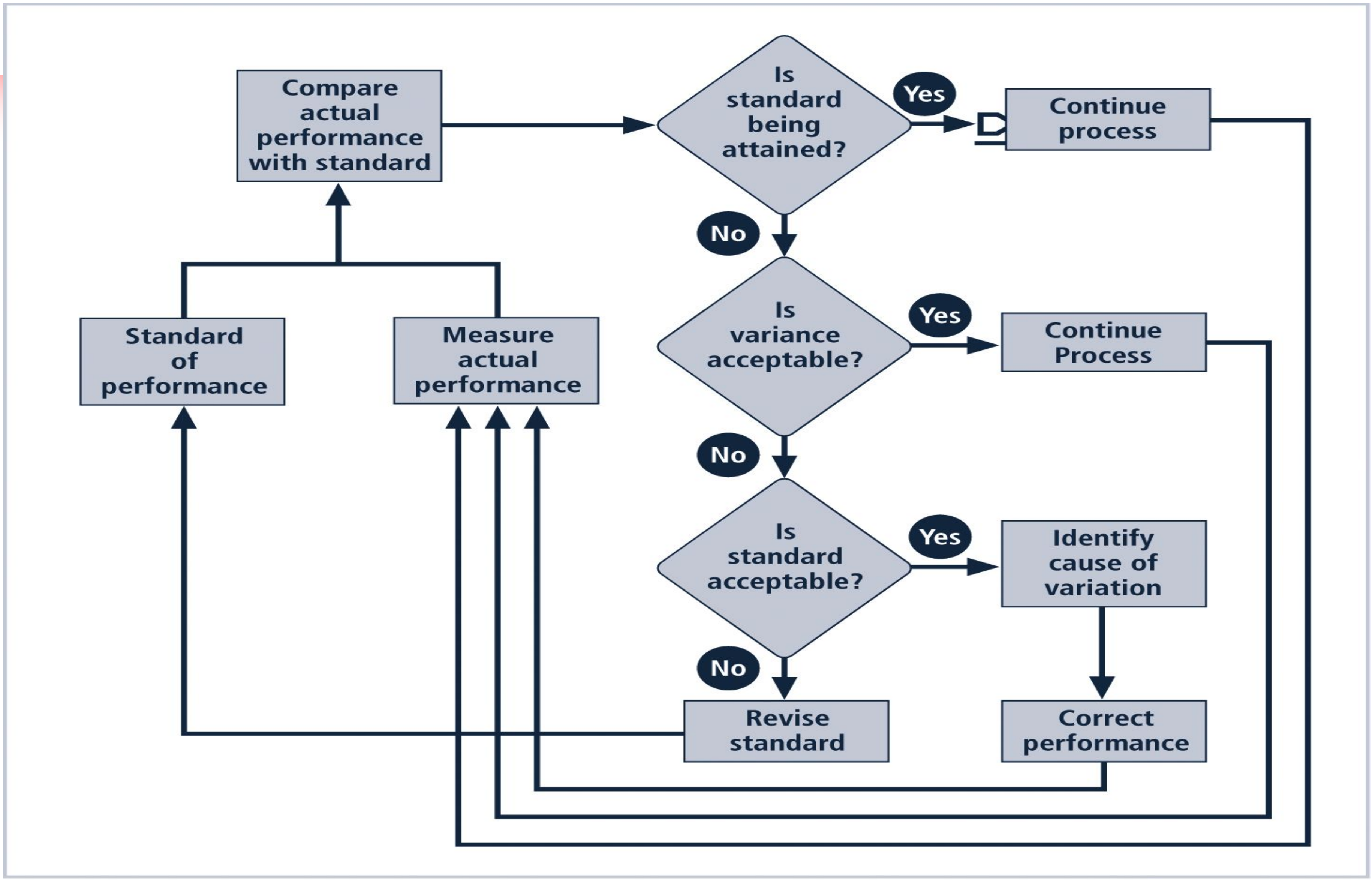


FIGURE 1-4 The Control Process

Solving Problems

- Step 1: Recognize and Define the Problem
- Step 2: Gather Facts and Make Assumptions
- Step 3: Develop Possible Solutions (Brainstorming)
- Step 4: Analyze and Compare the Possible Solutions (Feasibility analysis)
- Step 5: Select, Implement, and Evaluate a Solution

Feasibility Analyses

- Economic feasibility assesses costs and benefits of a solution
- Technological feasibility assesses an organization’s ability to acquire and manage a solution
- Behavioral feasibility assesses whether members of the organization will support a solution
- Operational feasibility assesses if an organization can integrate a solution

Principles Of Information Security Management

- The extended characteristics of information security are known as the six Ps:
  - Planning
  - Policy
  - Programs
  - Protection
  - People
  - Project Management

InfoSec Planning

- Planning as part of InfoSec management
  - is an extension of the basic planning model discussed earlier
- 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

InfoSec Planning Types

- Several types of InfoSec plans exist:
  - Incident response
  - Business continuity
  - Disaster recovery
  - Policy
  - Personnel
  - Technology rollout
  - Risk management and
  - Security program including education, training and awareness

Policy

- Policy: set of organizational guidelines that dictates certain behavior within the organization
- In InfoSec, there are three general categories of policy:
  - General program policy (Enterprise Security Policy)
  - An issue-specific security policy (ISSP)
    - E.g., email, Intenert use
  - System-specific policies (SSSPs)
    - E.g., Access control list (ACLs) for a device

Programs

- Programs are operations managed as
  - specific entities in the information security domain
  - Example:
    - A security education training and awareness (SETA) program is one such entity
  - Other programs that may emerge include
    - a physical security program, complete with fire, physical access, gates, guards, and so on

Protection

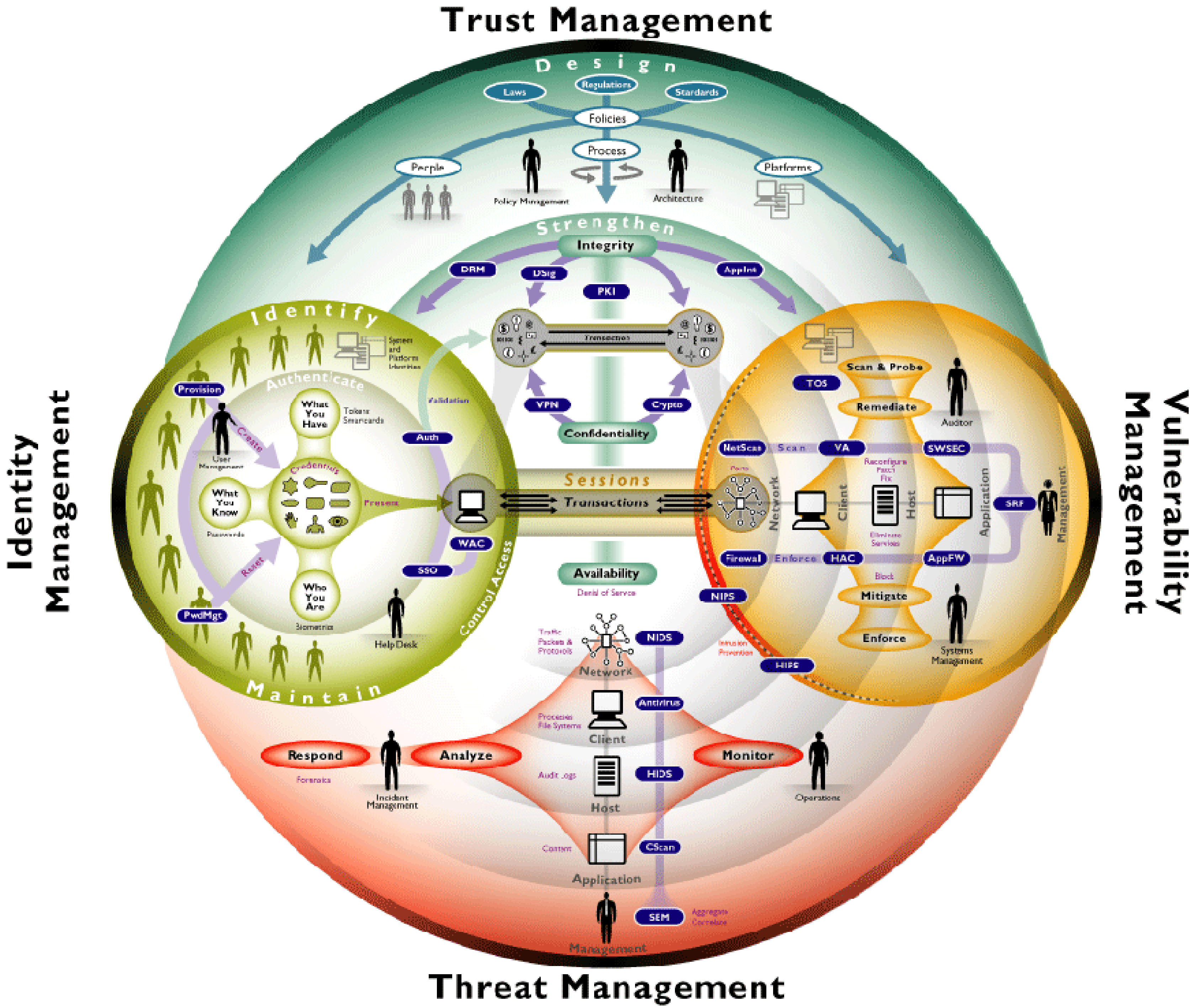
- Risk management activities, including
  - risk assessment and control, &
- Protection mechanisms, technologies & tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall security plan

People

- People are the most critical link in the information security program
    - Human firewall
- 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

Project Management

- Project management discipline should be present throughout all elements of the information security program
- Involves
  - Identifying and controlling the resources applied to the project
  - Measuring progress and adjusting the process as progress is made toward the goal


Trust Management
Design
Laws
Regulations
Standards
Policies
Process
People
Policy Management
Architecture
Platforms
Strengthen
Integrity
DRM
DSig
PKI
Applet
Transaction
VPN
Crypto
Confidentiality
Sessions
Transactions
Availability
Denial of Service
Identity Management
Identify
System and Platform Identities
Provision
Authenticate
What You Have
Tokens Smartcards
Validation
Auth
Create
User Management
Credentials
What You Know
Passwords
Present
WAC
SSO
Reset
PwdMgt
Who You Are
Biometrics
Help Desk
Control Access
Maintain
Vulnerability Management
Scan & Probe
TOS
Remediate
Auditor
NetScan
Scan
VA
SWSEC
Ports
Reconfigure
Patch
Fix
Network
Client
Host
Application
SRF
Management
Eliminate Services
Firewall
Enforce
HAC
AppFW
Block
NIPS
Mitigate
Enforce
Systems Management
Intrusion Prevention
HIPS
Traffic
Packets &
Protocols
NIDS
Network
Antivirus
Processes
File Systems
Client
Respond
Forensics
Incident Management
Analyze
Audit Logs
HIDS
Host
Monitor
Operations
Content
CScan
Application
SEM
Aggregate
Correlate
Management
Threat Management